

UNIVERSITY OF TARTU
FACULTY OF MATHEMATICS AND COMPUTER SCIENCE
Institute of Computer Science
Cybersecurity Curriculum

Sarbar Tursunova

**Comparing Security Risk-oriented Modelling
Languages to Manage Social Engineering
Risks**

Master's Thesis (30 ECTS)

Supervisor(s): Raimundas Matulevičius

Tartu 2015

Comparing Security Risk-oriented Modelling Languages to Manage Social Engineering Risks

Abstract:

Social engineering security risk management is emerging as a central technique for dealing with identification of occurring risks on the daily basis. Unfortunately, its standards might have limitations in support with security modelling languages and comprehension of users. This is a problem because lack of understanding can cause misinterpretation of analysis. Nowadays, same security events occur periodically, but they are not treated properly. It might be because ordinary users do not see vulnerabilities or their misunderstanding of on-going process of risk treatment. Without knowing what is clear to ordinary users and what should be improved any social engineering analysis is irrelevant.

The paper applies structured approach in identification of one security risk management standard that can be applied with different modelling languages. For a more in-depth analysis in this paper considered several modelling languages as BPMN, Secure Tropos and Misuse case. Taking into account the main aspect of the study in social engineering is psychological manipulation of people, author considered as a good foundation of the illustration a book of Kevin Mitnick "The art of deception". One case has been chosen for a further study and analysed using ISSRM domain model with application of aforementioned three security modelling languages.

To identify certain concepts or logic of ordinary users and taking into account their lack of knowledge in information technology this paper has been concentrated on weaknesses of modelling approaches for social engineering analysis. This led to the result that overall BPMN constructs and Secure Tropos concepts are preferred by users. Also based on collected results, we tried to make a parallel between understanding of concepts and constructs for participants. Percentage wise understanding of constructs showed higher results than concepts. Business asset, IS asset, threat, attack method, risk treatment, security requirement and control are easily identified in the form of constructs. Concepts are have received higher score in following aspects: Business Asset, Security criterion, Impact, Event, Vulnerability, Threat, Threat agent, Security requirement.

Keywords:

Social engineering, security risk management, ISSRM, CORAS, OCTAVE, ISO 17799, COBRA, BPMN, Secure Tropos, Misuse cases, Information system

Turvariskidele Orienteeritud Modelleerimiskeelte Võrdlus

Manipuleerimisrünnete Riskijuhtimiseks

Lühikokkuvõte:

Manipuleerimisrünnete turvariskide juhtimine on muutumas igapäevase riskide identifitseerimise keskseks tehnikaks. Kahjuks võivad selle standardid turva-modelleerimiskeelte ja kasutajate hõlmamise toetamisel olla piiratud. See on probleem, kuna vähene mõistmine võib viia analüüsi väärtõlgenduseni. Tänapäeval toimuvad korrapäraselt ühed ja samad turvasündmused, kuid neid ei käsitleta kohaselt. See võib tuleneda sellest, et tavakasutajad ei märka nõrkusi või tõlgendavad käimasolevat riskijuhtimisprotsessi vääralt. Teadmata, mis on tavakasutajale selge ja mida tuleks parandada, ei ole ükski manipuleerimisrünnete analüüs asjakohane.

Selles töös rakendatakse struktureeritud lähenemist ühe turvariskide juhtimise standardi identifitseerimisele, mida saab rakendada eri modelleerimiskeeltega. Sügavamaks analüüsiks on selles töös kasutatud eri modelleerimiskeeli, nagu äriprotsesside modelleerimiskeel (ingl BPMN), Secure Tropos ja Misuse Case. Võttes arvesse, et manipuleerimisrünnete uurimise põhiaspekt on inimeste psühhomaniipulatsioon, pidas autor heaks töö illustreerimise alusmaterjaliks Kevin Mitnicki raamatut „The art of deception”. Üks juhtum on valitud lähemaks uurimiseks ja analüüsitud, kasutades infosüsteemi turvariskide haldamise (ingl ISSRM) domeenimudelit eelpool mainitud kolme turva-modelleerimiskeele rakendusega.

Identifitseerimaks tavakasutajate konkreetseid kontseptsioone või loogikat ja võtmaks arvesse nende infotehnoloogiateadmiste vähesust, on see töö keskendatud modelleerimislähenemise nõrkadele külgedele manipuleerimisrünnete analüüsis. See viis tulemuseni, et kasutajad eelistavad üldisi BPMN-i konstruktsioone ja Secure Tropose kontseptsiooni. Samuti, tuginedes kogutud tulemustele, püüdsime tõmmata paralleeli kontseptsioonide mõistmise ja osalejate konstruktsioonide vahel. Protsentuaalselt olid konstruktsioonide mõistmise tulemused kontseptsioonide mõistmise tulemustest kõrgemad. Ärivar, IS-vara, oht, ründmeetod, riskihaldus, turvanõue ja kontroll on konstruktsioonide vormis kergesti identifitseeritavad. Kontseptsioonide skoor oli kõrgem järgnevais aspektides: ärivar, turvakriteerium, mõju, sündmus, nõrkus, oht, ohuagent, turvanõue.

Võtmesõnad:

Manipuleerimisrünne, turvariskide juhtimine, ISSRM, CORAS, OCTAVE, ISO 17799, COBRA, BPMN, Secure Tropos, Misuse Cases, infosüsteem

Table of Contents

List of Tables.....	6
List of Figures	8
Abbreviations	10
1 Introduction	11
2 Approaches for Security Risk Management	13
2.1 Security Risk Management.....	13
2.2 Different Risk Management Standards	13
2.3 Security Risk Management Methodologies.....	14
2.3.1 CORAS	14
2.3.2 OCTAVE.....	15
2.3.3 Domain Model of ISSRM	16
2.4 Summary.....	17
3 Social Engineering	19
3.1 Role of Social Engineering.....	19
3.2 Examples of Social Engineering Attacks	20
3.2.1 Example of Social Engineering Attack Via Telephone	20
3.2.2 Example of Social Engineering Attack Through Search in Recycle Bin.....	21
3.2.3 Example of Social Engineering Attack Through Internet.....	21
3.2.4 Example of Social Engineering Attack Through Persuasion	24
3.2.5 Example of Social Engineering Attack Breaking Through Computer Network	24
3.3 Summary.....	26
4 Security Modelling Languages	27
4.1 Overview of Security Modelling Languages.....	27
4.2 BPMN.....	28
4.2.1 Alignment of BPMN to ISSRM Domain Model.....	28
4.2.2 Social Engineering Example in BPMN.....	29
4.3 Misuse case.....	32
4.3.1 Alignment of SROMUC to ISSRM Domain Model	32
4.3.2 Social Engineering Example in SROMUC	33
4.4 Secure Tropos.....	34
4.4.1 Alignment of Secure Tropos with ISSRM	35
4.4.2 Social Engineering Example in Secure Tropos.....	37
4.5 Discussion.....	42
5 An Experiment Report Outline	44

5.1	Problem Statement.....	44
5.2	Planning of Questionnaire	44
5.3	Experiment Operation	45
5.4	Analysis and Interpretation.....	45
5.5	Threat to Validity	48
5.6	Discussion.....	48
5.7	Summary.....	49
6	Conclusion and Future Work	50
6.1	Conclusion	50
6.2	Limitations.....	50
6.3	Future Work.....	51
7	References	52
	Appendix	56
	I. Social Engineering Cases.....	56
	II. Social Engineering Examples in BPMN	93
	III. Social Engineering Examples in MUC	100
	IV. Social Engineering Examples in Secure Tropos	107
	V. Questionnaire of BPMN.....	115
	VI. Questionnaire of Misuse Case	118
	VII. Questionnaire of Secure Tropos	121
	VIII. Data upon BPMN Concepts and Constructs	124
	IX. Data upon Misuse Case Concepts and Constructs	130
	X. Data upon Secure Tropos Concepts and Constructs	136
	License	141

List of Tables

Table 1. Comparison of modelling approaches.....	18
Table 2. Example of managing Via phone securityrisk	21
Table 3. Example of managing Stevie’s scam security risk.....	22
Table 4. Example of managing Graduating without Honor’s case security risk	23
Table 5. Example of managing Steve Cramer’s story security risk	25
Table 6. Example of managing The dictionary as an attack tool security risk	26
Table 7. ISSRM assets concepts modelled in BPMN	31
Table 8. ISSRM risk treatment related-concepts modelled in BPMN	32
Table 9. ISSRM risks concepts modelled in BPMN.....	33
Table 10. ISSRM assets concepts modelled in SROMUC	35
Table 11. ISSRM risk treatment related-concepts modelled in SROMUC.....	36
Table 12. ISSRM risks concepts modelled in SROMUC	37
Table 13. ISSRM assets concepts modelled in Secure Tropos	39
Table 14. ISSRM risk treatment related-concepts modelled in Secure Tropos	40
Table 15. ISSRM risks concepts modelled in Secure Tropos	41
Table 16. Concept alignment of security languages with ISSRM domain model	43
Table 17. Comparison of concepts created using SRM language.....	46
Table 18. Comparison of construct using SRM languages	47
Table 19. General understanding of languages	47
Table 20. Example of managing Code breaking security risk	56
Table 21. Example of managing The Engineer Tap security risk.....	58
Table 22. Example of managing number please security risk	59
Table 23: Example of Young man on the run security risk	60
Table 24. Example of gas attack security risk.....	61
Table 25. Example of first call-Andrea Lopez security risk	62
Table 26. Example of Doyle Lonnegan’s Story security risk	63
Table 27. Example of card capture security risk.....	64
Table 28. Example of the one cent cell phone security risk.....	65
Table 29. Example of hacking into the Feds security risk	66
Table 30. Example of the networkd outage security risk.....	67
Table 31. Example of Craig Cogrune’s story security risk.....	68
Table 32. Example of Keeping up with Joneses security risk.....	69
Table 33. Example of I saw it at the movies security risk	70

Table 34. Example of Danny the Eavesdropper security risk	72
Table 35. Example of Phony sites and dangerous attachments security risk.....	72
Table 36 Example of Merry Christmas security risk	73
Table 37. Example of A visit to the Studio security risk	75
Table 38. Example of Do it now security risk	76
Table 39. Example of Mr Bigg wants it security risk	77
Table 40. Example of what the social security administration knows about you security risk	78
Table 41. Example of the police raid security risk.....	79
Table 42. Example of the art of fiendly persuasion security risk.....	81
Table 43. Example of cops aa dupes security risk	83
Table 44.Example of hacking behind bars security risk	84
Table 45. Example of speedy download security risk.....	85
Table 46.Example of Easy money security risk.....	86
Table 47. Example of the misleading caller ID security risk	87
Table 48. Example of the president of the United States is calling security risk.....	87
Table 49. Example of the invisible employee security risk	89
Table 50. Example of the helpful secretary security risk.....	90
Table 51. Example of traffic court security risk	91
Table 52. Example the Samantha's revenge security risk.....	92

List of Figures

Figure 1. Scope of the work	11
Figure 2. The OCTAVE Process (Hogganvik, 2007)	15
Figure 3. ISSRM Domain Model (Mayer, 2009)	16
Figure 4. BPMN concrete syntax (Altuhhova,2013).....	29
Figure 5. Janie Acton's Story- BPMN assets identification	30
Figure 6. Janie Acton's Story- BPMN risks identification	30
Figure 7. Janie Acton's Story- BPMN risks treatment	31
Figure 8. Asset modelling for Janie Acton's Story	34
Figure 9. Threat modelling for Janie Acton's Story	35
Figure 10. Risk treatment modelling for Janie Acton's Story	36
Figure 11. Janie Acton's Story- Secure Tropos assets identification.....	38
Figure 12. Janie Acton's Story- Secure Tropos risks identification	39
Figure 13. Janie Acton's Story- Secure Tropos risks treatment.....	40
Figure 14. Search in recycle bin - BPMN assets identification.....	93
Figure 15. Search in recycle bin - BPMN risks identification	94
Figure 16. Search in recycle bin – BPMN risk treatment	94
Figure 17. Through Internet – BPMN assets identification	95
Figure 18. Through Internet - BPMN risks identification.....	96
Figure 19. Through Internet – BPMN risk treatment.....	96
Figure 20. Through persuasion – BPMN assets identification	97
Figure 21. Through persuasion – BPMN risks identification	97
Figure 22. Through persuasion – BPMN risk treatment	98
Figure 23. Breaking through computer network – BPMN assets identification	98
Figure 24. Breaking through computer network – BPMN risks identification.....	99
Figure 25. Breaking through computer network – BPMN risk treatment.....	99
Figure 26. Search in recycle bin – misuse case assets model.....	100
Figure 27. Search in recycle bin – misuse case risk model.....	101
Figure 28. Search in recycle bin – misuse case risk treatment.....	101
Figure 29. Through Internet – misuse case assets model.....	102
Figure 30. Through Internet - misuse case risk model.....	102
Figure 31. Through Internet – misuse case risk treatment	103
Figure 32. Through persuasion – misuse case assets model	103
Figure 33. Through persuasion – misuse case risk model	104
Figure 34. Through persuasion – misuse case risk treatment	104

Figure 35. Breaking through computer network – misuse case assets model.....	105
Figure 36. Breaking through computer network – misuse case risk model	105
Figure 37. Breaking through computer network – misuse case risk treatment	106
Figure 38. Search in recycle bin – Secure Tropos asset identification	107
Figure 39. Search in recycle bin – Secure Tropos risk identification	108
Figure 40. Search in recycle bin – Secure Tropos risk treatment	108
Figure 41. Through Internet – Secure Tropos asset identificaiton.....	109
Figure 42. Through Internet – Secure Tropos risk identification.....	110
Figure 43. Through Internet – Secure Tropos risk treatment.....	110
Figure 44. Through persuasion – Secure Tropos asset identification	111
Figure 45. Through persuasion – Secure Tropos risk identification	112
Figure 46. Through persuasion – Secure Tropos risk treatment	112
Figure 47. Breaking through computer network – Seucure Tropos asset identification.....	113
Figure 48. Breaking through computer network – Secure Tropos risk identification.....	114
Figure 49. Breaking through computer network – Secure Tropos risk treatment.....	114

Abbreviations

IS Information System

ISO International Organization for Standards

SRM Security Risk Management

OCTAVE Operationally Critical Threat, Asset, and Vulnerability

ISSRM Information System Security Risk Management

COBRA Consultative, Objective and Bi-functional Risk Analysis

1 Introduction

The rapid development of information technology affected to the security of information systems. Traditional role of IS security specialist included technical competences, but in this latter days there is a need to have a mix of IT and business profile. One should also acknowledge the social engineering threats towards organization although it might not help in clarification of social engineering processes. As social engineering plays a vital role there is a need to construct such a modelling approach that will be suitable for ordinary users to comprehend those changes.

The study is centred on Social Engineering Security and Risk Management languages. Scope is summarized in Figure 1.

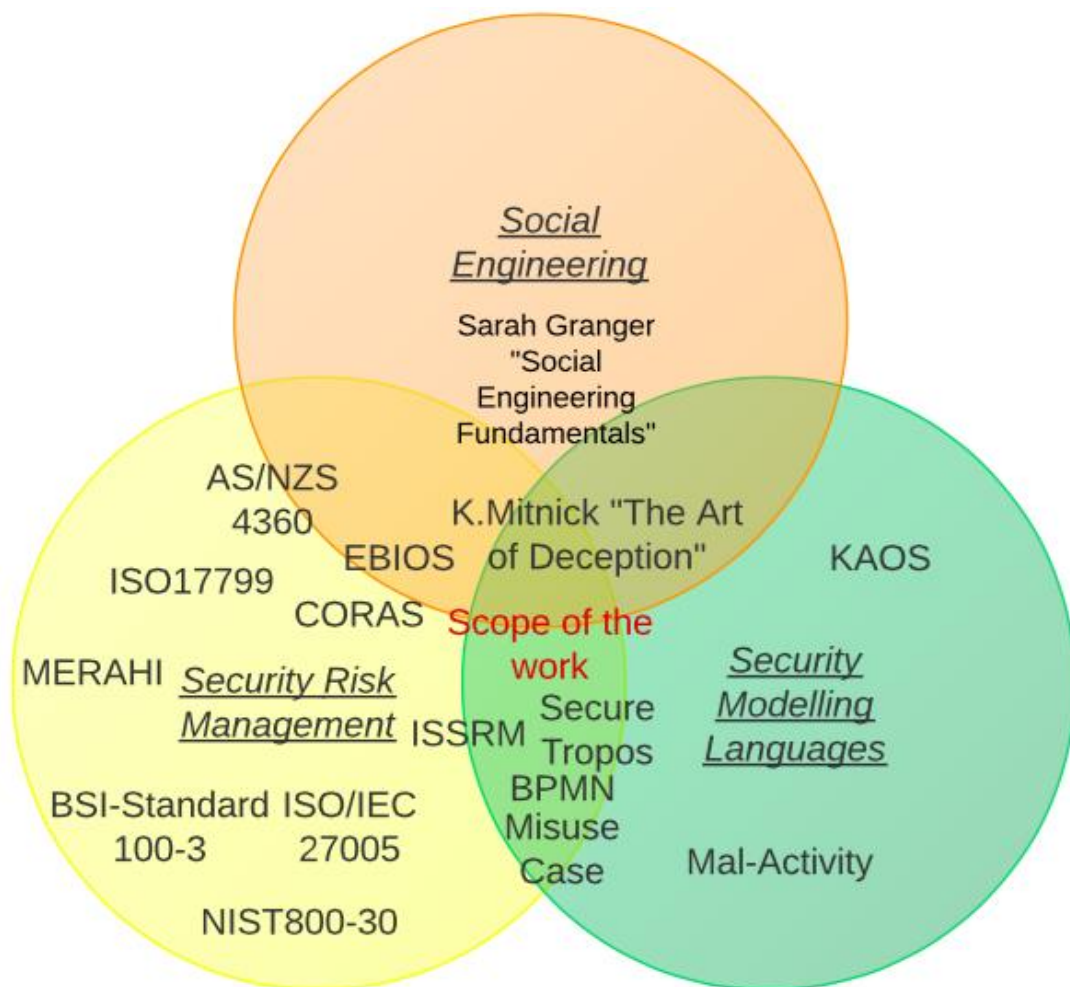


Figure 1. Scope of the work

The thesis is not concentrated only on security risk management aspects, but also takes care of social engineering aspects and existing modelling languages. Contribution aims to understand what existing modelling languages that support security risk management approach could be considered as the most understandable language for ordinary users to model Social Engineering risks.

In the thesis were overviewed security risk management standards as ISO 17799, NIST 700-30 and security risk management methods like COBRA (A. Jones, 2005), CORAS (Heidi, 2007), OCTAVE (Alberts and Dorofee, 2001) and ISSRM (Mayer, 2009). Considering the main subject area of the paper, basic introduction to social engineering was also given. As

the main aspect of the study in social engineering is psychological manipulation of people, author considered as a good foundation of the illustration a book of Kevin Mitnick “The art of deception” (D. Mitnick, 2002). Social Engineering cases were presented using three modelling languages: BPMN (Altuhhova, 2013), Secure Tropos (Matulevičius et al., 2008b), Misuse case (Soomro, 2012).

More specifically, the research question is *what modelling approach is most suitable for social engineering analysis?* To provide necessary analyses, there is a need to investigate existing languages and compare them with concept needs. In order to identify the understanding of participants to each considered modelling language, we have prepared a questionnaire. This helped to collect data with obtained results.

All above mentioned research process has led us to the result that overall BPMN constructs and Secure Tropos concepts are preferred by users. Also based on collected results, we tried to make a parallel between understanding of concepts and constructs for participants. Percentage wise understanding of constructs showed higher results than concepts. Business asset, IS asset, threat, attack method, risk treatment, security requirement and control are easily identified in the form of constructs. Concepts are have received higher score in following aspects: Business Asset, Security criterion, Impact, Event, Vulnerability, Threat, Threat agent, Security requirement.

Thus this thesis is organised in six chapter. Chapter 2 provides outline of existing security risk management standards and method, such as ISSRM domain model which has been studied in more details. Chapter 3 presents an overview of different type’s methods of social engineering attack and their alignment of ISSRM domain model. Chapter 4 introduces several modelling languages: BPMN, Misuse case, Secure Tropos and alignment of each language to ISSRM domain model with application to a studied case. Chapter 5 is about provided research and results of collected data. Chapter 6 summaries the major findings and deliberated future work.

The document ends with the list of references that were used. Finally Appendix section presents some research material that were excluded from the main thesis. It starts with Social Engineering Cases that collects all identified cases from the book of Kevin Mitnick “The art of deception”. To each of the case constructed table, which represents alignment of ISSRM domain model. Next section Social Engineering Examples in BPMN which has rest of cases that were divided based on Granger’s division of social engineering attacks and applied BPMN modelling language. After that Social Engineering Examples in Misuse Case and Social Engineering Examples in Secure Tropos. Moreover Questionnaire of BPMN, Questionnaire of Misuse Case and Questionnaire of Secure Tropos were included to the appendix list. Lastly, all collected data upon BPMN, Misuse case and Secure Tropos concepts & constructs were presented in last three sections.

2 Approaches for Security Risk Management

History has proven that stability, no matter how perfect it may be leading to degradation. Development is not possible without a risk. The same notion is applies to information technology. Its rapid development has affected the formation of security management methods and standards.

This chapter covers main security risk management risk management standards such as ISO 17799 (ISO/IEC 17799:2000), NIST 800-30 (G. Stoneburner, 2004) and security risk management methods like COBRA (A. Jones, 2005), CORAS (Heidi, 2007), OCTAVE (Alberts and Dorofee, 2003) and ISSRM (Mayer, 2009). During the studying process, we is explaining only selected ISSRM domain model is selected.

Section 2.1 which provides an overview of security risk management. Overview of different security risk management standards is presented in Section 2.2. Section 2.3 overview of security risk management methodologies like CORAS (Heidi, 2007), OCTAVE (Alberts and Dorofee, 2003), and ISSRM (Mayer, 2009). This chapter ends with Section 2.4 which outlines research study and makes a comparison of security risk management standards and methodologies.

2.1 Security Risk Management

Security risk management (SRM) is an extended process of analyzing and listing Information System's (IS) security risks and employing controls (i.e., countermeasures, safeguards) that address those risks (e.g., Albert and Dorofee 2003, ISO/IEC 2000; ITGI 2005; NIST 2004). It is getting increasingly important to every organization that has aimed to effectively manage information security issues. Customers in every business organization realizes the importance of confidentiality of their personal and business data. Investors from their side need to be confident, that the business and information assets are protected. Business partners expect that the company will operate without any failure which can be caused by error in information system, intentional or unintentional actions of staff, malicious software and other factors (Wozniak, 2004).

To avoid those uncertainties in organizational environment, some steps have to process for security risk management (Jenkins, 1998): recognition of assets; value position to each asset; identification of vulnerability to each asset; calculation of risk for identifying asset; mitigation of identifying risks and selection of remedy. Various approaches, techniques, methods and standards exist to manage risks. Besides several approaches, there are also standards that describe the risk management process and serve as quite for them.

2.2 Different Risk Management Standards

There is a number of information risk management standards as ISO 15408 (J. Wiley, 2006), ISO 17799 (M. Kaufman, 2009), and BSI (BSI Standard, 2005); as well as national standards NIST 80030 (G. Stoneburner, 2004), SAC (Z.Qian, 2012), COSO (J. Wiley, 2006), SAS 55/78 (M. Kaufman, 2009) and some other similar to them. These information risk management techniques involve following steps (Moffett, 2003):

- define the main goals and objectives to the protection of information assets;
- support the creation of an effective system of assessment and information risk management;
- help with the calculation of a set of detailed not only qualitative but also quantitative risk assessments, adequate stated business objectives;

- use special tools for assessments and risk management.

In this paper different standards focus on various aspects. For example, ISO (ISO27001, 2005) is the International Organization for Standardization that develops and publishes international standards. In ISO/IEC 17799 Information Technology - Security Techniques - Code of Practice for Information Security Management (ISO 17799) combines best practices and brings together information security, intellectual property rights, protection and audit controls.

Another example is NIST 800-30 (Mayer, 2009) The National Institute of Standards and Technology developed the standard NIST SP 800-30. It includes recommended guidelines for securing IT infrastructure from a technical perspective. NIST SP 800-30 is a well-accepted standard for risk assessment.

2.3 Security Risk Management Methodologies

Security Risk Management includes different strategies, policies, activities, roles, procedures and people that manage those risks. The aim is to have a system of controls that collectively guarantee protect IS security. As an example will be mentioned three methods: CORAS (Heidi, 2007), OCTAVE (Hogganvik, 2007), ISSRM (Mayer, 2009):

- Their history and background will look into these models following;
- Main steps for risk management approach;
- Purpose of the approach.

2.3.1 CORAS

CORAS method is a traditional security analysis technique combined with the system development approach such as the UML. From 1999-2003 method was developed in the EU funded CORAS project (Heidi, 2007). The aim of the project was to gather risk analysis techniques into an integrated security risk analysis method. It was called CORAS security analysis. The intent of it was to apply several risk analysis techniques in a mixed and easier manner.

The CORAS modelling technique has three main purposes (Stolen, 2003):

- i. to describe the target of assessment;
- ii. to support communication and integration between different groups of stakeholders involved in risk assessment;
- iii. To document risk assessment results and the assumption on which results depend.

CORAS method takes into account several international standards for risk management like Australian/New Zealand Standard for Risk Management (K. Roebuck, 2012), the ISO/IEC 13335 (J. Kouns, 2011) Guidelines for the management (J. Kouns, 2011) of IT-Security and the system documentation in the form of the Reference model for open distributed processing.

CORAS is structured in five stages: (1) context establishment, (2) risk identification, (3) risk estimation, (4) risk evaluation and (5) treatment identification (Braber et al., 2007).

To sum up this method over others, below outlined several advantages (Folker et al., 2007):

- It has a precise description of the target system and presents all relevant security features in accessible format;

- It uses the graphical representation which improves communication and interaction between parties involved in the analysis;
- It facilitates documentation of risk assessment results and the assumptions on which these results depend.

2.3.2 OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) technique appeared in the USA in the Software Engineering Institute of the Carnegie Mellon University. It has been published in 2001. Despite old version of other methods, it remains actual and relevant. The main interesting part of OCTAVE is a brainstorming method to investigate risks.

OCTAVE is used to assess an organization's information security needs. This is based on three phased approach. It helps to examine organizational and technological issues with a wider picture of the current situation in organization's information security needs (Hogganvik, 2007).

The main steps of this approach are presented in Figure 2. The aim of this method firstly is to study organizational and technological issues. Secondly it defines security strategy of an organization. The major steps are:

1. identifying critical assets and threats to them;
2. identifying the vulnerabilities, both organizational and technological, that expose those threats, creating risk to the organization;
3. Developing a practice-based protection strategy and risk mitigation plan to support the organization's missing and priorities.

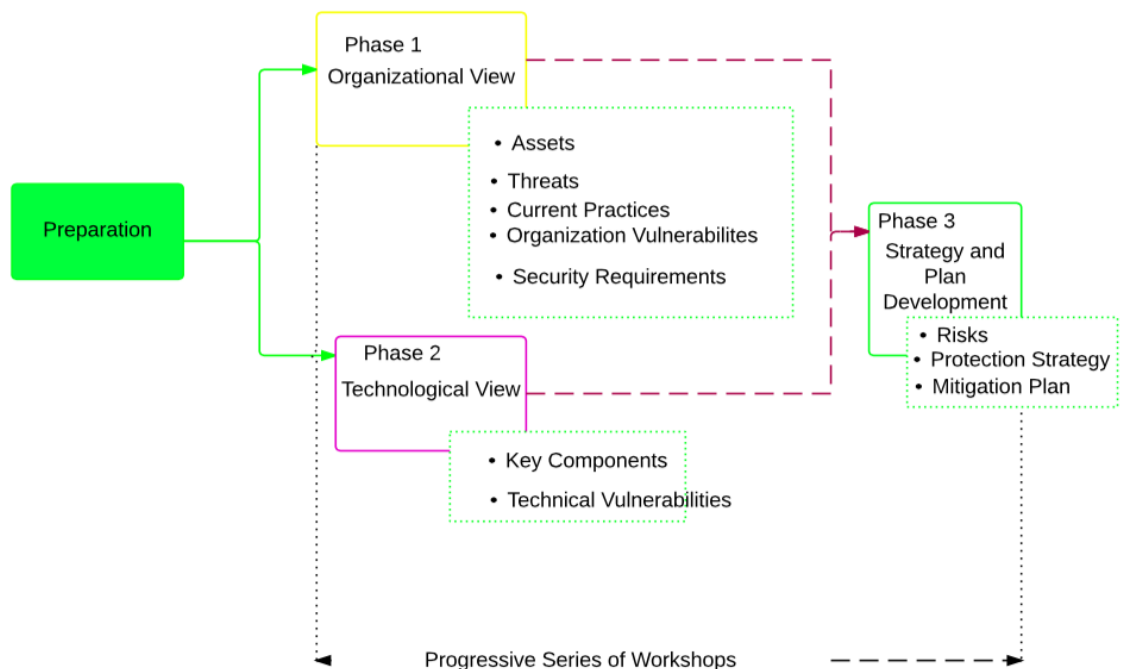


Figure 2. The OCTAVE Process (Hogganvik, 2007)

2.3.3 Domain Model of ISSRM

Information System Security Risk Management (ISSRM) method is a family of previous mentioned CORAS method (Mayer, 2009). The aim of this approach is to ensure the protection of an IS by defining security requirement and implementing the appropriate risk management solution. ISSRM's aim is to maximize the security level that an organization wants to achieve (AS/NZS 4360, 2004).

The process is followed by classical and common steps as (Stoneburner, 2002): context and asset identification, determination of security objectives, risk analysis and assessment, risk treatment, the security requirements definition, control selection and implementation. ISSRM process can be summarized in one activity form of a UML diagram.

This process model should be regularly performed by organization to keep business competitive and ensure security level. The ISSRM domain model illustrated in Fig. 2 considers three groups of concepts: (1) asset-related concepts, (2) *risk-related concepts* and (3) *risk-treatment related concepts*.

Asset-related concepts are used to describe assets of the organization that needs to be secured. *Asset* has an aim to support organization on a daily processes and distinguish security criteria. *Business asset* is valued information or process that assists in achievement of objectives that organization has. IS asset is a part of supported business asset in IS. *Security criterion* includes confidentiality integrity and availability of business asset (Matulevičius et al, 2008).

Risk related concepts represent risks itself and their components: *Risk* is a combination of a threat with one or several vulnerabilities that lead to negative impact to assets. *Impact* is the direct effect of risks when the threat (or an event) is accomplished, that may harm assets of the system or an organization. The *Event* is the combination of a threat and vulnerabilities. *Vulnerability* is a characteristic or group of IS assets that establish weakness or flat of IS security. *Threat agent* is an agent, who might cause a harm to the assets of the IS. *Attack method* is a method used by a threat agent who performs a threat (Matulevičius et al., 2008).

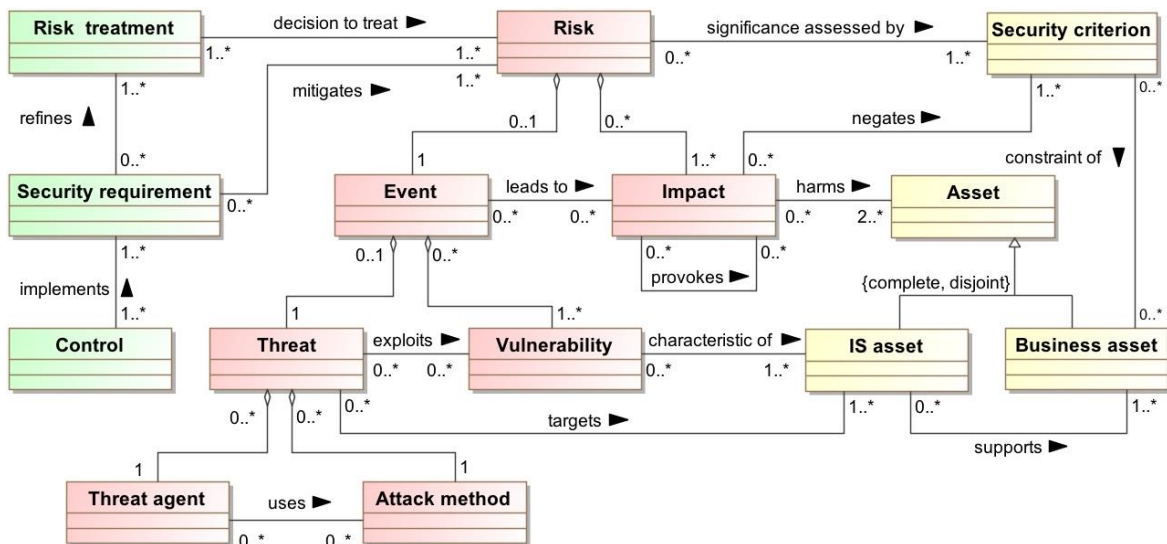


Figure 3. ISSRM Domain Model (Mayer, 2009)

Risk treatment — rafted concepts characterises what decisions, requirements and controls should be implemented to mitigate possible risks. In order to achieve this concepts aim, need to pursue following steps: *Risk treatment* is the decision of dealing for potential risks, like: avoiding, reducing, transferring and retaining. *Security requirement* is a step of

countermeasures that are identified to mitigate potential risks. *Control* countermeasures to improve security which are specified by security requirements (Matulevičius et al, 2008).

2.4 Summary

There are various approaches and standards related to security risk management. To identify the most suitable security risk management method that aligns with different modelling approaches for a further analysis, author made a Table 1. It represents different standards and methods which were reviewed before. Based on mentioned steps to processed security risk management, author decided to review mentioned standards and methods from perception of these different steps.

Table 1 shows that each method has its own strengths and weaknesses. For example CORAS risk management method can combine different methods of analysis, but this could be counted as a shortcoming because it is a time consuming and the process of application of inexperienced user is problematic. Taking into account that OCTAVE and CORAS approaches are quite similar, both of them will not be considered as a most suitable modelling approaches for a further study. If analyze ISO 17799, there is a lack of measurement precision of a technical standard and it is not as entire as other methods. NIST 800-30 has an inaccurate results in case of calculation of risk occurrence, which at the end might lead to totally diverse results. In this case ISSRM can be applied with different modelling approaches, but at the same time it has an unfavorable aspect as it might be difficult to determine a suitable approach.

All mentioned standards and methods deliver security orientation and risk-based approach. However, if we take a look to the application of methods to model-based approaches only CORAS and ISSRM provide some level of granularity. CORAS has a disconnection for standard terminology, therefore ISSRM domain model has been chosen for further application. ISSRM domain model will be applied to identify assets and risks, select security requirements and mitigation of risks to provided cases. The main advantage of ISSRM domain model is its alignment with Misuse cases (Soomro, 2012), Secure Tropos (Matulevičius et al., 2008b) and BPMN (Altuhhova, 2013).

Table 1. Comparison of modelling approaches

Risk Management Approach/Method	ISO 17799	NIST 800-30	CORAS	OCTAVE	ISSRM
Identification of assets	Asset management	Characteristics of the system	Refining the target description using asset diagrams	Identifying operational area management knowledge	Content and asset identification
Value assignment to each asset	Access control, communications and operations management, physical and environmental security	Definition of probability exploits	Approval of target description	Identifying stuff knowledge	Determination of security objectives
Identification of vulnerability to each asset	Physical and environmental security, human resources security	Identification of threats, vulnerabilities	Risk identification using threat diagrams	Create thread profile	Risk Analysis and assessment
Calculation of risk for identified asset	Information systems acquisition, development and maintenance	Identification of risks	Risk evaluation using risk diagrams	Conduct risk analysis	Risk Analysis and assessment
Mitigation of identified risks and selection	Information security incident management, business continuity management	Recommendations on measures of protection	Risk treatment diagrams	Development protection strategy and mitigation plan	Risk treatment, security requirements definition

3 Social Engineering

3.1 Role of Social Engineering

Today, the human factor in information security plays an important role (Thompson, 2006). Many companies who think that the problem of information security can be solved simply by using hardware and software, are mistaken. Security controls such as firewalls, device identification, encryption, Intrusion Detection System are ineffective in countering hackers using social engineering techniques. Evidently, there is a need of a strong staff development, its training and the use of security policies in confrontation techniques against social engineers. Thereby an integration of all mentioned above methods is a need to guarantee the system's security (Ibrahiem, 2013).

One of the hackers techniques, which uses weak spots based on the human nature called social engineering (Adam, 1996). This technique helps hackers to get information that is necessary to break through the secured system. The goal of social engineering is to trick the victim in order to obtain certain information or to force to act in a certain way (Rahul, 2013).

In order to obtain information, there are many methods that could be used. Some of the attack types are as follows (Granger, 2001):

- *Via telephone.* The attacker might put himself in the position of a victim and ask for an assistance or help. As people tend to pity those who are facing difficulty, the success of the attack is rather high. This method helps to obtain information directly from people, who are inside of the organization.
- *Search in the recycle bin.* This includes neglecting vital documents and placing them in the trash bin.
- *Through internet.* Using this method attacker searches password, as people tend to reuse the single password when entering to different systems. If an attacker gets one password, then it is easier to get to different accounts belonging to the same person. An attacker might send an email to the victim to assure the identity and search for all important information, which person will provide by updating it.
- *Through persuasion.* This technique is concentrated on the psychological side. The aim is to prepare an ideal psychological situation to get targeted information.
- *Breaking through a computer network.* Attacker breakthrough computer network in order to gain a trust from the user and force him to provide information of the organization.

The most vulnerable to social engineering attack are new employees. As a rule, they have not been able to talk about all the existing corporate rules, they did not examine the information security regulations (Christopher, 2011). Beginners do not yet know all their colleagues, especially in person. In addition, they are characterized by increased trust and willingness to help, in order to establish themselves as an active and responsive team member, on which organization could rely. They are unlikely to be interested in the rights of access of a social engineer who is impersonating another member, especially a superior (Rajendra, 2013).

Even the most vigilant employees are not always able to recognize the social engineering attack. Naturally, man should not act as a lie detector. A key success factor to the company is appropriate training. Security policies must enter into the flesh and blood of everyone

who works in the company. Employees need to know, that they might be attacked if their customer (Wozniak, 2004):

- i. increased interest to them,
- ii. exaggerated care and attention
- iii. refuses to give his coordinates
- iv. appeals with a strange or unusual request ,
- v. trying to insinuate in confidence, or flatters
- vi. speaks to emphasize the authoritative tone.

Certainly every organization has to develop those policies, before it crams employees with these policies. There are common defenses that might take a place (Mitnick K., 2002): show identity when try to enter to the building; password over the phone; use of technology ID; passwords are not left lying around.

To protect its organization from social engineering attacks employer has to understand the need to provide training programs for all categories of workers. All preventive measures and actions have to be taken in order to prevent exposure of vital information (Christopher, 2011). There should be policies and procedures to cover necessary security regulations: regulating helpdesk procedures, access privileges, others. These methods help to employees to be aware of social engineering attack. Through seminars workers can be aware on how to be more careful on what type of information they are providing and what they are throwing to trash. They will understand the value of information and immediately report to security personnel in case of any strange case.

3.2 Examples of Social Engineering Attacks

This section describes some cases that were taken from the book of Kevin D. Mitnick “The Art of deception”. Each case has been carved based on Granger’s division of social engineering attacks. We examine each case following the ISSRM principles.

The research method is done using the concept alignment of ISSRM domain model. It was represented in Figure 3. For each event shown in that table exist mutual events. To make those concepts presented in a table form shorted, some of those events are skipped. For example: threat agent and attack method together produce a threat. It is missing in the table as a threat agent and attack method are identified. Also threat and vulnerability represent an event that occurred in specific cases. Based on that term event is also not shows in the table. The same concept is used to asset. It is a representation of IS asset and Business asset. The reader should note that when analyzing and studying presented tables.

3.2.1 Example of Social Engineering Attack Via Telephone

Content identification: Jenny Acton is an employee, who worked in «Hometown Electric Power» more than three years at the service of customers. Once she received a call. The caller said, that he has damaged his computer by virus. In consequence of this he cannot get information to one of the vice-presidents. Caller asked to see from the system (CBIS) account number, phone number entry and service address. Then said goodbye and hung up.

Risk analysis. As presented in Table 2 in this context we identify the business asset as all the information requested by the caller. The risk is defined as follows: The caller, who knows CBIS and structure of organization and how to use the phone.

Risk-treatment concept: in order to mitigate and avoid potential risks Jenny needed verify that caller is an employee. She has to realize that some of the information might be publicly accessible and some information of her department is sensitive. From the organization's perspective it might be good to regularly organize security trainings to their employees (such as Jenny).

Table 2. Example of managing Via phone securityrisk

Business asset	Account number on CBIS, information on CBIS about is the account number current, service address, phone number.
IS asset	Customer Billing Information System, Jenny.
Security criterion	Confidentiality of information on CBIS about is the account number current, confidentiality of account number on CBIS, confidentiality of information on CBIS.
Impact	Negation of authentication of the caller, Jenny is not trusted.
Vulnerability	Jenny is not experienced to verify the caller.
Threat agent	Caller (attacker): knows how to use phone, knows CBIS, structure of organization.
Attack method	The caller said that he has damaged his computer by virus. In consequence of this he cannot get information to one of the vice-presidents. Caller collected data thorough search to confirm his authenticity. Caller asked to see from the system account number, phone number entry and service address.

3.2.2 Example of Social Engineering Attack Through Search in Recycle Bin

Content identification: The guy named Steve, called to a small central office telephone company building, which runs telephone lines to all homes and businesses in the service area. On duty switchman answered to the call. Steve said that he is from divisions of the company that publishes and distributes printed materials. He has a new version of Test Numbered Directory, but for security reasons we cannot give a copy to the switchman until he got old one. It seems reasonable to unsuspecting switchman. He did as he was asked, placed on the verge of building. Steve arrived and carefully looked around in search of the police or security staff of the company, which could hide behind trees, or wait for him in a parked car. There was no one on sight. He casually took directory and left.

Risk analysis. As presented in Table 3 in this context we identify the business asset as all information that is stored in Test Numbered Directory. The risk is identified as follows: Steve knows how to use the phone, also knows about Test Numbered Directory and who has the original Test Numbered Directory.

Risk-treatment concept: in order to mitigate and avoid potential risks Switchman needed to verify from his colleagues that there has been issued a new version of Test Numbered Directory and to ask from security specialist is there mentioned something about exchange of published and printed out materials copies in security policy. From the organisation's perspective it might be good to regularly organize security trainings to their employees.

3.2.3 Example of Social Engineering Attack Through Internet

Following one is through Internet which is also identified in the case of Graduating without Honors.

Table 3. Example of managing Stevie's scam security risk

Business asset	Test Numbered Directory
IS asset	Switchman on duty
Security criterion	Confidentiality of the information on Test Numbered Directory
Impact	Negation of authentication of a caller, switchman is not trusted
Vulnerability	Switchman is not experienced to verify the caller
Threat agent	Steve knows how to use the phone, knows who has the original Test Numbered Directory, knows about Test Numbered Directory
Attack method	Steve called to the small central office telephone company building and said that for security reasons he cannot give employees copy until he gets old one.

Content identification: Michael Parker decided to see if he could "create" his own accelerated bachelor's degree in computer science by searching for a graduate with the same name as his, who had earned a computer science degree any time during an appropriate span of years. If so, he could just put down the other Michael Parker's social security number on employment application forms; any company that checked the name and social security number with the university would be told that, yes, he did have the claimed degree. To achieve his goal first of all he went to the main library on the university campus, he sat down at a computer terminal, got up on the Internet, and accessed the university's Web site. Then he called the Registrar's office. The answer, admin.rnu.edu, gave him the name of the computer where student records were stored. This was the first piece of the puzzle: He now knew his target machine. He typed that URL into the computer and got no response--as expected, there was a firewall blocking access. So he ran a program to see if he could connect to any of the services running on that computer, and found an open port with a Telnet service running, which allows one computer to connect remotely to another computer and access it as if directly connected using a dumb terminal. All he would need to gain access would be the standard user ID and password. He made another call to the registrar's office, this time listening carefully to make sure he was talking to a different person. He got a lady, and again he claimed to be from the university's Computer Center. He told that they were installing a new production system for administrative records, he told her. As a favor, he'd like her to connect to the new system, which still is in test mode, to see if she could access student academic records. He gave her the IP address to connect to and talked her through the process. In fact, the IP address took her to the computer Michael was sitting at in the campus library. He had created a login simulator--a decoy sign in screen--looking just like the one she was accustomed to seeing when going onto the system for student records. She told to attacker that on screen is error message: Login incorrect. By now, the login simulator had fed the keystrokes of her account name and password to Michael's terminal; mission accomplished. He told her that he will set up your account, and call her back. Now Michael knew what computer system he needed to access and he had a user's ID and password. First step in clearing this last hurdle: Find out who could guide him through the mysteries of searching the student database. He called the Registrar's office again, this time reaching a different person. Minutes later he was on the phone with the college's database administrator, pulling the sympathy act. By the time they hung up, Michael had downloaded the entire list of computer science graduates for those years. Within a few minutes he had run a search, located two Michael Parkers, chosen one of them, and obtained the guy's social security number as well as other pertinent information stored in the database. He had just become "Michael Parker, B.S. in Computer Science, graduated with honors, 1998." In this case, the "B.S." was uniquely appropriate.

Table 4. Example of managing Graduating without Honor's case security risk

Business asset	University record about students, student name, social security number, graduation grades
IS asset	Login, password, Registration office, database, library, administration office, firewall, telnet service, dump terminal
Security criterion	Confidentiality of university records about students
Impact	Loss of username and password, loss of university record of a student
Vulnerability	Open telnet and the college's database administrator, pulling the sympathy act to Michael Parker
Threat agent	Michael Parker: has an access to the university campus library, has an access to the computer terminal, knows how to use phone, has a knowledge in networking, has a knowledge in creation of log simulator.
Attack method	<p>Going to the main library on the university campus, he sat down at a computer terminal, got up on the Internet, and accessed the university's Web site.</p> <p>Then he called the Registrar's office.</p> <p>The answer, admin.rnu.edu, gave him the name of the computer where student records were stored.</p> <p>He typed that URL into the computer and got no response--as expected, there was a firewall blocking access. So he ran a program to see if he could connect to any of the services running on that computer, and found an open port with a Telnet service running, which allows one computer to connect remotely to another computer and access it as if directly connected using a dumb terminal.</p> <p>He made another call to the registrar's office, this time listening carefully to make sure he was talking to a different person. He got a lady, and again he claimed to be from the university's Computer Center.</p> <p>He gave her the IP address to connect to, and talked her through the process. In fact, the IP address took her to the computer Michael was sitting at in the campus library.</p> <p>He had created a login simulator--a decoy sign-in screen--looking just like the one she was accustomed to seeing when going onto the system for student records. "It's not working," she told him. "It keeps saying 'Login incorrect. By now the login simulator had fed the keystrokes of her account name and password to Michael's terminal; mission accomplished. He told her, "Oh, some of the accounts haven't been brought over yet to this machine. Let me set up your account, and I'll call you back".</p> <p>Now Michael knew what computer system he needed to access, and he had a user's ID and password.</p> <p>He called the Registrar's office again, this time reaching a different person. Minutes later he was on the phone with the college's database administrator, pulling the sympathy act. By the time they hung up, Michael had downloaded the entire list of computer science graduates for those years.</p>

Risk analysis. As presented in Table 4 in this context we identify the business as university record about students; their name, social security number and graduation grades. The risk is

defined as follows: Michael Parker has an access to the university campus library, to the computer terminal and has a knowledge in networking with a creation of log simulator.

Risk-treatment concept: in order to mitigate and avoid potential risks all employees who are able to access any sensitive information have to know the importance of sensitive information. Maintain a list of people who have been specially trained in the procedures and who are trusted to authorize sending out sensitive information. Require that only these people be allowed to send information to anyone outside the workgroup. From the corporate perspective, there is a fundamental need for good training. But there is also a need for something else: a variety of ways to remind people of what they've learned.

3.2.4 Example of Social Engineering Attack Through Persuasion

The case mentioned in the book “Art of Deception” and reflecting social engineering attack through persuasion is Steve Cramer’s Story.

Content identification: Steve worked on the creation of new devices for GeminiMed Medical Products which worked on a new product called STH-100. On Saturday morning called Ramon Perez from tech support. He reported that three of the servers are not working and that tech specialist has to reinstall the drivers and restore all of the files. Since it was completely unacceptable for Steve and he wanted as quickly as possible to finish its work and not wait a few days, he began to push the technical department of the person to do his computer as soon as possible. For this, the caller started asking what server he uses, but the man from technical department said that he will also need a username and password. This issue has caused suspicion and he asked the chief of the name and surname of the person who called. The caller said that he could see what was written on the piece of filled paper in hiring time. He called the password "Janice". Thereby earning the trust of Steve said his ID and password. The caller asked for a couple of hours to restore the files. Steve graduated with a lawn, ate, and when he got to the computer, he found that his files were actually recovered.

Risk analysis. As presented in Table 5 in this context we identify the business as all files that are stored in computer servers with an information of STH-100. The risk is defined as follows: Ramon Perez has a phone number of employee, knows the structure of organization, has an access to old information of employee, knows how to use cell phone and how obtain trust of employee.

Risk-treatment concept: in order to mitigate and avoid potential risks Steve needed to verify that person who called is from technical support. From the organization’s perspective it might be good to regularly organize security trainings to their employees.

3.2.5 Example of Social Engineering Attack Breaking Through Computer Network

The last one is breaking through computer network which is considered in situation of the dictionary as an attack tool.

Content identification: Ivan Peters had a target of retrieving the source code for a new electronic game. After finding an un-patched vulnerability in the Web server software, his buddy had just about fallen out of his chair when he realized the system had been set up as a dual-homed host, which meant he had an entry point into the internal network. Instead of using a technical approach to finding out what server he needed to target, Ivan used a social engineering approach. He placed phone calls based on methods similar to those described

elsewhere in this book. First, calling IT technical support, he claimed to be a company employee having an interface issue on a product his group was designing and asked for the phone number of the project leader for the gaming development team..

Table 5. Example of managing Steve Cramer's story security risk

Business asset	All files, drivers, computer servers, STH-100
IS asset	Computer servers RM22 and GM16, username (ID), password
Security criterion	Confidentiality of username(ID) and password
Impact	Steve is not trusted, negation of authentication process
Event	Steve received a call from Ramon Perez from tech support with an information that three of the servers are not working and they'll need some time to reinstall the driver and restore all of their files. To have an access to his information as soon as possible Steven asked from tech support to deal with it urgently. Ramon Perez was pleased to help, but in order to help he needed to ask some verification questions.
Vulnerability	Steve is not experienced to verify the caller
Threat agent	Ramon Perez from tech support who knows how to use cellphone, who has a phone number of employee, who knows the structure of organization, who received an access to old information of employee and thanks to that gained a trust.
Attack method	Roman Perez did some research in advance to sound authentic Called to Steve and introduced himself as an employee from technical support, with a ready to help

Then he called the name he'd been given, posing as a guy from IT. He just gave the name of the servers, ATM5 and ATM6. At this point, Ivan switched to a technical approach to get the authentication information. The first step with most technical attacks on systems that provide remote access capability is to identify an account with a weak password, which provides an initial entry point into the system. While this attack was running, Ivan started another computer running a similar attack on the other server used by the development group, ATM6. He still had not been able to get a password for an account on the ATM5 machine. Using his hacker mindset, understanding the poor security habits of typical users, he figured one of the team members might have chosen the same password for both machines. In fact, that's exactly what he found. One of the team members was using the password "garners" on both ATM5 and ATM6. The door had swung wide open for Ivan to hunt around until he found the programs he was after.

Risk analysis. As presented in Table 6 in this context we identify the business as the source code for a new electronic game and web server software. The risk is defined as follows: Ivan Peters: has a good knowledge in finding vulnerabilities in software, also on how to make a technical attack and find out a password and about basic structure of an organization.

Risk-treatment concept: in order to mitigate and avoid potential risks employee shouldn't speak valuable information of the organization and do no use easy passwords. Preventing this kind of attack typically involves taking steps on both human and technical levels. Organization has to deploy all possible countermeasures of protection. Security policies should discourage deviation from procedure through a system of rewards and consequences. Naturally, the policies must be realistic, not calling on employees to carry out steps so burdensome that they are likely to be ignored.

Table 6. Example of managing The dictionary as an attack tool security risk

Business asset	The source code for a new electronic game, web server software
IS asset	Internal network (set up as dual-home host), IT technical support, project leader
Security criterion	Confidentiality of source code for a new electronic game program
Impact	Ivan: employees negated authentication process, IT technical support and project leader are not trusted
Vulnerability	Same password was used in servers ATM5 and ATM6, unpatched vulnerability in the Web-Server software
Threat agent	Ivan Peters: has a good knowledge in finding vulnerabilities in software, has a knowledge about basic structure of an organization, has a knowledge on how to make a technical attack and find out a password
Attack method	Noticed un-patched vulnerability in the Web-Server software Called to IT technical support, claims to be a company employee, asks phone number of project leader Called to project leader as a guy from IT and received name of servers Made a technical attacks on systems that provide remote access capability to identify weak password When he was not able to find a password to ATM5, he figured out that some member might have chosen the same password for both machines and did further research in that area.

3.3 Summary

In this Chapter, we have covered the role of social engineering and some examples of social engineering attacks with application to ISSRM domain model. First, we presented the role of social engineering. Second, an overview of some chosen cases with constructed ISSRM domain model. Based on conducted study, we decided to select only one provided example. It will be included in a further research of this paper. The chosen case is “Via telephone”. Others are also applied to the research, but are moved to Appendix. We ended this chapter by conclusion with regard of a further research.

In the next chapter, we start out introduction of ISSRM domain model’s alignment with Misuse case, BPMN and Secure Tropos. We introduce each modelling language and present its application to the chosen case. This applied concept presents an integration in an ISSRM modelling language.

4 Security Modelling Languages

Indubitably information system (IS) plays an important role in security of sensitive contexts. Albeit subsisting security modelling languages provide some designates to model security aspects, they do not contain concrete constructs to address vulnerably susceptible system assets, their risks and risk treatments (Matulevičius et al., 2012). Furthermore, security languages do not provide a crosscutting viewpoint relating all three together. Security analyst faces difficulties in detection of potential security imperfections. This situation advocates to review existing security-oriented modelling languages and their usage with security risk management (Matulevičius *et al.*, 2012). It is important to consider several modelling languages as Secure Tropos (Matulevičius et al., 2008b), BPMN (Altuhhova, 2013), Mal-activities (G. Sindre, REFSQ 2007), Misuse case (Soomro, 2012).

4.1 Overview of Security Modelling Languages

The Secure Tropos (Mouratidis, 2005) methodology is established on the basic elements of Tropos (Breasciani *et al.*, 2004). Fundamental points of this approach are: analyzing social issued of security in its early stage, security treated with other requirements of the system and security is introduced during the system design phases. These constraints are confidentiality, integrity availability of some goal, soft-goal or resource. Also Secure Tropos helps to identify who is the threat agent, which invasion method can be used and which counter-measures should be implemented.

Mal-activities are extension of UML (G. Sindre, REFSQ 2007) Activity diagrams. The violator's role is represented in a changed swim lane and shows the exploits of the system to achieve some gain or harm the assets. The main purpose of this modelling language is to reveal all possible threats of the system and to come up with security solutions.

Business Process Model and Notation (BPMN) is a standard for business process modelling (Altuhhova et al., 2012) that provides a graphical notation for designating business processes in a Business Process Diagram (BPD). BPMN is a part of IS development, as it avails to designate standard and optimized workflows of the organization (Cherdantseva, 2012). The primary purpose of BPMN is modelling of the business processes for both technical users and business users, by providing a notation that is intuitive to business users, yet able to represent intricate process semantics. BPMN acts as a bridge between business process design and implementation (Rodríguez, 2007).

Misuse Case is an extension of existing standard UML use case (Mayer, N., 2007). This language has to be implemented at the early stage of software system development. A Misuse Case highlights something that should not transpire (i.e. a Negative Scenario) and the threats. Also Misuse case has an extension with a concept of vulnerability and definition of security use cases (Pauli, 2005).

Taking into account the large amount of secure-oriented modelling languages this paper will study only BPMN, Misuse cases, Secure Tropos. Approach is based on identification of that language and to each of them is used only one running example to show alignment with ISSRM domain model. (Other cases which were presented in Chapter 3 will be considered in Appendix). The alignment is focused on concepts definition and relationship between them.

After all the objective is to present different modelling languages and show their alignment with ISSRM domain model. The goal of later subsections is to present how these languages can be used to model ISSRM concepts.

4.2 BPMN

The Business Process Model and Notation (BPMN) is a standard for modelling business processes and network services. It was released in May 2004. The primary goal of the BPMN standard was drawing up the deadlines understandable to all business users, from analysis's that create the initial project till the process developers who are responsible for implementation of technology. Over all other aspects of BPMN modelling besides business processes is out of its focus (Altuhhova *et al.*, 2012).

As a matter of fact to describe BPMN processes there are used block diagrams with standard elements. Its specification provides the ability to bind set elements of the schemes for the design and implementation of the executable programming languages. BPMN modelling can be used in three different levels (Silver, 2009). They are analytical, executable and descriptive modelling. In this section, discussion will be concentrated on descriptive modelling. Its main constructs are listed in Figure 4.

4.2.1 Alignment of BPMN to ISSRM Domain Model

Generally BPMN notations are known to follow business processes and their limits concern security management of enterprise's processes. This is a quandary, as business processes and security should be followed in parallel to fortify a development of the security information systems. The foregoing discussion implies that future part of the work is concentrated on BPMN extensions for security risk management predicted on the BPMN alignment to the ISSRM concepts.

Asset-related concepts. Altuhhova *et al* (2012) detected that such as task, gateway, and event especially sequence flow is used to describe ISSRM business assets. The container constructs are aligned to the ISSRM information system assets. ISSRM business asset represents BPMN data object and ISSRM IS asset defines BPMN data store.

Risk-related concepts. BPMN doesn't involve the direct means to model security risks, but might be used to model the negative and harmful processes (Altuhhova *et al.*, 2012). On this bases BPMN pool represents ISSRM threat agent. BPMN tasks, flow and data association flow show threat agent what is treated as ISSRM attack method. Exact BPMN construct to model the ISSRM risk, impact, event or vulnerability is missing. Essentially those ISSRM concepts can be locally analyzed from BPMN model.

Risk treatment-related concepts. BPMN task, gateway and event constructs linked to sequence flow and expressed on ISSRM security requirements. Nonetheless ISSRM controls expression is missing on BPMN. Different security control modules are pictured in late system development stages of BPMN task, gateway and event constructs.

Current research seems to validate that there BPMN is not committed to the security modelling rather than business process modelling. Despite that BPMN provides assets, their security risks and potential security requirements. Obviously this is not enough for security risk management and some language extensions are preferable to use. Aforetime performed alignment (Altuhhova *et al.*, 2012) of the BPMN constructs to the concepts of the ISSRM domain model is done in this paper.

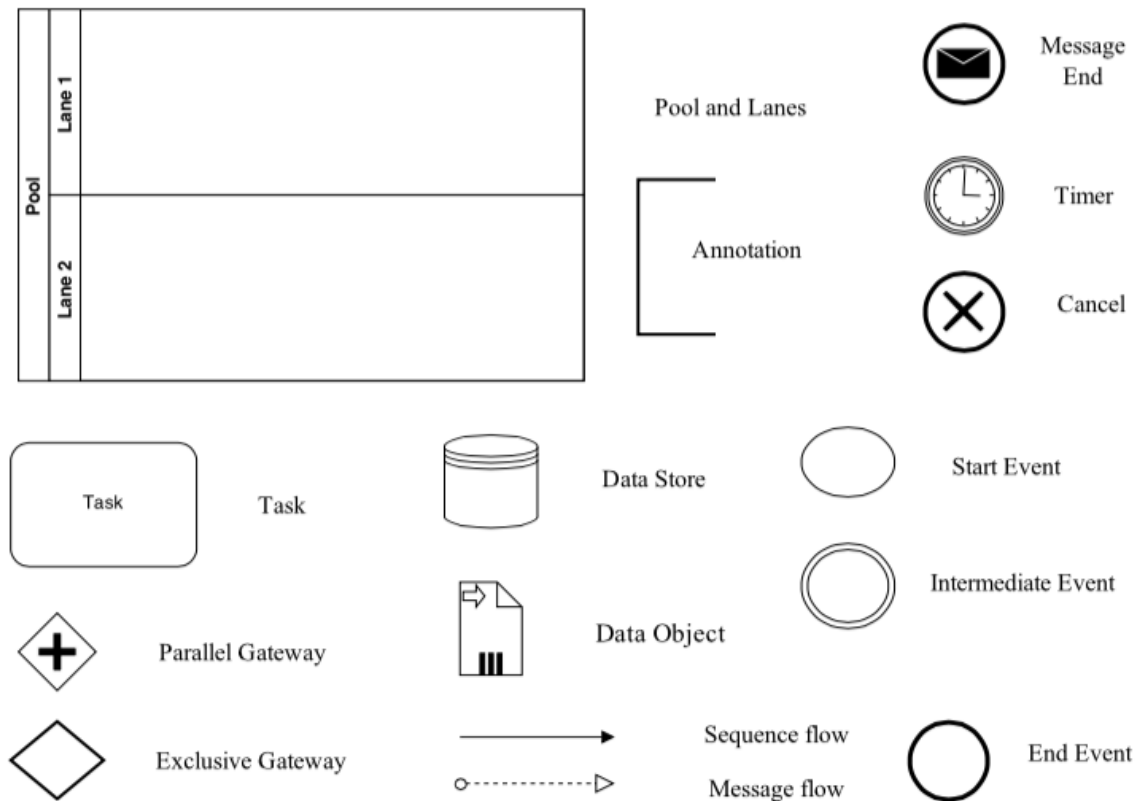


Figure 4. BPMN concrete syntax (Altuhhova,2013)

4.2.2 Social Engineering Example in BPMN

This section discusses different methods of social engineering attack. To illustrate the BPMN security extensions, below provided one chosen example, related to security criteria of the business assets.

Context and asset identification. Let's consider the following situation where the potential user (pool Jenny in Figure 5) receives a call and wishes to get information from the system (CBIS). In order to get any information Caller requests it (task *Call and ask for data*) while the user checks it from the system. Janie Acton call for data (task *Maintain data, Write query for data*), receive information (tasks *Data received*) and uses it (task *Uses data*). When Jenny asked data the CBIS system manages it (tasks *Retrieve data, Provide data*).

Determination of security objectives. In the current case existed violation of the confidentiality of information in CBIS system (it is shown by the *Lock* on the *Data object*). Violation of confidentiality of information caused a harm to the organization by usage of other person's private information for not intended purpose.

From the **Risk related concept** in this case the caller or attacker pretended to be an employee of the same organization. Attacker said that his computer has been damaged by virus. In consequence of this he cannot get information to one of the vice-presidents. Caller collected data thorough search to confirm his authenticity. Violator asked to see from the system account number, phone number entry and service address. In Figure 6 it is presented that in pool Caller the violator asks for an information (task *Calls and asks for a data*) then receives it (task *Data received*) and finally uses it (task *Uses data for unintended purpose*). In this case an employee, Jenny performs same actions as it was a Good Caller. She has an access to data (task *Maintain data*) checks it from the system (task *Write query for data*), receives (task *Data received*) and provides it to the requestor (task *Uses data*).

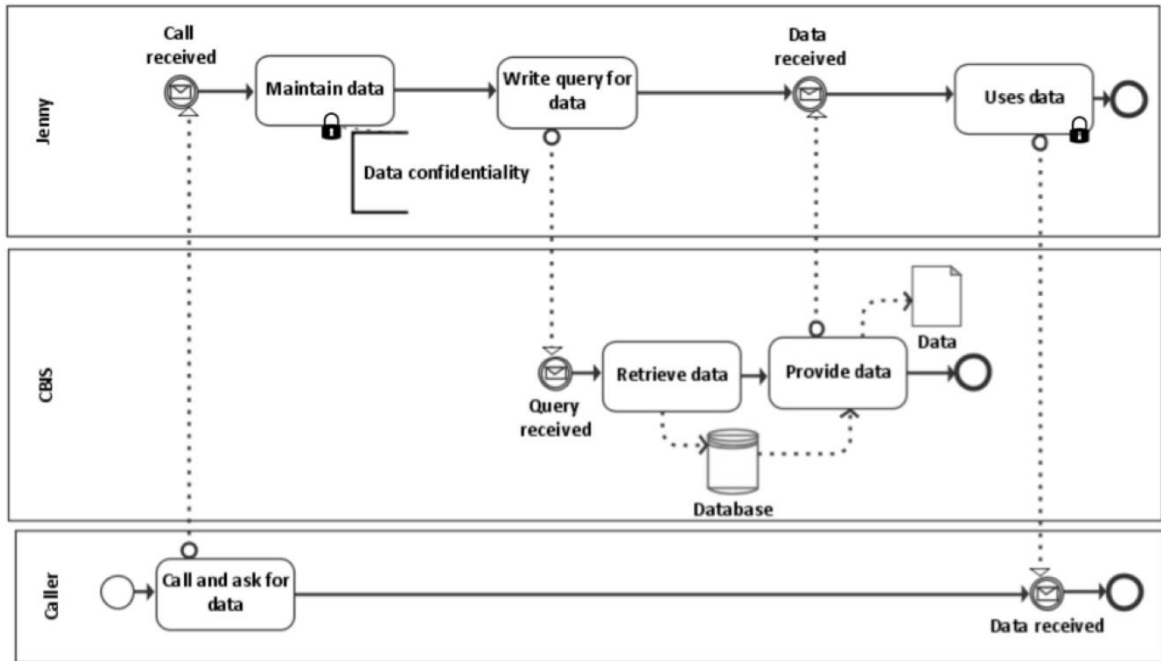


Figure 5. Janie Acton's Story- BPMN assets identification

Henceforth **Risk treatment concept** for a Janie Acton's story presented in Figure 7. Then the whole process will be slightly different, as Jenny asks for a verification (task *Ask for ID*) and when it is received, checks it (task *ID received, Check ID*). If it is not ok, she can decline request (task *Refuse to give data*). The Caller in such situation will give a not valid ID (task *Asked ID, Provide fake ID*).

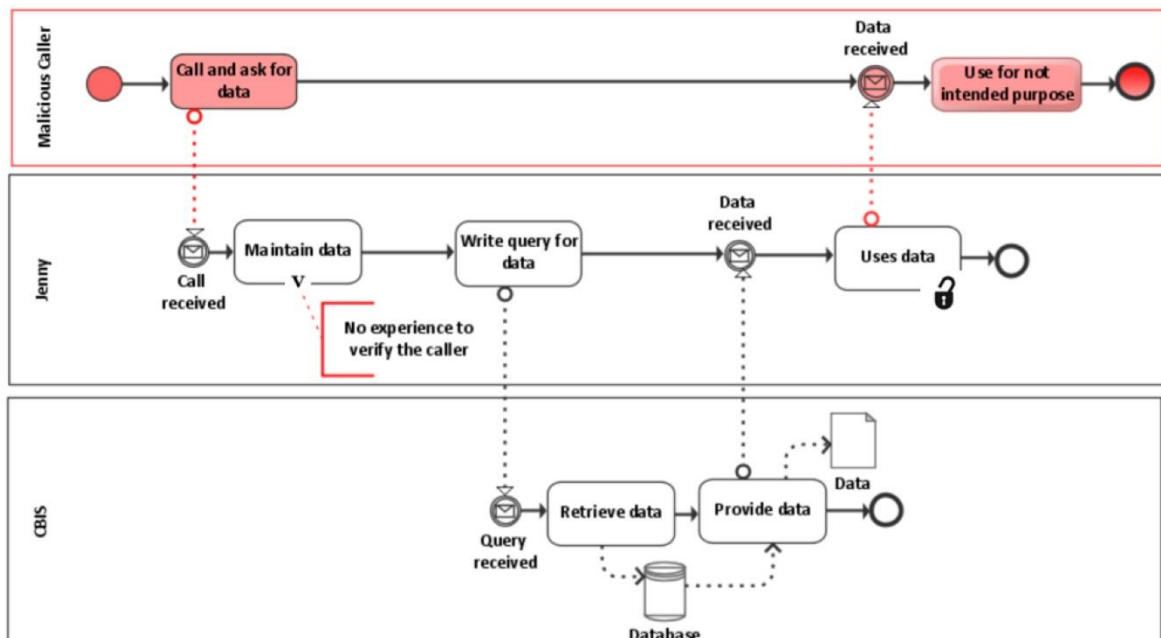


Figure 6. Janie Acton's Story- BPMN risks identification

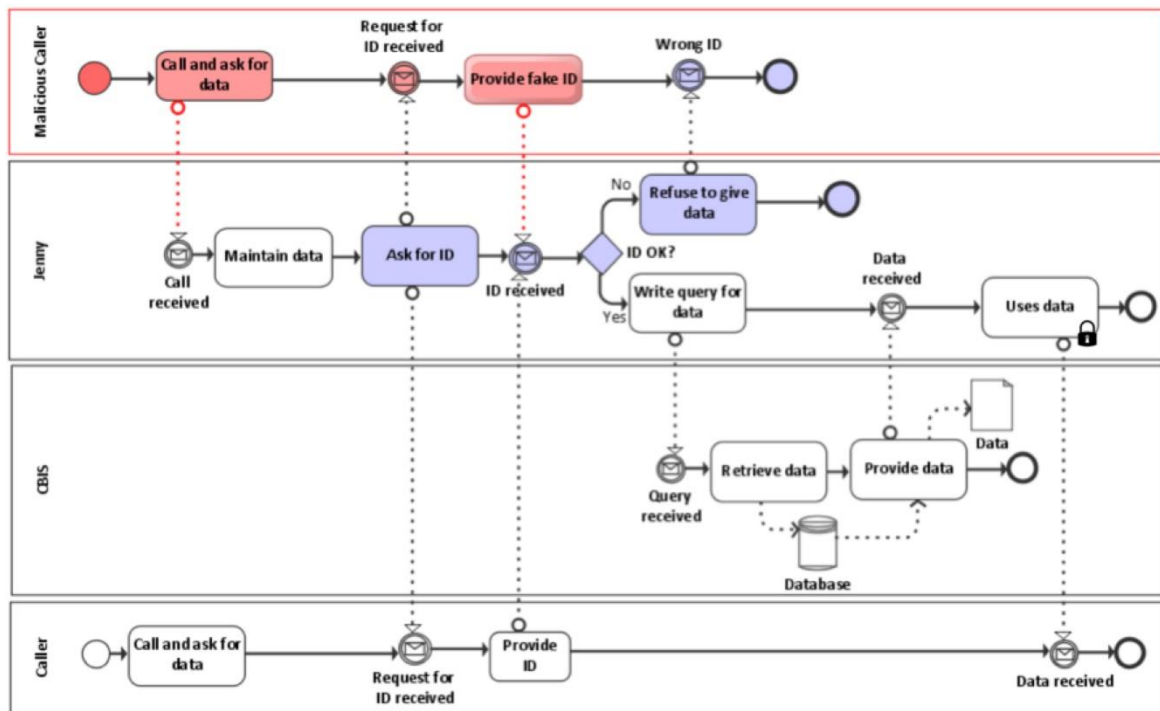


Figure 7. Janie Acton's Story- BPMN risks treatment

Table 7. ISSRM assets concepts modelled in BPMN


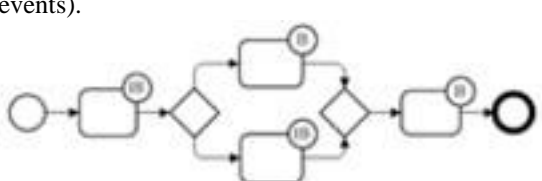
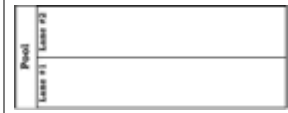
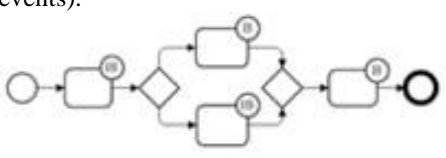



	What is ... ?	Which language construct expresses ... ?
Business asset	Data Caller and its business process including <i>Call and ask for data</i> and <i>Data received</i> Jenny tasks <i>Maintain data</i> and <i>Uses data</i> could be considered as business asset under some circumstance.	 Data store Combination of Flow objects (tasks, <u>sequence flow</u> and events). 
IS asset	Jenny Jenny's process <i>write query for data</i> , <i>data received</i> . Process executed in CBIS. Database	 Pool Combination of Flow objects (tasks, <u>sequence flow</u> and events).   Data store
Security criterion	Data confidentiality	 Annotation

Table 8. ISSRM risk treatment related-concepts modelled in BPMN

	What is ... ?	Which language construct expresses ... ?
Risk treatment decision	Data reduction	No construct
Security requirement	Ask for ID, After ID is received, check if ID is OK if not refuse to give data	Combination of Flow Objects (tasks, gateways and events) using Sequence Flow 
Control	Not proposed	No construct

4.3 Misuse case

Sindre and Opdhal proposed a misuse case that includes graphical notation and textual representation to model security concerns (Sindre *et al.*, 2005). The *misuse case* is characterized as by an agent, who can cause a harm to stakeholders or/and to the system if performs his tasks successfully. In such situation the *misuser* is identified as a performer who wants to use the system with damaging intents. At the beginning using the misuse case it was possible to model threats, but later there was adapted the concept of security use. Finally Rostad has enlarged the misuse cases with the vulnerability.

4.3.1 Alignment of SROMUC to ISSRM Domain Model

This section is concentrated on the alignment of SROMUC (Security Risk-oriented Misuse Cases) with the concept in ISSRM domain model. There is an outline of the ISSRM concepts in Figure 3.

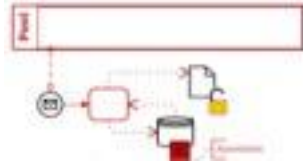

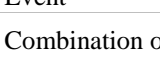

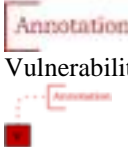



Alignment of asset-related concepts. In ISSRM domain model assets are resented by *Actor* and *Use case*. In SROMUC a *use case* model the business asset and the IS asset. The IS asset is expressed using the *supports relationship* and business assets using *extend* and includes relationships. The ISSRM *security criterion* is shown in *hexagon* construct of SROMUC. *Hexagon* is linked to the business *use case* though dotted line with *constraint of relationship* as on ISSRM domain model security criterion with business asset (Mayer, N., 2009).

Alignment of risk-related concepts. A *threat agent* in SROMUC is shown as a *misuser*, *misuse case* as *attack method* and *use case* and *vulnerability*. A mix of *misuser* and *misuse case* forms a *threat*, *threatened relationship* presented in *targets relationship*. *Rounded rectangle* is imported to model the *impact* on ISSRM concept.

Also there are use *exploits* in a link between *misuse case*, the *vulnerability* leads to definition of the link between the *misuse case* and the *impact*. The *harm* is identified between an *impact* and a *business use case*, *negates* is illustrated as a link between an *impact* and *security criterion*. *Threat agent*, *attack method*, *vulnerability*, *impact* are combined to represent an *event*, where *risk* is a combination of *event* and the *impact* (Matulevičius, R et al., 2008).

Alignment of risk treatment-related concepts. Security requirements represented in the visual syntax of *security use case* by adding a padlock to *security use case*.

Table 9. ISSRM risks concepts modelled in BPMN

	What is ... ?	Which language construct expresses ... ?
Risk	Malicious caller calls and asks for data, receives data, and uses data for not intended purpose because Jenny has no experience to verify the caller, this leads to data confidentiality negation and data reception for unintended use.	Combination of Event and Impact 
Impact	Data confidentiality negated Data received Harm to Jenny is not indicated	Unlock  Event 
Event	Malicious caller calls and asks for data, receives data, and uses data for not intended purpose because Jenny has no experience to verify the caller	Combination of constructs for Threat and Vulnerability 
Vulnerability	Jenny has no experience to verify the caller	Annotation  Vulnerability point for characteristic of
Threat	Malicious caller calls and asks for data, receives data, and uses data for not intended purpose	Combination of construct for Threat Agent and Attack method 
Threat agent	Malicious caller	Pool 
Attack method	Call and ask for data, data received, use for not intended purpose	Combination of flow objects (tasks and event) using Sequence Flow 

4.3.2 Social Engineering Example in SROMUC

This section illustrates application of SROMUC modelling to the Jane Acton's story. It is focused on confidentiality of information stored in CBIS system. For a better understanding of the case, model is divided into 3 pictures: for assets, risks, security requirements.

Asset Model. The case is focused on Jenny and the CBIS system. An asset is only Jenny who is a user of the CBIS system. In order to get any information *Jenny Maintain data*,

Write query for data and *Uses data*. The *Call and Ask for data* includes *Maintain data* and includes *Write query for data*. *Maintain data* has a security criterion *Confidentiality of data* represented as a hexagon. The *Provide data* includes *Retrieve data*. According to the ISSRM domain model *Maintain data*, *write query for data* and *Uses data* has been identified as an *IS asset* that has a value to the organization. *Retrieve data* and *Provide data* are Business asset.

Risk Model. In Figure 9 is presented security threat scenario. A misuser (i.e., Attacker) uses vulnerability (i.e., *No experience to verify the caller, Jenny is not trusted*) to initiate misuse case (i.e., *Call and ask for data*). In the grey filling represents a vulnerability, threat is shown in black. *Call and ask for data* exploits the fact that *No experience to verify the caller*. Threat *Receive data* threatens *uses data*.

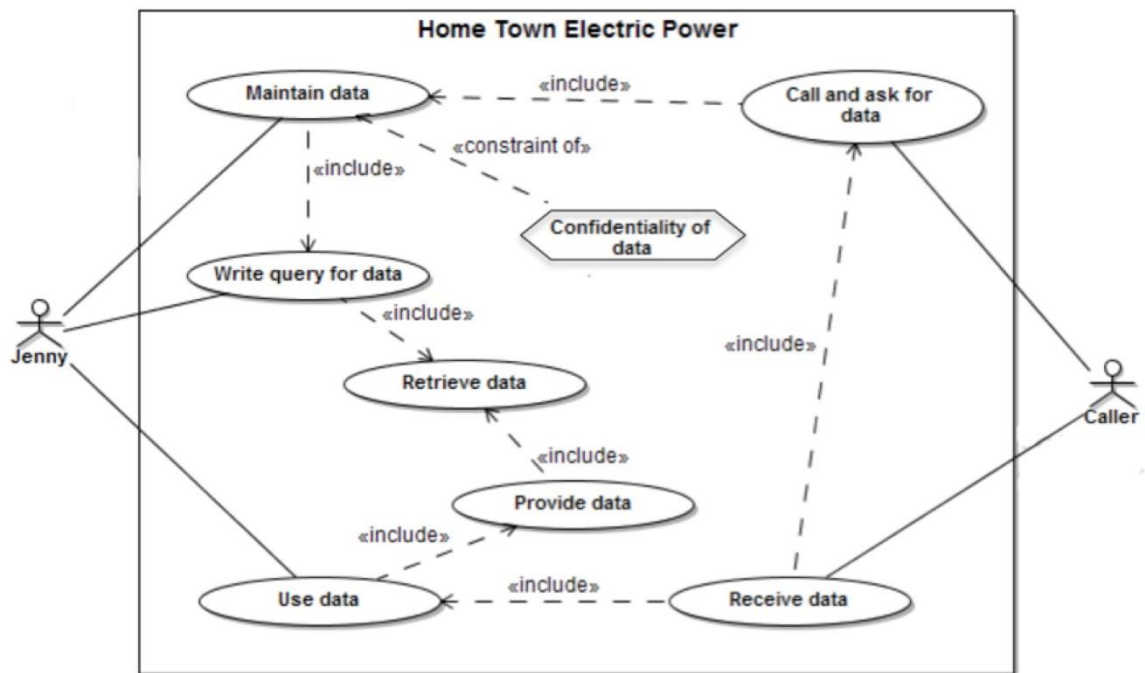


Figure 8. Asset modelling for Janie Acton's Story




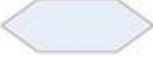
Risk treatment model. SROMUC does not support the risk treatment concept, but it is possible to model a security use case for identification of security requirement. In the Figure 10 represented security use case. It is shown by a use case diagram with a lock inside to mark security requirement for identified threats. The use case *Jenny* and *Maintain data* (i.e., IS Asset) has to include a security use case (i.e., *Ask for ID*). The security use case mitigates the misuse case (i.e., *Uses data for unintended purpose*). It ensures security criterion (i.e., *Confidentiality of data*) imposed by business use case (i.e., *Maintain data*).

4.4 Secure Tropos

In this section will be represented summary of another modelling language as Secure Tropos and its support management of IS security Risk.

Secure Tropos (Mouratidis and Giorgini, 2007a), (Mouratidis et al., 2003a) is built upon the Tropos methodology (Bresciano et al., 2004). It assists in growth of IS security in its development stage. There are existing four phases (Matulevičius et al., 2012): early and late requirements, architectural and detailed design. In this paper is thought-out only early and late requirement analysis (Bresciano et al., 2004) or early stage of the IS development.

Table 10. ISSRM assets concepts modelled in SROMUC

	What is ... ?	Which language construct expresses ... ?
Business asset	Data Call and ask for data, receive data Under some circumstances: use cases, like Maintain data, Write query for data, Use data	Not presented Use cases <u>and appropriate link to express <i>include</i></u> . 
IS asset	Combination of use cases, like Maintain data, Write query for data, Use data, Retrieve data, Provide data Home Town Electric Power	Use case <u>and appropriate link to express <i>include</i></u> .  System boundary: 
Security criterion	Confidentiality of data	 Construct for security criterion, “hexagon” <u>and link express <i>constraint of</i></u> .

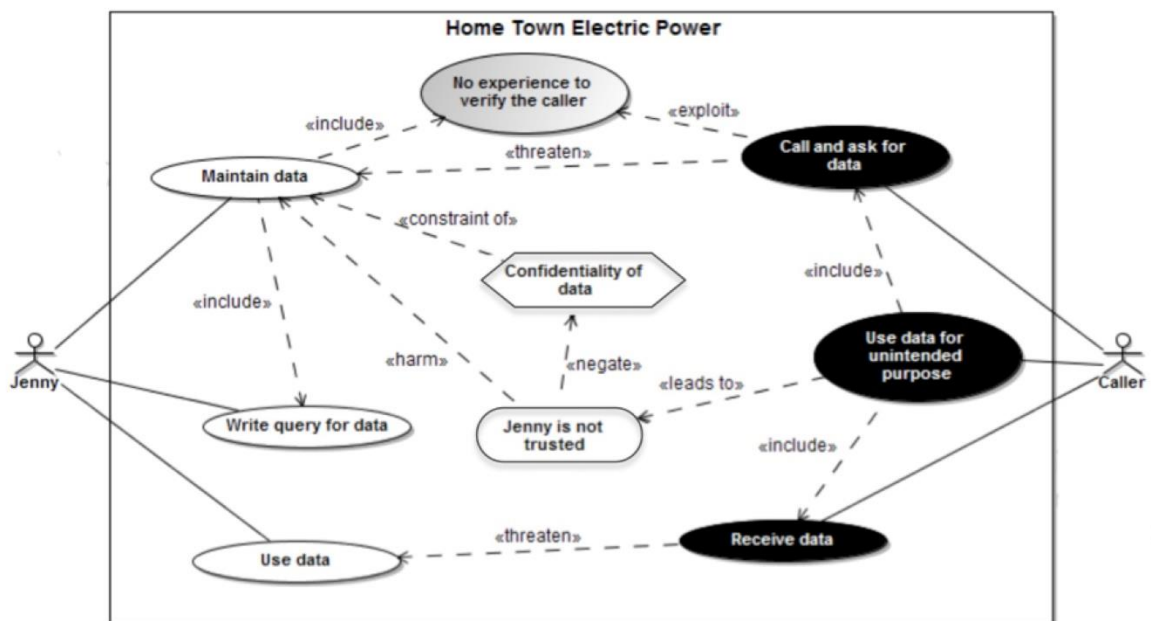


Figure 9. Threat modelling for Janie Acton's Story

4.4 1 Alignment of Secure Tropos with ISSRM

The Secure Tropos syntax has been decided to the three construct categories of ISSRM domain model: asset-related concepts, risk-related concepts and risk-treatment concepts. Besides underlined categories of syntax this section will also take into account how ISSRM relations (e.g., supports, constraint of, exploits, targets, mitigates and others) can be expressed in Secure Tropos (Matulevičius et al., 2012).

Asset-related concept. Actor, hardgoal, plan resource, softgoal constructs represent assets using compositions as dependency, meansends, contribution and decomposition relations.

Different Secure Tropos relationships can be expressed in ISSRM IS and business assets. Security criterion of ISSRM is expressed by softgoal and/or security constraint.

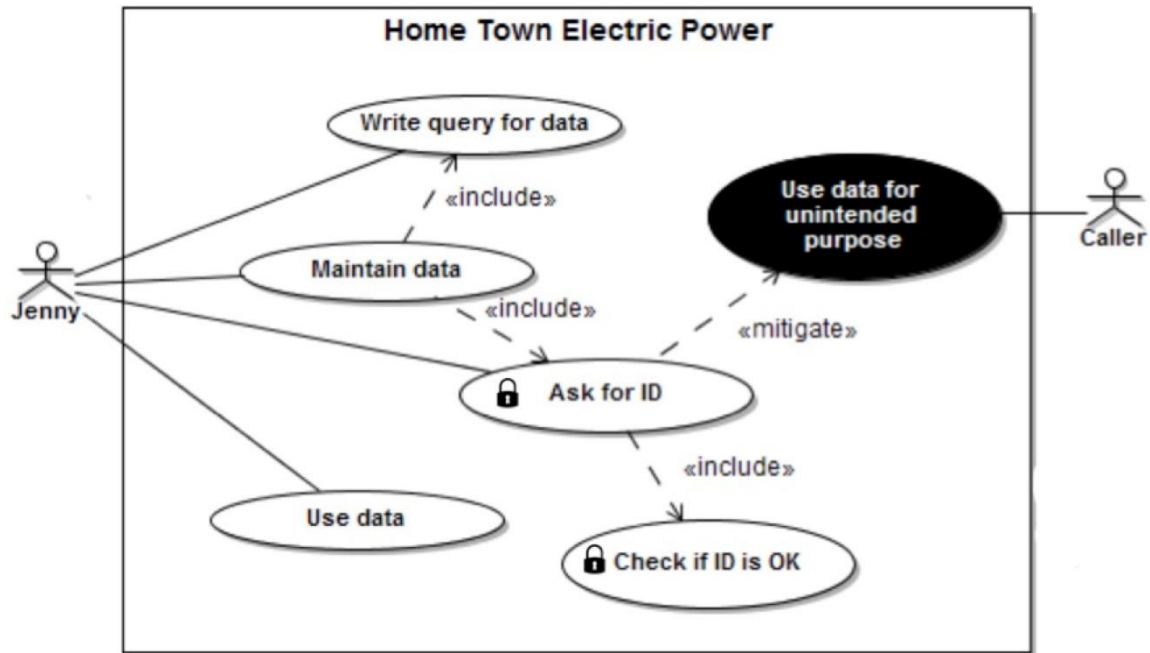



Figure 10. Risk treatment modelling for Janie Acton's Story








Table 11. ISSRM risk treatment related-concepts modelled in SROMUC

	What is ... ?	Which language construct expresses ... ?
Risk treatment decision	Risk reduction	No constructs
Security requirement	Ask for ID Check if ID is OK	 <u>Security use case construct and link include.</u>
Control	Not modelled. <u>There is a need to implement security policies.</u>	No constructs

Risk-related concept. Standard Secure Tropos constructs can represent a *threat agent* of ISSRM as an *actor*, *attack method* as a *plan*, *threat* as a *hardgoal* and/or *plan*. Extension presented by Elahi and Yu (Elahi and Yu, 2007) introduces representation of *vulnerability* as a *vulnerability point*. Representation of *threat agent*, *attack method* and *vulnerability* can serve event of the risk.

Risk treatment-related concepts. *Actor*, *hardgoal*, *plan*, *softgoal* and *security constraints* represent *security requirements*, which need to have dotted background pattern. Representation of the ISSRM security requirements concept in Secure Tropos is shown *mitigates* relationship (Matulevičius et al., 2012).

Table 12. ISSRM risks concepts modelled in SROMUC

	What is ... ?	Which language construct expresses ... ?
Risk	Caller calls and asks for data, receives data, and uses data for unintended purpose because no experience to verify the caller when maintaining the data. That leads to negation of confidentiality of data as Jenny is not trusted and harm to maintain data.	Combination of Event and Impact. 
Impact	<i>Negate</i> confidentiality of data Jenny is not trusted (harm to IS asset) <i>Harm</i> to maintain data (harm to business asset)	 Impact construct and appropriate links to express <i>harm</i> and <i>negation</i> of security criterion
Event	Caller calls and asks for data, receives data, and uses data for unintended purpose because no experience to verify the caller when maintaining the data	 Combination of constructs used to express <i>threat</i> and <i>vulnerability</i>
Vulnerability	<i>No experience to verify the caller</i> when maintaining the data	 Vulnerability use case
Threat	Caller calls and asks for data, receives data, and uses data for unintended purpose	 Combination of <i>misuser</i> and <i>misuse cases</i> . <u>Misuse cases are linked by include.</u>
Threat agent	Caller	 Misuser
Attack method	Call and ask for data, Receive data, Use data for unintended purpose	 <u>Misuse case construct and link to include cases.</u>

4.4.2 Social Engineering Example in Secure Tropos

This section illustrates application of Secure Tropos modelling to the chosen case - Jane Acton's story. Model is divided into 3 pictures: assets, risks, security requirements.

Asset Model. The first figure 11 represents an asset identification in Secure Tropos. In the picture is shown goals (e.g., *Query received*, *Provide data*, *Data provided*, *Data from CBIS received*) plans (e.g., *Call and ask for data*, *Uses data*, *Write query for data*) actors (e.g., *CBIS*, *Caller*, *Jenny*). It is also possible to identify security objectives by representation of softgoal (e.g., Confidentiality) with security constraints (e.g., *confidentiality of data*).

Risk Model. Figure 12 presents potential risks of Janie Acton's story. Event that concentrates provided figure called Social Engineering attack. It represents a situation, where threat agent calls as an employee in order to get required information. After indentation of the possible risk, we need to identify threat, vulnerability, and threat agent and attack method. Malicious caller has a threat (e.g., *Use data for not intended purpose*) by Data provided.

Caller attacks Data provided through exploiting the vulnerability identified in Uses data. Thus exploit link shows a relationship between an attack method and a vulnerable IS asset.

Security requirement. In order to mitigate the identified risk about Social engineering attack, it has been chosen risk reduction. Security requirement is presented in dotted background pattern. In our case it is *Check ID*. In this situation, the *Confidentiality of data* also becomes a security requirement mitigating the risk.

Tables 7-15 presents a semantic alignment of the language constructs to the concept of the ISSRM model. These tables representation has been done to each of language that this paper covers. At this stage of analysis such tables helped in understanding of semiotic clarity of the SRM language with respect to the ISSRM domain model. Further section is concentrated on discussion of founding and identification of one modelling language that has a better alignment with ISSRM concept.

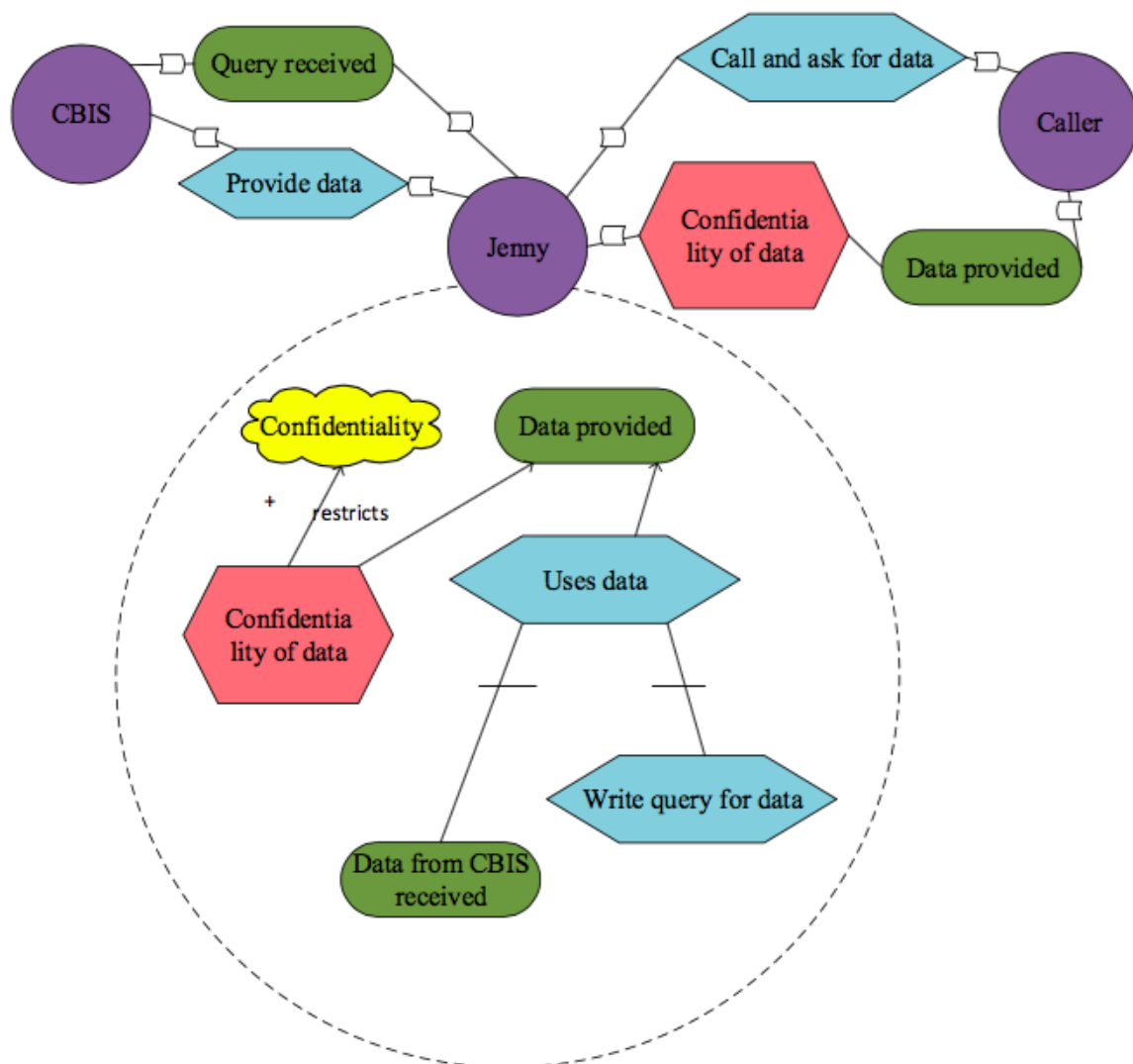


Figure 11. Janie Acton's Story- Secure Tropos assets identification

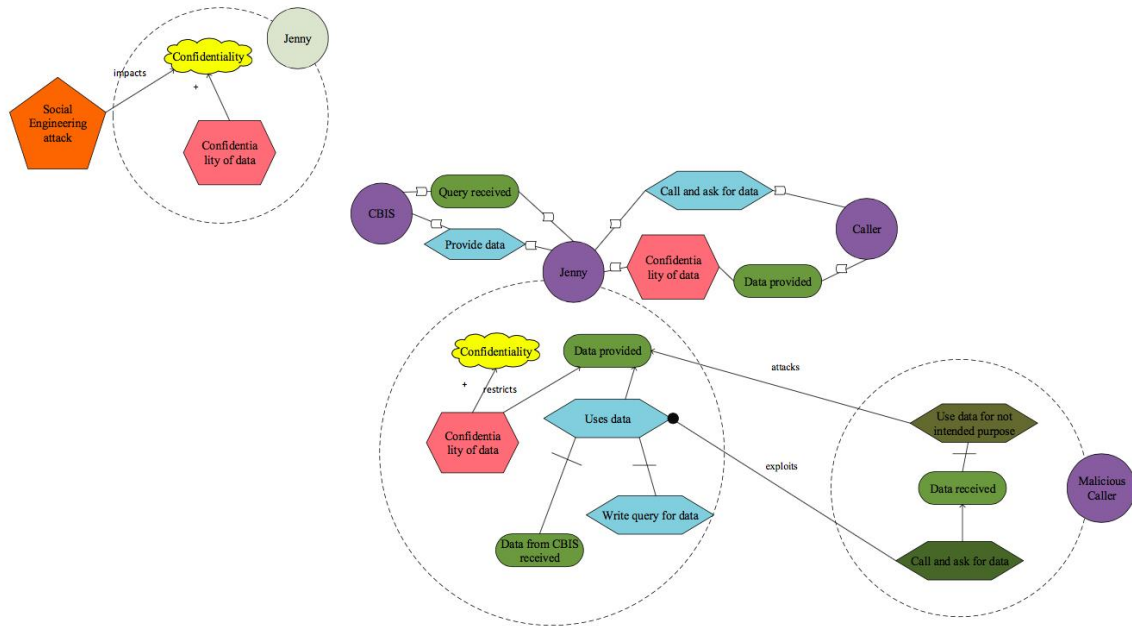
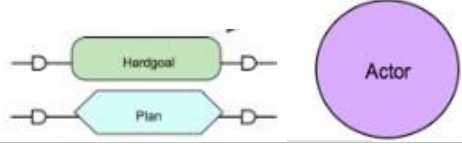


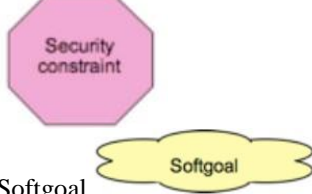


Figure 12. Janie Acton's Story- Secure Tropos risks identification

Table 13. ISSRM assets concepts modelled in Secure Tropos

	What is ...?	Which Language construct expresses ...?
Business Asset	Data Call and ask for data, Data provided Jenny and Caller Under some circumstances as business asset could be considered write query for data and data provided.	Not represented Combination of Actor, hardgoal and plan that support their dependency 
IS Asset	Jenny Jenny's process write query for data, uses data, data provided Process executed in CBIS as query received, provided data, data from CBIS received CBIS	Actor  Composition of the plan,hardgoal using decomposition and means-ends relationships Means-ends Decomposition 
Security Requirement	Confidentiality of data Confidentiality	Security constraint contribution  Softgoal

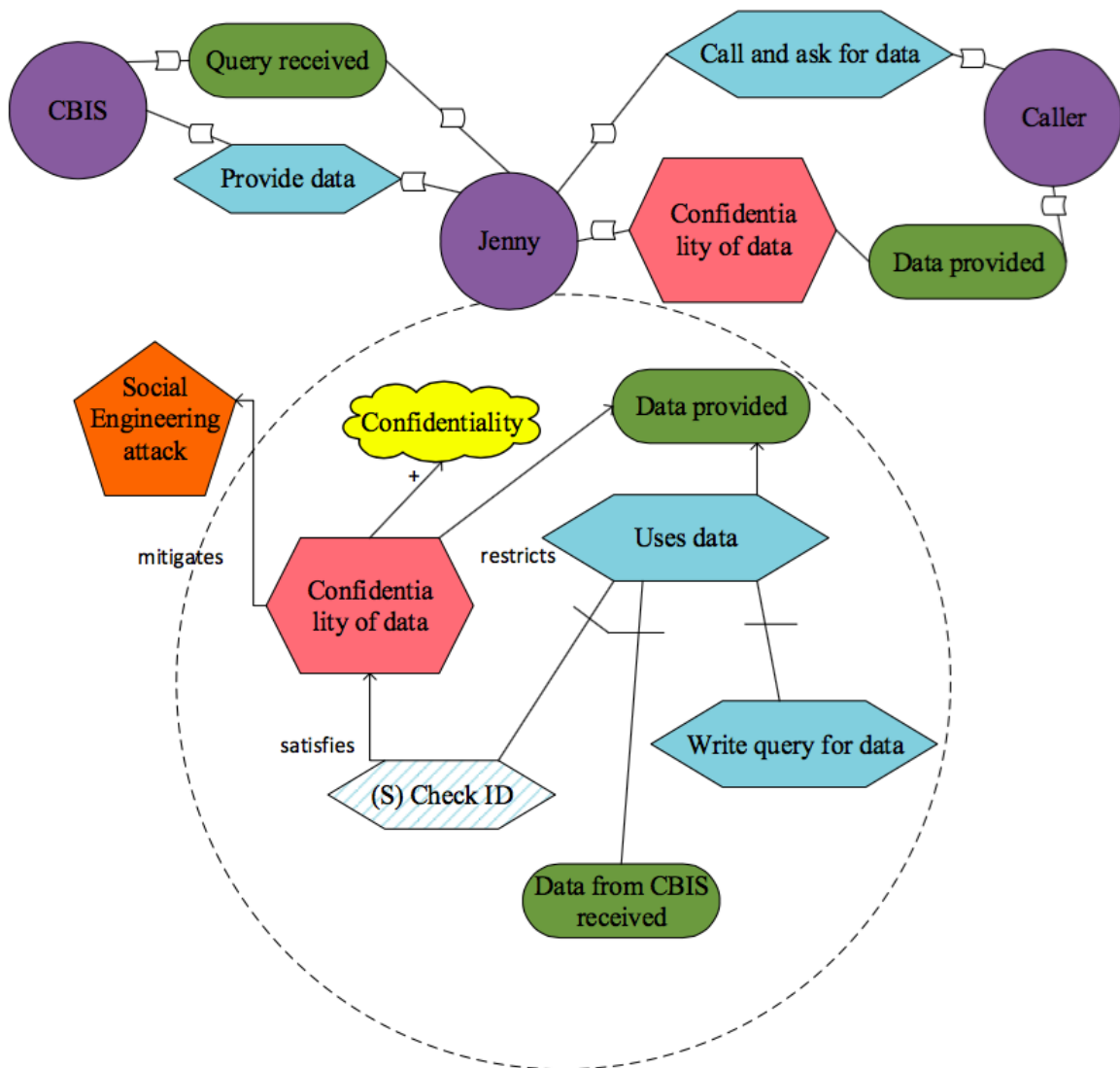


Figure 13. Janie Acton's Story- Secure Tropos risks treatment

Table 14. ISSRM risk treatment related-concepts modelled in Secure Tropos


	What is ...?	Which Language construct expresses ...?
Risk treatment decision	Risk reduction	No constructs
Security requirement	Check ID	Plan that has dotted background pattern 
Control	Not proposed	No constructs

Table 15. ISSRM risks concepts modelled in Secure Tropos

	What is ...?	Which Language construct expresses ...?
Risk	Malicious caller calls and asks for data, received data and uses data for not intended purpose to exploit use of data and attack data using social engineering attack to negate confidentiality of data	<p>Composition of Event and Impact</p>
Impact	Social engineering attack negates confidentiality of data	<p>Impacts</p>
Event	Malicious caller calls and asks for data, receives data, uses data for not intended purpose to exploit use of data and attack data (Data provided) using social engineering attack	<p>Combination of an Agent , goal, plan, exploits and vulnerability point</p>
Vulnerability	Not clearly identified but points out that vulnerable is use of data	<p>Is not modelled, but vulnerability point identified the attributes of the assets(plan)</p>
Threat	Malicious caller calls and asks for data, receives data and uses data for not intended purpose	<p>Combination of constructs for Threat Agent and Attack method</p>
Threat agent	Malicious Caller	<p>Agent</p>
Attack method	Call and ask for data, data received, use data for unintended purpose	<p>Agent executes plan and goal using mean ends, decomposition relationships</p>

4.5 Discussion

From the information obtained, through the study of different modelling languages, this section discusses our experience through use of these languages and alignment of them with ISSRM concept.

The first step of study and alignment of modelling languages, we also have carefully applied these modelling languages to a given case. Certainly based on our experience we have already made our mind regarding how easy it is to understand certain aspects in each of these languages. Despite the fact that BPMN has been introduced with the aim to the business users, it supports security management concepts (in an enterprise level). Based on our subjective opinion it has several advantages: clear description of processes and tasks performed by certain actors, visual reproduction of security objectives and vulnerability. Overall we count BPMN modelling language as more structured than other two. Moving on to Misuse case modelling language, it also has its own convenience in language use. For example, actors' illustration; separate constructs for security criterion, vulnerability, impact, security requirements, and attack method with a clear link to each concept. Lastly, Secure Tropos has its own language construct expression to each concept. All of them are simply to comprehend based on different forms and colors. Each user of these modelling languages might find something special in a particular language. We like better BPMN modelling language as count it as the most optimal and ease to use. Clear structural approach that is used in this language is one of the main aspects that attracts us. It should be noted that this observation is purely subjective, but it is done to express the hypothesis to be investigated in Section 5.

With regard to our analyses of BPMN, Misuse case and Secure Tropos we have done tables that we concentrated on theoretical part of language constructs. It is presented in Table 16. Also after each representation of modelling language and its application to the chosen example as a summary has been done separate tables. To readers convenience each table has been divided based on asset-related concepts, risk-related concepts and risk treatment-related concept. Based on Table 16 it is relatively easy to identify one common aspect in all three modelling languages, their absence of control and risk treatment construct. Probably it is better to start with Secure Tropos constructs as in most cases of ISSRM concept alignment they are used in a combination off their own constructs (to express one concept). Separate construct is used for security criterion, vulnerability, threat agent. Same separate constructs in the rest two modelling languages, however, for Misuse case added impact construct. Impact in Misuse case represented by impact construct. As vulnerability, security criterion and threat agent in each studied modelling language has its own construct it might be advisable to take a look to each of them. In BPMN vulnerability is characterized by text annotation V, Misuse case uses special vulnerability use case and in Secure Tropos it is not modelled, however vulnerability point helps in identification of the attributes. In case of a threat agent identification in BPMN it represents pool, Misuse case has misuser and Secure Tropos – an Actor. Lastly, security criterion is represented by security construct in Misuse case, Softgoal and Security constraint in Secure Tropos. In BPMN security criterion shown text annotation and lock. However, lock represent security need, not security criterion. Other ISSRM concepts can be identified by association with different constructs. Illustration of a threat in a Misuse case is a combination of a misuser and misuse cases. Also misuse cases are linked by include. In Secure Tropos it is presented by a combination of attacker, goal, plan constructs. BPMN uses pool with a combination of flow objects (tasks and event) using sequence flow to illustrate threat.

Table 16. Concept alignment of security languages with ISSRM domain model

ISSRM Concepts	BPMN constructs	Misuse cases constructs	Secure Tropos constructs
Asset	Task, Even, Sequence Flow	Actor	Actor, Goal, Soft-goal, Plan, Resource
Business Asset	Data Object, Task, Event, Sequence Flow	Use case	Actor, Goal, Soft-goal, Plan, Resource
IS asset	Task, Event, Sequence Flow, Datastore, Pool	Use case	Actor, Goal, Soft-goal, Plan, Resource
Security criterion	Text Annotation Lock(not security criterion, but security need)	Security construct	Security constraint, Softgoal
Risk	Task, Event, Sequence flow, Message Flow, Pool, Text Annotation, V (characteristics of vulnerability), Unlock, Message Flow, Event	Misuser, Misuse case, Vulnerability use case and Impact constraint	Composition of a Threat and Impacts relationship
Impact	Unlock, Message Flow, Event	Impact constraint	Contribution between the threat and soft-goal
Event	Task, Event, Sequence flow, Message Flow, Pool, Text Annotation, V (characteristics of vulnerability)	Misuser, Misuse case and Vulnerability use case	Threat
Threat	Task, Event, Sequence flow, Message Flow, Pool	Misuser and Misuse case	Goal, Plan
Vulnerability	Text Annotation, V (characteristics of vulnerability)	Vulnerability use case	Not modelled, but vulnerability point identifies the attributes of the assets (plan)
Threat agent	Pool	Misuser	Actor
Attack method	Task, Event, Sequence flow, Message Flow	Misuse case	Plan, relationship attacks
Risk treatment	None	None	Not mode
Security Requirement	Task, Even, Sequence Flow, Gateway, Message Flow	Misuse case	Actor, Goal, Soft-goal, Plan, Resource, Security constraint
Control	None	None	None

5 An Experiment Report Outline

Taking into account different modelling languages, which were discussed in chapter 4, we are interested in identification and investigation of modelling languages that could be better understood by ordinary people. To identify one language construct we prepared a questionnaire and collected some results from participants. Based on obtained results, some findings will be done.

This chapter has following structure: section 1 presents problem statement, section 2 demonstrates study design and how results were calculated, section 3 covers details of the empirical study, section 4 introduces results, section 5 considers threats to validity, section 6 discusses findings with other papers and finally, section 7 concludes results of the study.

5.1 Problem Statement

In this paper analysis will be concentrated on the security risk-oriented modelling languages. In the scope of this research is included BPMN, Secure Tropos and Misuse case. Those languages have an extension to express information security risk management. The aim of this research is to investigate whether ordinary model readers understand created figures and do those models carry the security related information. Thus, research questions are:

RQ1: Which language is easier to comprehend for the security risk management?

RQ2: Which model is better perceived by participants?

As we consider, results might be based on participant's background and experience. Overall assumed result of the study is that:

H1: Results of BPMN language concepts and constructs will be better than in Misuse case and Secure Tropos

5.2 Planning of Questionnaire

Questionnaire has been prepared from the modelled case using BPMN, Secure Tropos and Misuse case language constructs. In Appendix E, F and H are presented examples of questionnaires that all participants of this research have received. Step by step composition of this questionnaire looks as follows:

- Learned and studied regarding BPMN, Secure Tropos and misuse case
- Chosen case which will be constructed in BPMN, Secure Tropos and misuse case
- Prepared model for one case in those three modelling languages
- Constructed questionnaires
- Prepared answers to those questionnaires
- Distributed questionnaires to the participants of the course on "Principles of Secure Software Design"
- Collected results

Feedbacks from respondents allows to compare those models and many necessary analysis. In a survey document has been introduced modelled case with different concepts. To understand the participants readability of models, on survey were presented two rows. One of them requested to identify construct and second one was done to represent language construct expressions. The aim of this questionnaire was to investigate the understanding of modelling language among responders.

5.3 Experiment Operation

To answer a research question defined in Section 1, we made an analysis of collected data from students. Empirical study has been conducted at the University of Tartu during the course on “Principles of Secure Software Design”. The course was taken by the Cybersecurity study program. Participants took part in lectures and workshops on security risk management, security modelling, security requirements, and model driven security and development processes of the secure software. The questionnaire has been hand out during the lecture.

The study consists of few stages. Participants were requested to analyze diagrams of security risk model in all three concepts together and fill the open-ended questionnaire. The questionnaire requested to classify the ISSRM concept expressions in provided diagrams. Correct answers to those questions are presented in Tables 7-15. Also they are divided to asset related concepts, risk related concepts and risk-treatment related concepts. In risk related concept is presented vulnerability. It is conferred in concept of *Jenny has no experience to verify the caller* (BPMN uses text annotation and vulnerability point is identified by V, misuse case uses vulnerability use case, in Secure Tropos shown by vulnerability point). Control is not represented in all modelling languages concept expressions. If there are several concepts that represent one construct, then preliminary table of correct answers was divided based on actors. If even one of the concept has been mentioned by a participant, it has been included in the sheet of correct answers (see Appendix I, J and K).

For example business asset has several concepts as *Data*, *Caller* and its business process including *Call and ask for data*, *Receive data*, *Jenny tasks Maintain data* and *Uses data*. They were divided into three sections of correct answers as: *Data*, *Caller*, *Jenny*. Even when responder mentioned one process *Call and ask for data*, it has been counted as a correct answer in the field of *Caller*. Second column of the questionnaire has requested from responders to fill language constructs that are used to model the ISSRM concepts. Responders needed to identify the constructs or their combination of them as shown in Tables 7-15. There are no constructs to risk treatment decision and control in both modelling languages. If there is a combination of flow objected using sequence flow, events, tasks and only one correct answer is mentioned, then same technique as in case of concept expressions has been used.

5.4 Analysis and Interpretation

Students that took part in this research were not aware of intend of this study. They were informed to fill provided questionnaire based on they understanding of provided task. Primarily all of participants were not intended to participate in an experiment; they were participating a course.

Concept: Total amount of received answers is 34: (i) twelve responses in identification of BPMN constructs were identified as valid (ii) ten responses in identification of misuse constructs were valid (iii) twelve responses in identification of Secure Tropos. These numbers are included only as valid responses. Table 17 represents the results of the correct answers identified by the respondents. More detailed data of answers is presented in Appendix. To have a better understanding of results that have been received in the process of response and analyze correctness of provided hypothesis, further part is concentrated on evaluation of them.

Table 17. Comparison of concepts created using SRM language

ISSRM Concepts	BPMN concept	MUC concept	Secure Tropos concept
Number of responses	12	10	12
Business asset	42%	53%	63%
IS asset	17%	20%	44%
Security criterion	100%	90%	67%
Risk	60%	35%	46%
Impact	22%	50%	83%
Event	75%	55%	56%
Vulnerability	83%	80%	33%
Threat	58%	30%	50%
Threat agent	92%	100%	100%
Attack method	14%	27%	42%
Risk treatment decision	17%	100%	58%
Security requirement	72%	35%	58%
Control	0%	0%	8%
Overall	652%	675%	708%

Based on overall results it is evident that Misuse case is understood better than BPMN. Four ISSRM concepts (namely, *event*, *vulnerability*, *threat*, and *threat agent*) are identified in both languages. However five of concepts in BPMN are better recognized (i.e., *risk*, *attack method*, *risk treatment decision*, *security requirement*, *control*) than in misuse case. As seen from the table the overall results in Secure Tropos are better than in misuse case. *Business asset*, *IS asset*, *risk*, *impact*, *event*, *threat*, *attack method*, *security requirement* and *control* are understood by most responders in Secure Tropos. Also, only in Secure Tropos modelling language some responders could identify control concept.

In comparison of all three modelling languages BPMN concepts has better results in *security criterion*, *risk*, *event*, *vulnerability*, *threat*, and *security requirements identification*. In Misuse case all participants identified *risk treatment decision*. Following data from the Table 17 comes out that Secure Tropos concept got better results in evaluation of all received data among responders. *Business asset*, *IS asset*, *Impact*, *Threat agent*, *Attack method*, *Risk treatment decision*, *Security requirement* and *control* were identified in Secure Tropos by higher amount of participant.

Constructs: Total amount of received answers is 30: (i) ten responses in identification of BPMN constructs were identified as valid (ii) eight responses in identification of misuse constructs were valid (iii) twelve responses in identification of Secure Tropos. These numbers are included only as valid responses. Couple handed works were excluded due to the totally incorrect filling of the questionnaire. Obviously, such responders had a problem in understanding the task or/and the model. In each of the modelling languages questionnaire two responders have not filled construct's expression section. Main reason of such lack understanding of provided task might be difference in the disciplines that they have studies before. That led to misinterpretation of the assignment and incorrect filling of questionnaire.

In Table 18 presented results of understanding of constructs in analyzed modelling languages. The difference in concepts identification score between Secure Tropos and misuse case is very large. Moving on to the constructs of Secure Tropos modelling language all aspects were better identified excluding *vulnerability*, *control* and *impact*.

Table 18. Comparison of construct using SRM languages

ISSRM concept	BPMN construct	MUC construct	Secure Tropos construct
Number of responses	10	8	12
Business asset	36%	37%	100%
IS asset	32%	15%	79%
Security criterion	45%	63%	79%
Risk	55%	12%	42%
Impact	32%	50%	42%
Event	73%	40%	46%
Vulnerability	82%	62%	46%
Threat	82%	62%	83%
Threat agent	91%	62%	100%
Attack method	82%	12%	100%
Risk treatment decision	73%	12%	17%
Security requirement	82%	37%	75%
Control	55%	12%	8%
Overall	820%	487%	817%

Taking everything into consideration it is also should be compared Secure Tropos and BPMN constructs. Based on results of BPMN and Secure Tropos constructs it is obvious that BPMN has shown higher results by 3%. Secure Tropos constructs have been better understood in following aspects: *Business Asset, IS asset, security criterion, impact, threat, threat agent*. Others have shown good results in BPMN.

General results: On provided Table 19 are included general underling of concept and construct. It represents general understanding of those three modelling languages in percentage form. Generally, percentage wise understanding of constructs is higher than concepts. *Business asset, IS asset, threat, attack method, risk treatment, security requirement and control* are easily identified in the form of constructs. Concepts are have received higher score in following aspects: *Business Asset, Security criterion, Impact, Event, Vulnerability, Threat, Threat agent, Security requirement*.

Table 19. General understanding of languages

ISSRM concept	General understanding of concepts	General understanding of construct
Number of responses	34	30
Business asset	53%	58%
IS asset	27%	42%
Security criterion	86%	62%
Risk	47%	36%
Impact	52%	41%
Event	62%	56%
Vulnerability	65%	63%
Threat	57%	76%
Threat agent	85%	84%
Attack method	23%	65%
Risk treatment decision	29%	34%
Security requirement	56%	71%
Control	7%	25%
Overall	649%	713%

5.5 Threat to Validity

Validity of obtained data deals with the experiment's treatment. Treatment to the participants were given on principles of the subject, but not to the languages of security risk management. Taking into account that validity depends on the questionnaire, it has been reviewed thoughtfully.

- The first possible threat might be a misinterpretation of the ISSRM concepts. Self-study materials were provided to participants of a questionnaire to mitigate that threat. Also, based on the some studies a person who was in charge for treatment and the experiment design brings more advantage to the research. In this study has been used same technique. It helped to make the terminology of the questionnaire in the secure risk management questionnaire and treatment more consistent.
- Next threat might be students as usually they have a little will to participate in the assessment of the secure risk management languages and their models. As this threat reduction, students were required to fill questionnaire as a reward in the subject points.
- A rather small account of participants may represent a minor threat to validity.
- Some obtained results have very small difference between languages and it is hard to refer as a certain preference or understanding of one modelling language.

5.6 Discussion

In order to illustrate a comparison of running results that were obtained during conducted survey, author decided to study a paper by R. Matulevičius, 2014. Despite the different objectives of studies, there were also done research in understanding of language concepts and constructs. Upon the study of this paper, author found out contrasting results.

The findings of paper (R. Matulevičius, 2014) regarding language concept are very different. This paper results and data presented in R. Matulevičius, 2014 showed same information regarding better understood BPMN concept (security requirement) and Secure Tropos (risk treatment decision). Identified ISSRM concepts showed better results in comparison with analyzed modelling languages. On the model level in this paper better understanding showed Secure Tropos concept however in (R. Matulevičius, 2014) paper findings result that BPMN was best-comprehended model.

Next aspect that has been investigated in this paper is language constructs. Results of survey show that BPMN construct is better understood by participants. However in the paper of R. Matulevičius, 2014 the best perceived SRM language became Secure Tropos. Also in this paper is noted that overall number of valid responses has been only four. Overall score of compared modelling languages is not very large to have certain statement. In our paper difference between results is only 3% percent and number of valid responses differ. All these aspects leave a need for a further deeper analysis in that area.

The identified results in this paper and finding in R. Matulevičius, 2014 do not match and confirm each other in several aspects. The reason of such difference might be some threats to validity that were mentioned in section 5.5. Likewise different domain caused contrasting results. In this paper we have reviewed Social Engineering, but in R. Matulevičius, 2014 was System Engineering. Also it might be good to take into account the total number of valid answers that were received in each case.

5.7 Summary

In this chapter has been analyzed three secure risk management languages - BPMN, Secure Tropos and Misuse case. In other sections we have covered problem statement, planning of questionnaire, experiment operation, analysis and interpretation, threat to validity. The aim of this part of paper was to find out which language's concepts or constructs are better understood. Below are provided some findings, based on research questions and hypothesis.

RQ1: Which language is easier to comprehend for the security risk management?

BPMN concepts that have better results in *security criterion, risk, event, vulnerability, threat, and security requirements identification*. All left concepts were easily identified in MUC modelling language. The sum of all obtained results in each language provided the bases to state that BPMN is better than Misuse case. In comparison of Secure Tropos and Misuse case, indubitably Secure Tropos showed better results among participants. Calculation of the sum of obtained results gave the bases to assert that Secure Tropos concepts are better than BPMN. In comparison of all three modelling languages overall obtained results showed that Secure Tropos concepts are easier to comprehend for the security risk management to ordinary users.

RQ2: Which model better perceived by participants?

Users can understand BPMN modelling constructs better than in Misuse case and Secure Tropos. Nine constructs out of thirteen have shown great results in Secure Tropos in comparison with Misuse case. If compare Secure Tropos and BPMN, BPMN has higher score in understanding of: *security criterion, risk, event, vulnerability, threat, and security requirement*. In comparison of concepts and constructs understanding, constructs received higher amount than concepts. *Business asset, IS asset, threat, attack method, risk treatment, security requirement and control* are easily identified in the form of constructs. Concepts are have received higher score in following aspects: *Business Asset, Security criterion, Impact, Event, Vulnerability, Threat, Threat agent, Security requirement*.

6 Conclusion and Future Work

This chapter summaries what has been done in the paper, state the limitations for the work and identified a contribution of future research.

6.1 Conclusion

In this thesis has been reviewed various approaches and standards with regard of ISSRM domain model. Also one case from the book of Kevin Mitnick “The art of Deception” with application them into three different modelling languages with their alignment to the ISSRM domain model. This paper introduces figures of BPMN, Secure Tropos and misuse case to asset, risk and security requirement modelling. We assumed that based on studied language constructs and concepts understanding BPMN will be chosen during the research process. Then has been conducted a survey in order to evaluate and confirm or deny our hypotheses regarding which modelling language is better understood by ordinary users. This allowed us to answer to our research question.

RQ: What modelling approach is most suitable for social engineering analysis?

In order to introduce different modelling approaches and their support with security risk management standards and methods, first of all, studied some existing standards and modelling approaches. In this paper also have been taken into consideration alignment of modelling languages with security risk method as the ISSRM domain model. We have selected one social engineering case and analysed it with BPMN, Misuse case and Secure Tropos. To understand what modelling approach is most suitable and understandable for social engineering analysis survey has been conducted. This led to the result that overall BPMN constructs and Secure Tropos concepts are preferred by users. Also based on collected results, we tried to make a parallel between understanding of concepts and constructs for participants. Percentage wise understanding of constructs showed higher results than concepts. *Business asset, IS asset, threat, attack method, risk treatment, security requirement and control* are easily identified in the form of constructs. Concepts are have received higher score in following aspects: *Business Asset, Security criterion, Impact, Event, Vulnerability, Threat, Threat agent, Security requirement*.

In conclusion, our analyses showed that security risk aware Secure Tropos is evaluated better regarding the concept recognition of security risk-oriented BPMN and Misuse cases. However the result is not significant. Similarly, we observe that security risk oriented /aware BPMN and Secure Tropos are rather equal (and better accessed than security risk oriented Misuse cases) regarding their construct recognition. But then again in different case study situation can change because of the subjectivity and the chosen case.

6.2 Limitations

The work reported in this thesis has several limitation. The limitations that were noticed are:

- The ISSRM domain model that was picked in Chapter 2 is one of the research assumption. However, it might interesting to take a look to other security risk methodologies and do a research using them.
- The study regarding methodological part on how to use models to support ISSRM has been started in Chapter 4. There is presented a limitation to the work which is based on usability of a modelling support for ISSRM.

- The conclusion that has been achieved is based on the evaluations that were limited due to specific chosen security risk methodology and modelling languages.
- In the comparison of modelling languages, only conceptual support has been presented. However, it might be necessary to consider metric level to have a full overview of the language.
- The validation is limited due to specific background of respondents and included threats to validity. They were highlighted in Chapter 5.
- The scope of this work is limited to only three modelling languages.

6.3 Future Work

The Contribution and the limitation of this work point out some open issues for further research:

- Validation of obtained results through further research. The extension proposed for modelling languages could be further validation by using metrics.
- Validation of the domain model through use of different standards and methods.

7 References

- AS/NZS4360, Australian/New Zealand Standard for Risk Management Standards Australia/ Standards New Zealand, 1999.
- Alberts, C.J. and Dorofee, A.J. (2001). *OCTAVE Method Implementation Guide Version 2.0*. Carnegie Mellon University- Software Engineering Institute.
- Altuhhova O., Matulevičius R. and Ahmed N., An Extension of Business Process Model and Notation for Security Risk Management. Estonia, 2012.
- AS/NZS 4360. Risk management. SAI Global, 2004.
- Andy Jones, Debi Ashenden., Risk Management for Computer Security: Protecting Your Network & Information Assets, 2005.
- Braber F.D., Hogganvik I., Lund M. S., Stolen K. and Vraalsen F. Model_based Security Analysis in seven steps-a guided tour to the CORAS method” BT Technology Journal, Volume 25 Issue 1, pages 101-117, 2007.
- Bresciani, P., Giorgini, P., Giunchiglia, F., Mylopoulos, J., and Perini, A. (2004). Tropos: an Agent-oriented Software Development Methodology. Journal of Autonomous Agents and Multi-Agent Systems, 8:203-236.
- BS7799-2, Information Security Management Systems - Specification with guidance for use (replaced by ISO27001): British Standards Institute (BSI), 1999.
- C. Alberts and A. Dorofee. Managing information security risks: The OCTAVE SM approach. Boston: Addison Wesley Anderson, 2003.
- Chowdhury M., Matulevičius R., Sindre G., Karpati., “ Alignment Mal-Activity Diagrams and Security Risk Management for Security Requirements Definitions”, rEFSQ 2012, LNCS 7195, Springer-Verlag Berlin Heidelberg., pp 132-139, 2012.
- Cherdantseva, Y., Hilton, J., & Rana, O. (2012). Towards SecureBPMN – Aligning BPMN with the information assurance and security domain. In *Proceedings of the 4th International Workshop, BPMN 2012* (pp. 107-115). Springer Heidelberg, LNBIP.
- Dhillon, G., and Backhouse, J. 2000. Information System Security Management in the New.
- Millennium. Communications of the ACM (43:7), pp125-128.
- Elahi, G. and Yu, E. (2007). A Goal Oriented Approach for Modelling and Analyzing Security Trade-Offs. In Parent, C., Schewe, K-D., Storey, V.C., and Thalheim, B., editors, *Proceedings of the 26th International Conference on Conceptual Modelling (ER 2007)*, volume 4801, pages 87-101. Springer Verlag Berlin Heidelberg.
- Ellie Myler, CRM, and George Bordbent. ISO17799: Standard for Security. p 44.

Folker den Braber, Ida Hogganvik, Mass Soldal Lund, ketil Stolen and Fredrik Vraalsen.

Model based security analysis in seven steps - a guided tour to the CORAS method. Vol. 25 (1) of BT Technology Journal, pages 101-17. Springer Verlag, 2007.

Gary Stoneburner, Alice Goguen and Alexis Feringa "Risk Management Guide for Information Technology Systems." National Institute of Standards and Technology Special Publication 800-30, 54 pages (July 2002).

Granger, Sarah, Social Engineering Fundamentals, available at web <http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-1-tactics>, 2001.

Hossein Bidgoli, John Wiley & Sons., Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management, 2006.

Horton, Thomas. Managing Information Security Risks.

Heidi E.I.Dahl, Ida Hogganvik and Ketil Stolen. Structure Semantics for the CORAS Security Risk Modelling Language. In proceedings of 2nd International Workshop on Interoperability Solutions on Trust, Security, Policies and QoS for Enhanced Systems (IS- TSPQ'07), pages 79-92. Helsinki University Printing House, 2007.

Ibrahiem M.M. El Emary, Mohammed H. Shalhoub, Mohammad J. Arif, Hassan A. Al-sereihy, Leena A. Shalhoub, Dr. Ing. Nars A. Al-Sahhaf "Social Engineering and its effective role in securing and defending the knowledge community", 2013.

ISO/IEC. Information technology-Security techniques-Information security risk management. ISO/IEC 27005:2011, 2011.

ISO/IEC. Information technology – code of practice for information security management. 17799.

ISO/IEC. Information technology-security techniques-management of information and communications technology security-Part 1: Concepts and models for information and communications technology security management. 2004. TR 13335-1.

ISO/IEC Guide 73. Risk management - Vocabulary - Guidelines for use in standards. International Organisation for Standardization, Geneva, 2002.

5. J.Moffett and B.A. Nuseibeh. A framework for Security Requirements Engineering. Department report, Department of Computer Science University of York, UK, 2003

Jake Kouns, Daniel Minoli, John Wiley & Sons. Information Technology Risk Management in Enterprise Environments: A review of Industry Practices and a Practical Guide to Risk Management Teams, 2011.

Kevin Roebuck., Risk Management Standards: High-impact Strategies- What You need to Know: Definitions, Adoptions, Impact, Benefits, Maturity, Vendors, 2012.

Matulevičius, R., Mayer, N., Mouratidis, H., Dubois, E., Heymans, P., and Genon, N. (2008b). Adapting Secure Tropos for Security Risk Management during Early Phases of the Information Systems Development. In Proceedings of the 20th International Conference on Advanced Information System Engineering (CAiSE2008). Springer-Verlag Berlin Heidelberg.

Matulevičius R., Mayer N., Heymans P., Alignment of Misuse Cases with Security Risk Management, IEEE Computer Society, 2008.

Mayer, N., Heymans, P., Matulevičius, R.: Design of a Modelling Language for Information System Security Risk Management. In: Proceedings of the First International Conference on Research Challenges in Information Science, RCIS 2007. pp. 121-132 (2007).

Mayer N., Model - Based Management of Information System Security Risk. Belgium, 2009.

Raimundas Matulevičius, Haralambos Mouratidis: “Syntactic and Semantic Extensions to Secure Tropos to Support Security Risk Management”, 2012.

Mitnick K. The art of deception — controlling the Human Elements of Security. Hungry Minds Inc., 2002.

Morgan Kaufmann, John R. Vacca., Computer and Information Security Handbook, 2009.

Mouratidis, H. and Giorgini, P. (2007a). Secure Tropos: A security-oriented Extension of the Tropos Methodology. International Journal of Software Engineering and Knowledge Engineering (IJSEKE), 17(2):285-309.

Mouratidis, H., Giorgini, P., and Manson, G. (2003a). Integrating Security and Systems Engineering Towards the Modelling of Secure Information Systems. In Proceedings of the 15th Conference on Advanced Information Systems Engineering (CAiSE'03), pages 63-78. Springer-Verlag.

Object Management Group (OMG). Unified Modelling Language: Superstructure, version 2.0, 2004.

Pauli, J.J., Xu, and D.: Trade-off Analysis of Misuse Case-based Secure Software Architectures: A Case Study. In: Proc. of MSVVEIS Workshop. Pp.89-95. INSTIL Press (2005).

Rodríguez, A., Fernandez-Medina, E., & Piattini, M. (2007a). A BPMN extension for the modeling of security requirements in business processes. [IEICE.]. *Transactions on Information and Systems*, 4, 745–752.

SANS Institute 2007. An Introduction to Information System Risk Management. pp.13.

Sindre, G., Opdahl, and A.L.: Eliciting Security Requirements with Misuse Cases. *Require. Eng.* 10(1), 34-44 (2005).

Zhihong Qian, Lei Cao, Weilian Su, Tingkai Wang, Huamin Yang., *Recent Advances in Computer Science and Information Engineering*, 2012.

Woznia, Steve and William, LSimon. (2004): *The Art of Deception: Controlling the Human Element of Security* (published by John Wiley and Sons).

Appendix

I. Social Engineering Cases

Case: Code breaking

An employee who is working on a contract has an access to procedures of transmission and the ability to observe the actions of other employees. Thus he learned that the bank employees received an everyday code. Employees receive every day new code that is not easy to remember. That is why they were recording it on a piece of paper and put it somewhere in sight. In this particular November day Rifkin walked into this room with a special visit. He wanted to look at this piece of paper. Entering the room, he fiddled a bit with his work, making sure that the backup system works correctly with the main system. Meanwhile, he quietly read and remember the code on sticky piece of paper. A few minutes later he came out. Leaving the room about 3 hours in the afternoon, he went straight to the pay phones in the marble lobby of the building, dropped a coin and dialed room for transfers. Then he changed his hat, transformed from Stanley Rifkin, bank consultant to Michael Hansen, an employee of the International Department of the Bank. Girl FPIC internal number. Rifkin heart skipped a beat, it was a question that he did not expect something slipped out of his attention during training. He said that the call back to check this number. He again changed his hat and called to another bank, this time, sounding an employee of the premises for transfers. He received a number and call again to the girl. Few days later Rifkin flew to Switzerland to take their money.

Table 20. Example of managing Code breaking security risk

Business asset	Daily code to each wire transformation, internal number
IS asset	Wire room, employees who receive daily code
Security Criterion	Confidentiality of received code, confidentiality of internal number, integrity of wire transformation process
Impact	Employees are not trusted, negation of basic security rules
Threat agent	A person who has an access to the wire room, knows the process of transaction and knows how to get missing information within that organization.
Attack method	Person worked in the targeted organization and based on observation of internal employees found a weakness of daily actions. Attacker got to the targeted room and took a look to the piece of paper with necessary information. He remembered it and then used it to transfer money from one account to another.
Security requirement	Security requirement Technologies like authentication devices (for proving identity), access control (for managing access to files and system resources), and intrusion detection systems (the electronic equivalent of burglar alarms) are necessary to a corporate security program.
Control	Deploying countermeasures to protect the organization

Case: The Engineer Tap

Lady decided to organize a raid on the cellular service provider to see whether it was possible to find there a few engineers who might be tempted to move to a competitor. She could not just call the communications center and say, "Let me talk to someone with five years of experience as an engineer." Instead, for obvious reasons, she began the hunt for talent to find pieces of information that seem very minor, information that people of companies say almost anyone who asked. First call: Registrar attacks, using the name Didi Sands, make a call to the corporate office by cell phone service. To provide themselves with fallback in case the call to the Transportation Department will not give what she was looking for, Didi also said that she wants to talk to the Department of Real Estate. And just as the registrar gave her the number. When Didi asked to connect it with the Transport, receptionist tried, but the line was busy. Then Didi asked for the third issue - the department works with the accounts - located in the corporate headquarters in Austin, Texas. Registrar asked him to wait and disconnected from the line. She told the security service that has received a suspicious phone call, and I thought that there is something strange. It was a small, but typical trouble everyday work registrar. After about a minute recorder back on line, the Accounting department looked the number and connected Didi. Second call: Peggy. Just chatted for a long time with someone wanting to be helpful, Didi acquired a number of settlement center, which she needed - one of those pieces of information that no one thinks to defend, because he can not represent any value to an outsider. The third call: Useful wrong number. She has started with a call to the Department for Real Estate, pretending to hit the wrong number. She stated that she was an employee who has lost his corporate directory, and asked if he was calling about a new copy. The man replied that the printed copy is already outdated, because all of this is available on the corporate website. Didi said she prefers to use a copy of the paper, and the man told her to call the Publisher, and then, perhaps, only to a little chat with sexy-sounding lady on the phone, looked up the number and helpfully gave her. The fourth call: Bart Publishers. She of said hard copy would be preferable, even if it is a bit dated. Barth said that she must fill out a form and send requisition emu. Didi said that she had no hand forms, and could not Bart kindly fill out the form for her? He agreed with not too much enthusiasm, and Didi told him the data. Rather than address the fictional contractor, she reported number that social engineers call reset mail, in this case, the mailing address of the company where her company rented mailboxes specifically for situations like this. Now instead of working with a shovel had to work hard handles: We needed a settlement center, who come by for delivery directory. Fine - Didi gave a settlement center for Thousand Oaks. Few days later when he arrived corporate directory, Didi found that he was even more awards than she had expected: It was not only a list of names and phone numbers, but also shows who is working for whom - the corporate structure of the whole organization.

Case: Number please

Offensive called the official telephone number of the company, in the center of the destination mechanized lines (Mechanized Line Assignment Center). The man who called, should be aware that information on unpublished rooms are available only to authorized persons. It is assumed that the center of the known only to employees of the company. And if the information is never made public, who could refuse to help the company's employees do the heavy work? She sympathized with him, it was the most difficult days at work, and she broke the rules a bit to help a colleague with a solution to the problem. She told him the current number and address for each of the cable pairs.

Table 21. Example of managing The Engineer Tap security risk

Business asset	Number of settlement center
IS asset	Employees, cellular service provider
Security Criterion	Integrity of department's phone numbers, confidentiality of phone numbers of departments
Impact	Loss of phone number
Vulnerability	Employee of the organization is not experienced to verify the caller
Threat agent	Caller who knows how to use phone system, get necessary phone number, whom and what to ask
Attack method	Caller by making several calls to different departments and finally got to publishing department. Attacker asked a copy of corporate directory and employee sent to delivery directory after a filled necessary form by himself.
Security requirement	To verify that the person really worked there and not provide phone number, especially internal
Control	Deploying countermeasures to protect the organization. Every company needs a written, well-publicized policy on disclosure of this type of information. The safeguards should include maintaining an audit log that records instances when sensitive information is disclosed to people outside of the company.

Case: Young man on the run

The man, whom we'll call Frank Parsons, was on the run for many years, while the federal wanted list for participation in the underground anti-war group in the 1960s. For people like Frank, with its advanced computer skills (skills and social engineer, although he never mentioned this when applying for) finding a good job is not usually a problem. Except in cases where the organization is limited in the media, people with good computer skills are usually in high demand and it is easy to settle. Frank quickly found a highly paid, permanent job near his home. Simply classified, he thought. But when he began to fill in the questionnaire, it was faced with a surprise. The employer is required to provide a copy of the applicant's criminal characteristics, which he had to bring himself out of the state police. A stack of documents include a form with place for fingerprints. Even if only the required impression of right index finger, but it would have been reconciled with the imprint of the FBI database, soon he would have to work in the food service federal prison (shelter). On the other hand, Frank had the idea that he could avoid it. Perhaps the fingerprint templates are not sent from the State of the FBI. To find out whether there are his fingerprints in the database he called the patrol of state. When answered the phone a local expert, Frank asked a series of questions about what system they use, the possibilities of research and storage of fingerprints. Were they a hardware problem? They are connected with a card file prints national information center or work within the state? Is the equipment easy enough for anyone who is trained using it? The answer was music to his ears: they are not linked to the

national center, they only reconciled to the criminal database state (Criminal Information Index).

Table 22. Example of managing number please security risk

Business asset	Information on unpublished rooms
IS asset	Employee, check of the destination mechanized lines
Security Criterion	Integrity of Information on unpublished rooms, confidentiality of Information on unpublished rooms
Impact	Negation of security requirements, Employee is not trusted
Vulnerability	Employee of the organization is not experienced to verify the caller
Threat agent	Caller who knows how to use phone system, how to get office phone number of the organization and gain trust of employee
Attack method	Caller who knows how to play on sympathy and get necessary information
Security requirement	Not provide private phone number
Control	Deploying countermeasures to protect the organization

Case: Gas Attack

Project Art Sealy. Art Sealy refused to work free editor, when opened, I could make more money by doing research for writers and commercial firms. He was contacted by a man who wrote a book on the cabinet during the reign of Nixon. He was looking for someone who could find the sensational news about William Simon (William E. Simon), the Minister of Finance. Mr. Simon died, but the author was named a woman who was in his state. He was sure that she lived in the District of Columbia, but could not find the address. To her name was not specified phone, or at least was not among those listed. So he called me. Sure, no problem, I told him. This work, which usually can be performed using one or two calls, if you know what you are doing. We can assume that each local utility company provides information beyond its limits. Of course, you have to lie a little.

Case: The first call- Andrea Lopez

Women in social engineering have a clear advantage due to the fact that they can use their sexuality to get to the cooperation. First Up: Andrea Lopez. Andrea Lopez responded to a phone call in the video box office, where she worked, and immediately smiled always nice when a client says good things about the service. The one who called and said that he had left a very good impression of the video rental service, and he wanted to send a letter to the manager, and report it. He asked the manager's name and postal address. Andrea told him that the manager is Tommy Allison, and gave the address. When the caller wanted to hang up, he had a different idea, write to the office and for that the mind needed to know the number of the store. The girl also gave him this information. He thanked added something nice about it, how useful was it, and said goodbye. Second call Ginny. The caller introduced

himself Tomy Alison store manager 863 in Forest Park. The reason for the call was a customer who wants to rent Rocky 5, but they do not have it in the store. She provided him with the necessary information. Three or four times over the next few weeks, Ginny received calls from Tommy to help in a particular case. These were the type of legitimate requests, and he was always very friendly, did not try to push strongly. He was very talkative. Once Tommy called and asked about problems with computers. Under this pretext Tommy gave the customer's name and address, and Ginny found it in the computer. She gave Tommy account number. Due to the fact that the client with him were no cards he asked them to learn from the database. She gave him the number, along with the expiration date.

Table 23: Example of Young man on the run security risk

Business asset	Criminal characteristics, documents including a form with place for fingerprints
IS asset	Police department's local expert, system that stores fingerprints
Security Criterion	Integrity of information stored in the system, confidentiality of information stored in the system
Impact	Police department's local expert is not trusted, negation of confidentiality of private information as criminal characteristics, documents including a form with place for fingerprints
Vulnerability	Employee of police department is not trusted
Threat agent	Caller who knows how to use phone system, get necessary phone number and gains a trust of employee
Attack method	Attacker called the patrol of state. A local expert answered to the phone. Frank asked a series of questions about what system they use, the possibilities of research, storage of fingerprints and received all necessary to him information.
Security requirement	Not provide private phone number
Control	Deploying countermeasures to protect the organization

Table 24. Example of gas attack security risk

Business asset	Address of the woman
IS asset	Employee of the organization
Security Criterion	Integrity and confidentiality of address or phone system of a person
Impact	Negation of confidentiality of caller, employee is not trusted
Vulnerability	Employee of the organization is not trusted to verify the caller
Threat agent	Caller who knows how to use phone system, get necessary phone numbers
Attack method	Attacker performs one or two phone calls and receives address of the woman
Security requirement	Security training with respect to company policy designed to protect information assets needs to be for everyone in the company, not just any employee who has electronic or physical access to the company's IT assets.
Control	Deploying countermeasures to protect the organization

Case: Doyle Lonnegan's story

Lonnegan - this is not the young man whom you would like to see when you open the front door. Former debt collector in gambling, he still does it sometimes. In this case, he was offered a large bag of cash in a few phone calls to the video store. Sounds simple enough. None of these "clients" did not know how to do the trick; They need someone with talent Lonnegan. People do not write checks to cover their debts when they were unlucky or they foolishly playing poker. That man had no money, so they took the check. At \$ 3,230. Naturally, he cheated. I do not close the door to the people who came to see me. In addition, currently there are better ways. I told them that my 30 percent commission, and I'll see what I can do. So they gave me his name, address, and I found in the computer next to him the video store. I'm not in a hurry. Four phone calls to the store manager, and then, bingo - I have a number of Visa card fraud.

Table 25. Example of first call-Andrea Lopez security risk

Business asset	Customer's name and address, account number, manager's name and postal address of the store, the number of the store
IS asset	Employees / Andrea & Ginny
Security Criterion	Integrity of account number of customer, confidentiality of account number of customer
Impact	Negation of authentication of the caller, Andrea & Ginny are not trusted
Vulnerability	Employees are not experienced to verify the caller
Threat agent	Caller who knows how to use phone system, get necessary phone numbers
Attack method	The one who called and said that he had left a very good impression of the video rental service, and he wanted to send a letter to the manager, and report it. He asked the manager's name and postal address, number of the store. All requested information was provided by an employee. Then attacker did second call to Ginny. The caller introduced himself Tommy Alison store manager 863 in Forest Park. The reason for the call was a customer who wants to rent Rocky 5, but they do not have it in the store. She provided him with the necessary information. Three or four times over the next few weeks, Ginny received calls from Tommy to help in a particular case. Once Tommy called and asked about problems with computers. Under this pretext Tommy gave the customer's name and address, and Ginny found it in the computer. She gave Tommy account number. Due to the fact that the client with him were no cards he asked them to learn from the database. She gave him the number, along with the expiration date.
Security requirement	Security training with respect to company policy designed to protect information assets needs to be for everyone in the company, not just any employee who has electronic or physical access to the company's IT assets.
Control	Deploying countermeasures to protect the organization

Table 26. Example of Doyle Lonnegan's Story security risk

Business asset	All information that attacker obtained in advance by calling to the store and gaining a trust of employee
IS asset	Employee
Security Criterion	Integrity to the valuable information
Impact	Required private information of the company received attacker
Vulnerability	Employee of the organization provided information as trusted to the attacker.
Threat agent	Required private information of the company received attacker
Attack method	Person called to the organization several times and obtained a trust as a colleague
Security requirement	Security training with respect to company policy designed to protect information assets needs to be for everyone in the company, not just any employee who has electronic or physical access to the company's IT assets.
Control	Deploying countermeasures to protect the organization

Case: Card Capture/Surprise for Daddy

During the conversation, Henry blamed his father in the distribution of the number of his credit card as if it was his phone number. He pulled out his cell phone, he asked his father how he uses the branch and call the assistant director as well as on the number of stores in nearby Sherman Oaks. Then, using only a slight change in technique, he asked to read the account information: address, telephone number, and the date when the account was opened. In conversation, he also asked the credit card number and expiration of due date. When conversation was finished, he put a towel in front of his father, who has watched it with my mouth open. Mr. Conklin looked completely shocked, as if his confidence just collapsed.

Table 27. Example of card capture security risk

Business asset	Account information, address, telephone number, the date when the account was opened, credit card number and its expiration of due date.
IS asset	Database of the store, employee.
Security Criterion	Integrity of account information, integrity of address, integrity of telephone number, integrity of the credit card number and its expiration of due date, confidentiality of account information, confidentiality of address, confidentiality of telephone number, confidentiality of the date when the account was opened, confidentiality of credit card number and its expiration of due date.
Impact	Negation of authentication of caller, employee is not trusted.
Vulnerability	Employee is not experienced to verify the caller.
Threat agent	Caller: who knows how to use cell phone, how to get necessary phone number, who knows where potential victim uses his card.
Attack method	Henry blamed his father in the distribution of the number of his credit card as if it was his phone number. He pulled out his cell phone, he asked his father how he uses the branch and call the assistant director as well as on the number of stores in nearby Sherman Oaks. Then, using only a slight change in technique, he asked to read the account information: address, telephone number, and the date when the account was opened. In conversation, he also asked the credit card number and expiration of due date. When conversation was finished, he put a towel in front of his father, who has watched it with my mouth open.
Security requirement	Security training with respect to company policy designed to protect information assets need to be for everyone in the company, not just any employee who has electronic or physical access to the company assets.
Control	Deploying countermeasures to protect the organization

Case: The one-cent cell phone

One social engineer in Philadelphia drew a cheap phone, cell phone company in the proposed contract, but he hated the tariff plans that were in the contract. First call: Ted. First, the social engineer calls in an electronics store in West Girard. Buyers who introduced a few days ago said the seller of cell phone, said he would call back. Call: Ketiye next call the store of the same company on North Broad Street. Given that the attacker knew the name of the seller, he introduced this time colleague and asked to take a client's action "cell phone for one cent." When the guy who called himself Ted Janes, will be in stores on the street North Broad St. Katie billed and sold cell phone for one cent, as her colleague asked. She caught the trick cheater. When it came time to pay, the buyer did not have a penny in his pocket, so he got to the small plates with small change at the cash register, took one, and

gave the girl behind the register. He received a phone without paying a single cent for it. Now he can go to another company that uses the same standard telephones and ordered another tariff plan without any contractual obligations.

Table 28. Example of the one cent cell phone security risk

Business asset	All information that attacked obtained in advance by calling to the store and gaining a trust of employee
IS asset	Employee
Security Criterion	Integrity to the valuable information
Impact	Required private information of the company received by attacker
Vulnerability	Employee of the organization provided information as trusted to the attacker
Threat agent	A person who gains a trust of employee
Attack method	Employee treats as innocuous
Security requirement	Security training with respect to company policy designed to protect information assets needs to be for everyone in the company, not just any employee who has electronic or physical access to the company's IT assets.
Control	Deploying countermeasures to protect the organization

Case: Hacking into the Feds/ Tapping into the system

Found a copy of the manual to gain access to the databases of the National Center of Information of crimes on the Internet. Later discovering really working guide NCIC, secret document, which allows to search for information from a national database FBI. Guide is a reference for the agencies of law enforcement agencies, which allows codes to search for information about criminals and crimes of the national database. Agencies across the country can find the same database for information to help in the fight against crime in their jurisdiction. The manual contains the codes used in the database starting with tattoos, ending marking the stolen money and commitment. Anyone with access to the leadership can find the syntax and commands to get the information from the national database. Then, follow the instructions from the manual, everyone can retrieve information from the database. Management also provides technical support telephone numbers in the system. You can have similar descriptions in your company offering product codes or codes for access to sensitive classified information. If the social engineer has such codes, that obtaining information for it easy process. In this example, it could start to call the local police department employee and ask questions regarding one of the codes in the manual for example, a code violation. He could, for example, saying "when I do a request to the NCIC, I get the error" System error ". You get the same thing as making a request? Could you try this for me? "Or it can be said that he tried to find a wpf police jargon file on the wanted individuals. An employee at the other end of the phone learns by jargon that the caller is familiar with the procedures and query commands to the database NCIC. After the employee

confirms that the system works well. The attacker only has to look at the base of NCIC, to learn the meaning of numbers: what crimes committed people.

Table 29. Example of hacking into the Feds security risk

Business asset	All information that attacker obtained in advance by a call
IS asset	Employee
Security Criterion	Integrity to the valuable information
Impact	Required private information of the company received attacker
Vulnerability	Employee of the organization provided information as trusted to the attacker
Threat agent	A person who gains a trust of employee
Attack method	Employee treats as innocuous
Security requirement	Employee needs to be trained to recognize social engineering scams
Control	Deploying countermeasures to protect the organization

Case: The Network Outage

Man of the breakdown called to the accounting department and was interested if they had a problem with the connection. Accountant politely replied that no, but the scammer gave his phone number on the special case. The last question asked as casually is to view the port number to which computer is connected. Second call: Man of maintenance. A few days later I received a call to the department LAN. Man of the technical department asked disable port 647. Man of the workshop said that it would be done in a few minutes, and asked him to call back when the need to enable the port. Third call: Help from the enemy. About an hour later, a man who introduced himself as Eddie Martin, was shopping at Circuit City and suddenly the telephone rang. He looked up the caller's number, learned that he was from the shipbuilding company. He asked for help. The fourth call was 45 minutes later. All connection was ok but for this issue in the future, suggested a scammer program. Eddy told Him how to download a small application with a single site. Once the program is downloaded, Eddie said to run it by doubleclick. He tried it and it turned out that the program does not work, in response to the fraudster helped and told how to delete the program permanently. (With a running program, Bobby gets full control of the computer Tom called remote command line. When connected to a PC Bobby Tom, he was able to see all the accounting files that may be of interest, and copy them. Then, for fun, he checked files for information that will give customers what they are looking for).

Table 30. Example of the networkd outage security risk

Business asset	All information that attacker obtained in advance by a call
IS asset	Employee
Security Criterion	Integrity to the valuable information
Impact	Required private information of the company received attacker
Vulnerability	Employee of the organization helped to run al necessary actions as trusted to the attacker
Threat agent	A person who gains a trust of employee
Attack method	Employee treats as innocuous
Security requirement	Employees need to be trained to recognize social engineering scams. If a stranger does you a favor, then asks you for a favor, don't reciprocate without thinking carefully about what he's asking for.
Control	Deploying countermeasures to protect the organization

Case: Craig Cogburne's Story

Craig Coborn was a salesman in a hightech company, and did his job very well. In search of work, he began to engage in industrial espionage. It was an urgent task. The client sent me a fax, a clipping from a medical journal, which said that GeminiMed working heart with fundamentally new structure, and it will be called STH100. Loud said this, some reporter has already done most of the work for me. He already had important information even before it started the name of the new product. To get information about employees who worked on STH100 or need watching his schemes. Telephone operator called and said he did not remember his name, and his name starts with "C". She said there's Scott

Archer and Sam Davidson. Then he asked next question is which of them is working on STH100. It turned out to Scott Archer. Caller introduced himself as Mike, from the mail department. They should get the parcel to a group of developers Artificial Heart STH100. He called me the name of the project manager, Jerry Mendel. I was even able to persuade him to see his room for me. Mendela was not there, but his answering machine said that he will be on vacation until the 13th, which meant that he had a whole week for skiing or anything else another, and in his absence can call Michelle on the phone 9137. The next call was introduced Michelle and Bill Thomas and called on Jerry. He began to ask and systems that they use and asked for an email list of people from the development team. The attacker wanted to get all the same fax, against what Michelle was not opposed. Secretary called and found room fax machine he got there the necessary documents. The receptionist kindly agreed to send data to another room, which an attacker sent to a company nearby. So had to talk to three or four different people in just a few hours, and already closer to the computers on a huge shag. First of all dialin number to the server from outside engineering. Called the GeminiMed again, and asked to be connected with the Department of IT, with someone who helps with the computer. phoned and found that they had set up a terminal server, which allows the caller to connect to any computer on their network. After heaps of attempts, I

came across someone's computer, where he was the guest account without having to enter a password. Some operating systems, when they are only installed, forcing the user to create a username and password, as well as provide a guest account. The user must supply your password on the guest account on or off it, but many do not even know about it or do not want anything to do. This system is most likely was just installed, and the owner did not even bother to disconnect the guest account. Thru guest account, I now have access to one computer, which was the old version of the operating system Unix. In Unix'e, the operating system contains a file which has encrypted passwords of everyone who has access to your computer. Password file contains oneway hash (ie, irreversible form of encryption) password of each user. With the hash, password, for example «justdoit» will be presented in an encrypted form; in this case, the hash will be converted to Unix in 13 numericalalphabetical characters.

Table 31. Example of Craig Cogrone's story security risk

Business asset	All information that attacker obtained in advance by a call
IS asset	Employee
Security Criterion	Integrity to the valuable information
Impact	Required private information of the company received attacker
Vulnerability	Employee of the organization helped to obtain all necessary information as trusted to the attacker
Threat agent	A person who gains a trust of employee
Attack method	Employee treats as innocuous
Security requirement	Employees need to be trained to recognize social engineering scams. Keep sensitive information safe
Control	Deploying countermeasures to protect the organization

Case: Keeping up with Joneses

Sales and other units located throughout the world, coupled with the headquarters of the company through a global network (WAN). Cracker named Brian (Brian Atterby), knew that almost always easier to network in one of the remotest places where the security level should be lower than in the main office. Cracker called to the office in Chicago and asked to be connected with Mr. Jones. They turned 3 Johnson. Attacker got to the division where he asked the desired Port .When Jones picked up the phone, the attacker said that he was in the section on transfer of wages. Jones was distraught at the thought that his money could go to someone's account, he began to think that the guy on the other end should not have to hurry. Before the victim began talking attacker immediately asked best room, for allegedly help. Business trip. Afterwards called System Administrator Sales in Austin, Texas. The caller introduced himself from the department of business development Joseph Jones. He needed access to email during business trip. Attacker carefully prepared and was ready to answer all the specific questions the system administrator.

Table 32. Example of Keeping up with Joneses security risk

Business asset	All information that attacker received to provide to the system administrator, port number
IS asset	Employee of the organization, access of email, global network (WAN)
Security Criterion	Integrity of all information that attacker received to provide to the system administrator, confidentiality of port number, confidentiality of all information that attacker received to provide to the system administrator
Impact	Negation of authentication of caller, employees in Chicago & Jones are not trusted
Vulnerability	Employees in Chicago, Jones & system administrator sales in Austin, Texas are not experienced to verify the caller
Threat agent	Caller (Brian): who knows how to use cell phone, knows weakness in global networks, knows divisions of the organization, knows how to get correct phone number.
Attack method	Cracker called to the office in Chicago and asked to be connected with Mr. Jones. Attacker got to the division where he asked the desired Port. Attacker immediately asked best room. Afterwards called System Administrator Sales in Austin, Texas. The caller introduced himself from the department of business development Joseph Jones. He needed access to email during business trip. Attacker carefully prepared and was ready to answer all the specific questions the system administrator.
Security requirement	Employees need to be trained to recognize social engineering scams. Keep sensitive information safe.
Control	Deploying countermeasures to protect the organization. Every company needs a written, well-published policy on disclosure of this type of information.

Case: I saw it at the movies

An example from the famous film that many people remember. In "Three days of the Condor" protagonist Turner (the role played by Robert Redford) is working with a small research firm under contract to the CIA. Once he returned from lunch and discovers that all his employees were shot. He had to find out who did it and why, knowing that at this time the bad guys are looking for him. Later he managed to find the phone number of one of the guys. But who he is and how to find it? He was lucky: screenwriter, David Ralph, fortunately, provided him with experience that includes training in the Signal Corps, which gives him an idea of the telephone companies. With the number of Man, Turner knows exactly what to do further. Turner, thanks to the experience lineman knows what number it is necessary to call the office of the company, which is called "Hour of names and

addresses." Customer names and addresses of subscribers is for the convenience of installers and other personnel of the company. The installer can call customer service and call the number. The clerk will report the name and address of the person who owns the phone.

Table 33. Example of I saw it at the movies security risk

Business asset	Customer names and addresses.
IS asset	Clerk, The Singal Corps.
Security Criterion	Integrity of customer names and addresses, confidentiality of customer names and addresses, availability of customer names and addresses.
Impact	Negation of authentication of caller, clerk is not trusted.
Vulnerability	Lineman experience.
Threat agent	Caller: who has a lineman experience, knows how to use cell phone, knows how to get customer service number.
Attack method	Attacker knows what number it is necessary to call the office of the company, which is called "Hour of names and addresses." Thanks to received information caller contacts with customer service and calls the number. The clerk will report the name and address of the person who owns the phone.
Security requirement	Employees need to be trained to recognize social engineering scams. Keep sensitive information safe.
Control	Deploying countermeasures to protect the organization. Every company needs a written, well-published policy on disclosure of this type of information.

Case: Danny the Eavesdropper

Scanning enthusiast and skilled hackers who we'll call Danny decided to see if he could get the source code of a topsecret program interposer one of the leading manufacturers of secure radio systems. Danny wanted to examine the items carefully guarded company's product just to satisfy a burning curiosity and wonder clever innovations that could be implemented in the company. Danny began with careful preparation. Soon he gathered together enough information to impersonate this employee. He had a name, department, phone number, employee, and the name and telephone number of the head. Now it was the calm before the storm. On scheduling Danny needed was one more thing before you take the next step, and it was something he did not manage: he needed a blizzard. He needed help from a nature in the form of weather, which would not allow workers to reach office. At the beginning of Friday night snowstorm. Snow quickly turned to hail, so that in the morning the roads were covered with ice. It was a great opportunity for Danny. He called on the plant, ask for the engine room and contacted the operator, who introduced himself as Roger Kowalski. Calling the name of the employee, Danny said that he was working in a group protected connections. Problem was that I need access to my computer and the server from home, and I left a secure ID in the table. Given that the operator she could Pokuna their workplace attacker asked to

borrow a secure ID, when he will need to enter the network. The operator was not ready to give access immediately. He called his boss and asked his permission. So on the weekend, every time Danny wanted to enter into a corporate network, he had only to call the computer center and ask to consider the six digits displayed safe ID. As Danny entered keywords "encrypted radio" and the name of the company, and found a message from a year ago an employee. It was placed, when the company began developing a product, perhaps long before the police authorities and federal authorities took control of the radio signals. Message containing a digital signature, which gives not only a person's name, Scott Press, but his phone number and even the name of the working group, the Group of secure communications. He introduced himself as an employee of IT department. Danny got the press to name the servers used for development. These servers can store source code containing proprietary encryption algorithm and the firmware used in the security product of company. On the rest of the weekend he could enter into the company's network when he'd wanted to, thanks to the cooperation with the head of the computer center. He knew how to apply servers. But when he dialed the number, the terminal server, for which he came, he did not allow connection to the development of the Group's secure communications. It was an internal firewall or router, the protected computer systems group. We had to find another way to enter. The next step was the hold of an account on one of the computers to use Telnet to connect to my system. Head has approved the disclosure of access code displayed on synchronized tokens, so the new requirement does not seem excessive. Kowalski created a temporary account and password on one of the computers, the computing center and asked Danny "call when the account is no longer needed, so I deleted it." Going with a temporary account, Danny was able to connect over the network to the computer systems of the Group secure communications. After hours of searching vulnerabilities, which gave him access to the main server, he hit the jackpot. Obviously, the system administrator has followed the latest news about security bugs that allowed remote access. But Danny was well aware of this. In a short time he found the source files and send them to a site that provides free storage space. Here, even if the files have been found on his trail could never get out. Before leaving there was one final step: the systematic destruction of their *tracks*.

Case: Phony sites and dangerous attachments

Once you get a letter from a friend or business partner that contains the application. After all, cannot be something dangerous to come from someone you know, is not it? Especially if you know who to blame, if the information on your computer was damaged. You run the file and ... BOOM! Your computer has just been infected with a worm or a Trojan.

Case: Merry Christmas

Happy New Year ... A retired insurance salesman named Edgar received an email from PayPal, a company that provides a fast and convenient way of committing online shopping. This kind of service is very handy when a person from one part of the country (or the world) to buy anything from a person with whom he is not familiar. PayPal will charge the buyer's credit card and transfer money directly to the seller. As a collector of antique glass mugs, Edgar made many transactions through online auction eBay. He often used PayPal, sometimes several times a week. In general, Edgar was interested in receiving emails on weekends, 2001, which seemed to have been sent from someone on PayPal, offers him a reward for his PayPal account updates. He clicked on the link, fill out the information request name, address, phone number, credit card information and sat down to wait, when \$ 5 will go to his account. But instead, began to appear on the list of expenditure items, that he never ordered.

Table 34. Example of Danny the Eavesdropper security risk

Business asset	Source code of a program, name, department, phone number, employee, and the name and telephone number of the head.
IS asset	Employee.
Security Criterion	Integrity and confidentiality of source code of a program, name, department, phone number, employee, and the name and telephone number of the head.
Impact	Employee is not trusted
Vulnerability	Employee is not experienced to verify the caller
Threat agent	Caller: how knows how to use cell phone, how to get some information in advance.
Attack method	Attacker obtained some information in advance. Snowy day allowed him to call to the targeted company and pretend that he is an employee. Problem was that he need access to my computer and the server from home, and I left a secure ID in the table. After some talking with employees he got an access to the server. Finally he used his technical skills and got necessary information.
Security requirement	Employees need to be trained to recognize social engineering scams
Control	Deploying countermeasures to protect the organization

Case: A visit to the Studio

Talk a way into places that You would not have thought possible. First of all did some research , for a couple of days. Wrote down names, products, different studios from the information in magazines. Called to the Ron Hillyard's office and told that he is his colleague and came on board to work. He has a writer to come this evening and do not know how to receive an entrance. He doesn't want to bother Biran's office. Right touch to her and she helped with an information for a further research (by providing name and information of Security people). Victim himself gave a correct phone number and told whom to ask, so that person can help.

Table 35. Example of Phony sites and dangerous attachments security risk

Business asset	Letter from a friend or business partner.
IS asset	User, letter.
Security Criterion	Integrity of the letter from a friend or business partner, confidentiality of the letter from a friend or business partner, availability of the letter from a friend or business partner.
Impact	Letter from a friend or business partner is not trusted.
Vulnerability	User is not experienced to verify and identify vulnerable sender of the letter.
Threat agent	Sender of the letter: who knows how to gain trust of user, how to compose a letter, how to send a letter, how to infect a letter with a worm or a Trojan.
Attack method	Attacker send a letter from a friend or business partner that contains the application. You run the file and ... BOOM! Your computer has just been infected with a worm or a Trojan.
Security requirement	User needs to be trained to recognize social engineering scams
Control	Deploying countermeasures to protect the computer, inform the user not to open suspicious files

Case: Do it now

Linda moved out from a boyfriend. To revenge him she called him on least pleasant time which was around 11.00 on Saturday night, but he had changed his phone number. The new one was unlisted. As she worked before at the phone company she had an idea how to get a phone. From previous job left one repair ticket from one when there was a problem and printout listed the cable and pair for his phone. She still had the same pair of copper wires running from her house to the telephone company switching office. Knowing targeted cable & pair, the only thing that she wanted to find out the phone number. Based on location and nearby COs and to force worker to quickly help based on emergency situation. Worker went to Webster CO, checked cables, and did line verification. What Linda wanted to get the phone number.

Table 36 Example of Merry Christmas security risk

Business asset	Information about name, address, phone number, credit card information.
IS asset	Edgar, PayPal system.
Security Criterion	Integrity of information about name, address, phone number, credit card information; confidentiality of information about name, address, phone number, credit card information; availability of information about name, address, phone number, credit card information.
Impact	Email from the PayPal is not trusted, negation of authentication of received email.
Vulnerability	User is not experienced to verify the email.
Threat agent	Attacker who knows how to send fake emails from PayPal.
Attack method	User received an emails, which seemed to have been sent from someone on PayPal, offers him a reward for his PayPal account updates. He clicked on the link, fill out the information request name, address, phone number, credit card information and sat down to wait, when \$ 5 will go to his account. But instead, began to appear on the list of expenditure items that he never ordered.
Security requirement	User needs to be trained to recognize social engineering scams
Control	Deploying countermeasures to protect the computer, inform the user not to open suspicious files

Table 37. Example of A visit to the Studio security risk

Business asset	Correct phone number and information whom to ask.
IS asset	Employee.
Security Criterion	Integrity of correct phone number, confidentiality of correct phone number.
Impact	Employee is not trusted, negation of authentication of caller.
Vulnerability	Employee is not experienced to verify the caller.
Threat agent	Caller: who knows how to use phone system, how to do some research.
Attack method	Caller called to the office and told that he needs an invitation to this evening. He doesn't want to bother Biran's office. Right touch to employee and she gave a correct phone number and told whom to ask, so that person can help.
Security requirement	To verify that the person really works there.
Control	Your employees are truly conscientious about stopping anyone with or without a visitor's badge who is on his own, and questioning him. If the answers aren't satisfactory, your employees have to be willing to contact security.

Case: Mr. Bigg wants it

Name dropping. Attacker played on urgency and told that they haven't received report from them (whom called). They need it immediately as tomorrow they have to present their work. They will have to work all night in order to meet deadline. Pushed to the person who responded a call because he is on a lower level in the company.

Table 38. Example of Do it now security risk

Business asset	Repair ticket, printout listed the cable and pair for his phone.
IS asset	Employee.
Security Criterion	Integrity of repair ticket, integrity of listed the cable and pair for this phone, availability of repair ticket, availability of listed the cable and pair for his phone.
Impact	Negation of authentication of caller, employee is not trusted.
Vulnerability	Employee of the organization is not experienced to verify the caller.
Threat agent	Caller: who worked before at the phone company and has an idea how to get a phone; has left one repair ticket, printout listed the cable and pair for his phone.
Attack method	Attacker still had the same pair of copper wires running from her house to the telephone company switching office. Knowing targeted cable & pair, the only thing that she wanted to find out the phone number. Based on location and nearby COs and to force worker to quickly help based on emergency situation. Worker went to Webster CO, checked cables, and did line verification.
Security requirement	Companies need to prepare for social engineering attacks from current or former employees who may have an axe to grind. Background checks may be helpful to weed out prospects who may have a propensity toward this type of behavior. But in most cases, these people will be extremely difficult to detect. The only reasonable safeguard in these cases is to enforce and audit procedures for verifying identity, including the person's employment status, prior to disclosing any information to anyone not personally known to still be with the company.
Control	Deploying countermeasures to protect the organization

Table 39. Example of Mr Bigg wants it security risk

Business asset	Report.
IS asset	Employee.
Security Criterion	Integrity of report, availability of report, confidentiality of report.
Impact	Negation of authentication of caller, employee is not trusted.
Vulnerability	Employee is not experienced to verify the caller.
Threat agent	A caller: who knows how to use a cell phone, how to get a correct phone number, knows the structure of the organization.
Attack method	Attacker played on urgency and told that they haven't received report from them (whom called). They need it immediately as tomorrow they have to present their work. They will have to work all night in order to meet deadline. Pushed to the person who responded a call because he is on a lower level in the company.
Security requirement	People must be trained that it's not only acceptable but expected to challenge authority when security is at stake. Information security training should include teaching people how to challenge authority in customer-friendly ways, without damaging relationships. Moreover, this expectation must be supported from the top down. If an employee is not going to be backed up for challenging people regardless of their status, the normal reaction is to stop challenging--just the opposite of what you want.
Control	Deploying countermeasures to protect the organization

Case: What the social security administration knows about you

Accountant Mary Harris received a phone call from a company who does tech support to her firm. Based on the callers information many people in the office troubleshoot, so he wants to run couple of tests with her. She had to log into her computer and tell him, what she was typing. She told her ID, password. "Tech support" told that it is her private info and she doesn't have to tell it anybody. He on his screen will see just asterisks. She can let him know when computer will start up. He installed update to change her password and asked her to use that tool. For the first password he asked to use "test123". He worked through again of disconnecting from the server, then again connected (with a new password). Afterward they changed to original one. He was very pleased and she thanked him. (He installed a program that allows him to access the company's computer system whenever he wanted, by using his own password). The aim of this trick is to receive an access to other contracts and to help Alice. She wanted to receive a job in that company but wasn't sure that conditions are good (comparing with others).

Table 40. Example of what the social security administration knows about you security risk

Business asset	ID, password.
IS asset	Accountant (Mary Harris), server.
Security Criterion	Integrity of ID, integrity of password, confidentiality of ID, confidentiality of password.
Impact	Negation of authentication of caller, accountant is not trusted.
Vulnerability	Accountant is not experienced to verify the caller.
Threat agent	Caller: who knows how to use cell phone, how to get correct phone number, how to install update, how to disconnect and connect to server.
Attack method	Accountant Mary Harris received a phone call from a company who does tech support to her firm. Based on the callers information many people in the office troubleshoot, so he wants to run couple of tests with her. She had to log into her computer and tell him, what she was typing. He installed update to change her password and asked her to use that tool. For the first password he asked to use "test123". He worked through again of disconnecting from the server, then again connected (with a new password). Afterward they changed to original one.
Security requirement	Employees need to be trained to recognize social engineering scams. The premise is to trigger an automatic response based on psychological principles, and rely on the mental shortcuts people take when they perceive the caller as an ally.
Control	Deploying countermeasures to protect the organization

Case: The police raid

The government has been trying to lay a trap for a man named Arturo Sanchez, who has been distributing movies free over the Internet. The Hollywood studios say he's violating their copyrights, he says he's just trying to nudge them to recognize an inevitable market. Arturo came home late one night and learned that there was indeed a police raid in the building. He checks his apartment. The bad news is that there's a paper from the police requiring that he call immediately and set up an appointment for an interview within three days. The worse news is that his computers are missing. Arturo satisfied his need to know like this: To start with, he got the phone number for a nearby copy store, called them, and asked for their fax number. Then he called the district attorney's office, and asked for Records. When he was connected with the records office, he introduced himself as an investigator with Lake County, and said he needed to speak with the clerk who files the active search warrants. After a small talk he asked a clerk to fax all documents on this case. As on the police office they didn't have a fax machine, she was ready to help and from Clerk's office to send fax. In Clerk's office lady asked who will pay to this service. She needed accounting code. To receive it he called to the DA's office and asked receptions. She gave him account code without hesitation. The he called back to the Clerk's office and

provided accounting number. That also gave a good excuse to manipulate the lady in the further. After several calls to the store, he finally received documents. Then he called to the Clerk's office and told that they can throw them away. They are not necessary anymore. By obtaining all info he knew that police is after him and crossed the state line.

Table 41. Example of the police raid security risk

Business asset	Movies, documents of his case.
IS asset	Clerk's office, fax number, district attorney's office, records office, accounting number.
Security Criterion	Integrity of movies, confidentiality of movies, integrity of documents of his case, confidentiality of documents of his case.
Impact	Negation of authentication of caller, Clerk's office is not trusted, district attorney's office is not trusted, records office is not trusted.
Vulnerability	Clerk's office, district attorney's office & records office employee is not experienced to verify the caller.
Threat agent	Caller: who knows how to use cell phone, how to get correct phone number.
Attack method	Attacker got the phone number for a nearby copy store, called them, and asked for their fax number. Then he called the district attorney's office, and asked for Records. When he was connected with the records office, he introduced himself as an investigator with Lake County, and said he needed to speak with the clerk who files the active search warrants. After a small talk he asked a clerk to fax all documents on this case. As on the police office they didn't have a fax machine, she was ready to help and from Clerk's office to send fax. In Clerk's office lady asked who will pay to this service. She needed accounting code. To receive it he called to the DA's office and asked receptions. She gave him account code without hesitation. The he called back to the Clerk's office and provided accounting number. That also gave a good excuse to manipulate the lady in the further. After several calls to the store, he finally received documents. Then he called to the Clerk's office and told that they can throw them away. They are not necessary anymore. By obtaining all info he knew that police is after him and crossed the state line.
Security requirement	Employees need to be trained and to pay attention on daily decisions when providing information.
Control	Deploying countermeasures to protect the organization

Case: The art of friendly persuasion

Vince Cappelis has received a task to receive information about Joe Markowitz's bank account savings / situation. First of all he needed branch number of that department. One call and information obtained right from the bank. Second step, call to Angela and knows that she leaves at 12:30 to lunch. Third one is to Louis Halpburn. Attacker introduced himself as Neil Wenster from department 3182, who wants to talk with Angela. He needs to send information about a client urgently, so as verification & safety measures asks to B (be) no, not E. That way he received 2 codes. Next call is to Walter. He asks to give code C, but attacker found an excuse and asks to request code B or E. After some time attacker received fax with sig card. One more call gave me the 800 number that customers use for the automated service where an electronic voice reads you off the information you ask for. From the sig card, he had all of target's account numbers and his PIN number, because that bank used the first five or last four digits of the social security number. Pen in hand, he called the 800 number and after a few minutes of pushing buttons, he had the latest balance in all four of the guy's accounts, and just for good measure, his most recent deposits and withdrawals in each.

Case: Cops as Dupes

One particular social engineer--Eric Mantini. Eric figured it was unnecessarily increasing his risk to call the Department of Motor Vehicles (DMV) and go through the same ruse time after time whenever he needed that information. He wondered whether there wasn't some way to simplify the process. He did it by taking advantage of a service provided by his state's Department of Motor Vehicles. Many state DMVs (or whatever the department may be called in your state) make otherwise-privileged information about citizens available to insurance firms, private investigators, and certain other groups that the state legislature has deemed entitled to share it for the good of commerce and the society at large. In the state Eric then lived in, the required identification was a Requestor Code issued by the DMV, along with the officer's driver's license number. He wanted to pretend as a cop, so he started to investigate and get as much information as possible. First call: asked for the phone number of DMV headquarters in the state capitol. He then called a nearby sheriff's station and asked for Teletype--the office where communications are sent to and received from other law enforcement agencies, the national crime database, local warrants, and so forth. When he reached Teletype, he said he was looking for the phone number for law enforcement to use when calling the DMV state headquarters. So Eric now had the special phone number for law enforcement officers to call the DMV. He called the state Telecommunications Department and claimed he was from Nortel, the manufacturer of the DMS-100, one of the most widely used commercial telephone switches. To defend against outside intruders, commercial switches of this type are password-protected, just like every corporate computer network. Any good social engineer with a phonephreaking background knows that Nortel switches provide a default account name for software updates: NTAS (the abbreviation for Nortel Technical Assistance Support; not very subtle). He found out a password and got an access to the line as an automated user. He picked line number eighteen in the sequence, and entered the code that added call. When copes forwarding to that line. For the call-forwarding number, he entered the phone number of his new, cheap, prepaid cell phone. That way he started to collect all information from cops. After taking calls for a few hours and obtaining dozens of requestor codes, Eric dialed into the switch and deactivated the call forwarding.

Table 42. Example of the art of fiendly persuasion security risk

Business asset	Branch number, codes, sig card, account number, pin number, social security number.
IS asset	Employee, bank account's information.
Security Criterion	Integrity of branch number, integrity of codes, integrity of sig card, integrity of account number, integrity of pin number, integrity of social security number, confidentiality of branch number, confidentiality of codes, confidentiality of sig card, confidentiality of account number, confidentiality of pin number, confidentiality of social security number.
Impact	Negation of authentication of caller, employee is not trusted.
Vulnerability	Employee is not experienced to verify the caller.
Threat agent	Caller knows how to use cell phone, how to get correct phone number, know the structure and process in bank.
Attack method	First of all he needed branch number of that department. One call and information obtained right from the bank. Second step, call to Angela and knows that she leaves at 12:30 to lunch. Third one is to Louis Halpburn. Attacker introduced himself as Neil Wenster from department 3182, who wants to talk with Angela. He needs to send information about a client urgently, so as verification & safety measures asks to B(be) no, not E . That way he received 2 codes. Next call is to Walter. He asks to give code C, but attacker found an excuse and asks to request code B or E. After some time attacker received fax with sig card. One more call gave me the 800 number that customers use for the automated service where an electronic voice reads you off the information you ask for. From the sig card, he had all of target's account numbers and his PIN number, because that bank used the first five or last four digits of the social security number. Pen in hand, he called the 800 number and after a few minutes of pushing buttons, he had the latest balance in all four of the guy's accounts, and just for good measure, his most recent deposits and withdrawals in each.
Security requirement	Make some kind of validation technique before providing valuable information
Control	Properly trained, the character in the first story in this chapter would not have had to rely on his instincts, easily overcome, when asked to give a security code to a stranger. Verbal security codes are equivalent to passwords in providing a convenient and reliable means of protecting data. But employees need to be

	knowledgeable about the tricks that social engineers use, and trained not to give up the keys to the kingdom.
--	---

Case: Hacking behind bars

One of the grifters, Charles Gondorff was tossed into a correctional center near San Diego. His pal Johnny Hooker knew that Charlie was going to need a defense attorney. The money for a good lawyer would have to come from running another scam. He'd wanted to get in touch with Gondorff anyway. After a couple of tossing-and-turning nights brainstorming a plan, Johnny woke up one mornng with the whole thing laid out in his mind, in five steps. First, he'd find out the phone numbers for those ten direct-connect telephones to the PDO. He'd have all ten changed so that the phones would allow incoming calls. He'd find out which housing unit Gondorff was on. Then he'd find out which phone number went to that unit. Finally, he'd arrange with Gondorff when to expect his call, without the government suspecting a thing.

Case: The speedy download

Ned Racien owned his business. One of his clients was very successful accounting firm that specialized in mergers and acquisitions. They hadn't used Ned for long, just long enough for him to realize they were involved in deals that, once they hit the newspapers, would affect the stock price of one or two publicly traded companies. He knew a man, who knew a man, who was wise about things not exactly in the mainstream. The man listened to the plan, got fired up and agreed to help. For a smaller fee than he usually charged, against a percentage of Ned's stock market killing, the man gave Ned instructions on what to do. He also gave him a handy little device to use, something brand-new on the market. For a few days in a row Ned kept watch on the parking lot of the small business park, where the accounting company had its unpretentious, storefront-like offices. Most people left between 5:30 and 6. By 7, the lot was empty. The cleaning crew showed up around 7:30. Perfect. On one of the evenings, he knocked to the door and showed in the office as a worker. The man unlocked the door, locked it again behind Ned, and then went down the corridor turning on lights, so Ned could see, where he was going. And why not--he was being kind to one of the people who helped put food on his table. Or so he had every reason to think.

Case: Easy Money

Author (attacker) distracted the woman, chatting her up. Meanwhile Vinny, out of her sight line, had gone to work.

Vinny, squatting down at the back of the booth, so he couldn't be seen, picked the lock on the cabinet that housed their PDP-11 minicomputer and the cable terminations. Vinny plugged the cable leading from the console port into one of the terminals on the show floor. Because the LOCK-11 software now identified that attacker was logging in from an authorized terminal, it granted me access, and attacker was connected with system administrator privileges. Attacker patched the operating system by changing it, so that from any of the terminals on the floor, I would be able to log in as a privileged user. Attacker did a directory listing, to find out what files were on the computer, looking for the LocK-11 program and associated files and stumbled on something attacker found shocking: a directory that should not have been on this machine. The developers had been so overconfident, so certain their software was invincible, that they hadn't bothered to remove the source code of their new product. Moving to the adjacent hard-copy terminal, attacker

Table 43. Example of cops aa dupes security risk

Business asset	Requestor code, driver's license number, phone number of DMV, account name, password, special phone number for law enforcement officers.
IS asset	Employees, DMV, DMS-100
Security Criterion	Confidentiality of requestor's code, confidentiality of driver's license number, confidentiality of phone number of DMV, confidentiality of account name, confidentiality of password, confidentiality of special phone number of law enforcement officers.
Impact	Negation of authentication of caller, employee is not trusted.
Vulnerability	Employee is not experienced to verify the caller.
Threat agent	Caller knows how to use cell phone, how to get necessary phone number, knows about telephone switches.
Attack method	<p>First call: asked for the phone number of DMV headquarters in the state capitol. He then called a nearby sheriff's station and asked for Teletype--the office where communications are sent to and received from other law enforcement agencies, the national crime database, local warrants, and so forth. When he reached Teletype, he said he was looking for the phone number for law enforcement to use when calling the DMV state headquarters. So Eric now had the special phone number for law enforcement officers to call the DMV. He called the state</p> <p>Telecommunications Department and claimed he was from Nortel, the manufacturer of the DMS-100, one of the most widely used commercial telephone switches. To defend against outside intruders, commercial switches of this type are password-protected, just like every corporate computer network. Any good social engineer with a phone-phreaking background knows that Nortel switches provide a default account name for software updates: NTAS (the abbreviation for Nortel Technical Assistance Support; not very subtle). He found out a password and got an access to the line as an automated user. He picked line number eighteen in the sequence, and entered the code that added call. When copes forwarding to that line. For the callforwarding number, he entered the phone number of his new, cheap, prepaid cell phone. That way he started to collect all information from cops. After taking calls for a few hours and obtaining dozens of requestor codes, Eric dialed into the switch and deactivated the call forwarding.</p>
Control	At the very least, the employee should record the caller's name, phone number, and office or department, and then hang up. Before calling back he should verify that the organization really does have

	an employee of that name, and that the call back phone number matches the phone number in the on-line or hard-copy company directory.
--	---

Table 44.Example of hacking behind bars security risk

Business asset	Phone numbers of the necessary <i>unit, number</i> for the RCMAC
IS asset	PDO, employee of correctional center
Security Criterion	Confidentiality of phone numbers of the necessary unit, confidentiality of number for the RCMAC, integrity of phone numbers of the necessary unit, integrity of number for the RCMAC.
Impact	Employee is not trusted, negation of authentication of caller.
Vulnerability	Employee is not experienced to verify the caller.
Threat agent	Caller, who knows how to use cell phone, how to get correct phone number, knows how to change the phone system.
Attack method	First, attack found out the phone numbers for those ten direct-connect telephones to the PDO. He'd have all ten changed so that the phones would allow incoming calls. He'd <i>found</i> out which housing unit Gondorff was on. Then he'd <i>found</i> out which phone number went to that unit. Finally, he'd arranged with Gondorff when to expect his call, without the government suspecting a thing.
Control	At the very least, the employee should record the caller's name, phone number, and office or department, and then hang up. Before calling back he should verify that the organization really does have an employee of that name, and that the call back phone number matches the phone number in the on-line or hard-copy company directory.

started printing out portions of the source code onto the continuous sheets of the green-striped computer paper used in those days.

Case: The misleading caller ID

Linda Hill's phone rang just as she was in the middle of writing a memo to her boss. She glanced at her caller ID, which showed that the call was from the corporate office in New York, but from someone named Victor Martin--not a name she recognized. She picked up the phone and the caller introduced himself and said he was from PR, and working on some material for the CEO. He needs the top-line financials for the current quarter & his financial projections on the Apache project. She sent the fax a few minutes later. But Victor did not work for the PR department. In fact, he didn't even work for the company.

Table 45. Example of speedy download security risk

Business asset	Login, password, USB
IS asset	Database of the accounting company, employee
Security Criterion	Confidentiality of login, confidentiality of password, integrity of USB.
Impact	Employee is not trusted, negation of authentication of an entering person.
Vulnerability	Employee is not experienced to verify an entering person.
Threat agent	Person who entreated to the building, who knows companies timetable.
Attack method	For a few days in a row Ned kept watch on the parking lot of the small business park, where the accounting company had its unpretentious, storefront-like offices. Most people left between 5:30 and 6. By 7, the lot was empty. The cleaning crew showed up around 7:30. Perfect. On one of the evenings, he knocked to the door and showed in the office as a worker. The man unlocked the door, locked it again behind Ned, and then went down the corridor turning on lights, so Ned could see, where he was going.
Control	Deploying countermeasures to protect the organization

Case: The president of the United States is calling

As co-host of a radio show in Los Angeles called "Dark side of the Internet" on KFI Talk Radio, I worked under the station's program director. David, one of the most committed and hardworking people I've ever met, is very difficult to reach by telephone because he's so busy. He's one of those people who doesn't answer a call unless he sees from the caller ID that it's someone he needs to talk to. I talked over what to do about this with a long-time friend, who is the cofounder of a real estate firm that provides office space for high-tech companies. Together we came up with a plan. He had access to his company's Meridian telephone switch, which gives him the ability to program the calling party number, as described in the previous story. Whenever I needed to reach the program director and couldn't get a call through, I would ask my friend to program any number of my choosing to appear on the caller ID. Sometimes I'd have him make the call look as if it was coming from David's office assistant, or sometimes from the holding company that owns the station. But my favorite was programming the call to appear from David's own home telephone number, which he always picked up. H1 give the guy credit, though. He always had a good sense of humor about it when he'd pick up the phone and discover I had fooled him once again.

Table 46.Example of Easy money security risk

Business asset	<i>Console</i> port, terminal, LOCK-11 software, source code.
IS asset	Woman (employee), show floor
Security Crite- rion	Integrity of console port, integrity of terminal, confidentiality of LOCK-11 software, integrity of LOCK-11 software, confidentiality of source code.
Impact	Woman is not trusted.
Vulnerability	Employee is not experienced.
Threat agent	Attackers: one of which distracted the woman, second one has technical skills.
Attack method	Author (attacker) distracted the woman, chatting her up. Meanwhile Vinny, out of her sight line, had gone to work. Vinny, squatting down at the back of the booth, so he couldn't be seen, picked the lock on the cabinet that housed their PDP-11 minicomputer and the cable terminations. Vinny plugged the cable leading from the console port into one of the terminals on the show floor. Because the LOCK-11 software now identified that attacker was logging in from an authorized terminal, it granted me access, and attacker was connected with system administrator privileges. Attacker patched the operating system by changing it, so that from any of the terminals on the floor, I would be able to log in as a privileged user. Attacker did a directory listing, to find out what files were on the computer, looking for the LocK-11 program and associated files and stumbled on something attacker found shocking: a directory that should not have been on this machine. The developers had been so overconfident, so certain their software was invincible, that they hadn't bothered to remove the source code of their new product. Moving to the adjacent hard-copy terminal, attacker started printing out portions of the source code onto the continuous sheets of the <i>green striped</i> computer paper used in those days.
Control	Deploying all possible countermeasures to protect the software

Table 47. Example of the misleading caller ID security risk

Business asset	Financials for the current quarter, financial projections on the Apache project
IS asset	Employee
Security Criterion	confidentiality of financials for the current quarter, confidentiality of financial projections on the Apache project
Impact	Employee is not trusted, negation of <i>authentication</i> of caller.
Vulnerability	Employee is not experienced to verify the caller.
Threat agent	Caller who has knowledge in telecommunication, has knowledge in the current process of the organization.
Attack method	Attacker caller and introduced <i>himself as Victor Martin (made corresponding ID)</i> . He said that was from PR and working on some material for the CEO. He needs the top-line financials for the current quarter & <i>his</i> financial projections on the Apache <i>project</i> . <i>She</i> sent the fax a few minutes later. But Victor did not work for the PR department. In fact, he didn't even work for the company.
Control	Organization has to deploy all possible countermeasures of protection.

Table 48. Example of the president of the United States is calling security risk

Business asset	Caller ID
IS asset	company's Meridian telephone switch
Security Criterion	Integrity of caller ID, confidentiality of caller ID
Impact	Negation of access to the company's meridian telephone switch
Vulnerability	Company's meridian telephone switch is accessible to third party
Threat agent	Attacker: who has an access to company's Meridian telephone switch and programming skills
Attack method	Attacker had access to the company's Meridian telephone switch, which gives him the ability to program the calling party number, as described in the previous story. Whenever he needed to reach the program director and couldn't get a call through, he would ask a friend to program any number of my choosing to appear on the caller ID.
Control	Organization has to deploy all possible countermeasures of protection.

Case: The invisible employee

Shirley Cutlass has found a new and exciting way to make fast money. Today she has set her sights on getting confidential information from the customer service department of a credit card company. After doing the usual kind of homework, she calls the target company and tells the switchboard operator who answers that she'd like to be connected to the Telecom Department. Reaching Telecom, she asks for the voice mail administrator. Using information gathered from her research, she explains that her name is Norma Todd from the Cleveland office. Using a ruse that should by now be familiar to you, she says she'll be traveling to corporate headquarters for a week, and she'll need a voice mailbox there so she won't have to make long distance calls to check her voice mail messages. No need for a physical telephone connection, she says, just a voice mailbox. He says he'll take care of it, he'll call her back when it's set up to give her the information she'll need. Shirley phones in, changes the password, and records her new outgoing greeting. She calls the customer service department of the company. And she goes on to provide the name and date of birth of the person whose identity she is intent on stealing. Then she lists the information she wants: address, mother's maiden name, card number, credit limit, available credit, and payment history. She keeps busy with errands for the rest of the morning, and then checks her voice mail that afternoon. It's all there, everything she asked for. Before hanging up, Shirley clears the outgoing message; it would be careless to leave a recording of her voice behind.

Case: The helpful secretary

Cracker Robert Jorday had been regularly breaking into the computer networks of a global company, Rudolfo

Shipping, Inc. The company eventually recognized that someone was hacking into their terminal server, and, that through that server the user could connect to any computer system at the company. To safeguard the corporate network, the company decided, to require a dial-up password on every terminal server. Robert called the Network Operations Center posing as an attorney with the Legal Department and said he was having trouble connecting to the network. The network administrator he reached explained that there had been some recent security issues, so all dial-up access users would need to obtain the monthly password from their manager. Robert wondered what method was being used to communicate each month's password to the managers and how he could obtain it. The answer, it turned out, was that the password for the upcoming month was sent in a memo via office mail to each company manager. That made things easy. Robert did a little research, called the company just after the first of the month, and reached the secretary of one manager who gave her name as Janet. He asked her to send this password by fax as he lost that paper somewhere. He gave the receptionist a fax number that went to an on-line fax service. When this service receives a fax, the automated system sends it to the subscriber's email address.

Case: The Traffic Court

The traffic violator was Paul Durea. First call was done to Subpoena Control. Attacker wanted to know when Officer Kendall will not be available. He received all necessary information. Second call to the Municipal Court, to schedule a court date. Next action was a meeting in the Municipal court, where violator didn't want to attend traffic school and asked to set for trial. Also violator told that he will have a business trip and informed the court when he will be available. On next meeting Paul arrived at court early on the 8th. When the judge came in, the clerk gave him a list of the cases for which the officers had not appeared. The judge called the defendants, including Paul, and told them their cases were dismissed.

Table 49. Example of the invisible employee security risk

Business asset	Voice mailbox, name, date of birth of the person whose identity, address, mother's maiden name, card number, credit limit, available credit, and payment history.
IS asset	Switchboard operator, telecom
Security Criterion	Availability of voice mailbox, name, date of birth of the person whose identity, address, mother's maiden name, card number, credit limit, available credit, and payment history; confidentiality of voice mailbox, name, date of birth of the person whose identity, address, mother's maiden name, card number, credit limit, available credit, and payment history.
Impact	Switchboard operator is not trusted, negation of authentication of caller.
Vulnerability	Switchboard operator is not experienced to verify the caller.
Threat agent	Caller: who knows how to use cell phone, gather some information in advance.
Attack method	Attacker calls the target company and tells the switchboard operator who answers that she'd like to be connected to the Telecom Department. Reaching Telecom, she asks for the voice mail administrator. Using information gathered from her research, she explains that her name is Norma Todd from the Cleveland office. No need for a physical telephone connection, she says, just a voice mailbox. And she goes on to provide the name and date of birth of the person whose identity she is intent on stealing.
Control	Try calling your own voice mail once in a while; if you hear an outgoing message that's not yours, you may have just encountered your first social engineer.

Table 50. Example of the helpful secretary security risk

Business asset	Dial-up password, terminal server.
IS asset	Network Operations Center, secretary.
Security Criterion	Confidentiality of dial-up password, terminal server; integrity of dial-up password, terminal server; availability of dial-up password, terminal server.
Impact	Secretary is not trusted, negation of authentication of a caller.
Vulnerability	Secretary is not experienced to verify the caller.
Threat agent	Caller: who knows how to use cell phone, how to get correct phone number.
Attack method	Attacker wondered what method was being used to communicate each month's password to the managers and how he could obtain it. The answer, it turned out, was that the password for the upcoming month was sent in a memo via office, mail to each company manager. That made things easy. Robert did a little research, called the company just after the first of the month, and reached the secretary of one manager who gave her name as Janet. He asked her to send this passwords by fax as he lost that paper somewhere. He gave the receptionist a fax number that went to an on-line fax service. When this service receives a fax, the automated system sends it to the subscriber's email address.
Control	Organization has to deploy all possible countermeasures of protection.

Table 51. Example of traffic court security risk

Business asset	Serial number of officer
IS asset	Employee of Municipal Court, Subpoena Control.
Security Criterion	Availability of serial number of officer, confidentiality of serial number of officer.
Impact	Negation of authentication of a caller, employee is not trusted.
Vulnerability	Employee is not experienced to verify the caller.
Threat agent	Caller: who knows how to use cell phone, how to get necessary phone number.
Attack method	First call was done to Subphoena Control. Attacker wanted to know when officer Kendall will not be available. He received all necessary information. Second call to the Municipal Court, to schedule a court date. Next action was a meeting in the Municap court, where violator didn't want to attend traffic school and asked to set for trial. On next meeting Paul arrived at court early on the 8th. When the judge came in, the clerk gave him a list of the cases for which the officers had not appeared. The judge called the defendants, including Paul, and told them their cases were dismissed.
Control	Law enforcement agencies have to inform their workers about possibility of attack and steal of information.

Case: Samantha's revenge

Samantha Gregson was angry. She hasn't received promotion and decided to revenge the company. She had been in young Mr. Johansson's office one day shortly after that when he logged onto the corporate network. Without thinking, she had watched his fingers (shoulder surfing, this is sometimes called). He had entered "marty63" as his password. Her plan was beginning to come together. There was a memo, she remembered typing not long, after she came to the company. She found a copy in the files and typed up a new version, using language from the original one. When most everybody was gone at lunch, she cut Mr. Cartright's signature from the original memo, pasted it onto her new version, and daubed Wite-Out around the edges. She made a copy of the result, and then made a copy of the copy. You could barely see the edges around the signature. She sent the fax from the machine "near Mr. Cartright's office. Three days later, she stayed after hours and waited till everyone left. She walked into Johansson's office, and tried logging onto the network with his username and the password, marry63. It worked. In minutes she had located the product specification files for the Cobra 273, and downloaded them to a Zip disk.

Table 52. Example the Samantha's revenge security risk

Business asset	Information about COBRA 273, password,username, signature
IS asset	Samantha Gregson
Security Criterion	Integrity of information about COBRA 273, password, username, signature; confidentiality of information about COBRA 273, password, username, signature.
Impact	Negation of confidentiality of password.
Vulnerability	Samantha Gregson is not trusted.
Threat agent	Insider (Samantha Greyson): who has all necessary access inside of the company
Attack method	Attacker used shoulder surfing and memorized password. She found a copy in the files and typed up a new version, using language from the original one. She walked into Johannsson's office, and tried logging onto the network with his username and the password, marry63. It worked. In minutes she had located the product specification files for the Cobra 273, and downloaded them to a Zip disk.
Control	Organization has to deploy all possible countermeasures of protection.

II. Social Engineering Examples in BPMN

Search in Recycle Bin

Context and asset identification. Illustration to the applied BPMN security extension to the case “Search in recycle bin” is presented in Figure 14. As an employee wants to receive Test Numbered Directory he sends a request (task *Ask for Test Numbered Directory*) to certain department (task *Retrieves Test Numbered Directory*). When the division of the company receives request, it provides the copy of Test Numbered Directory to the switchman.

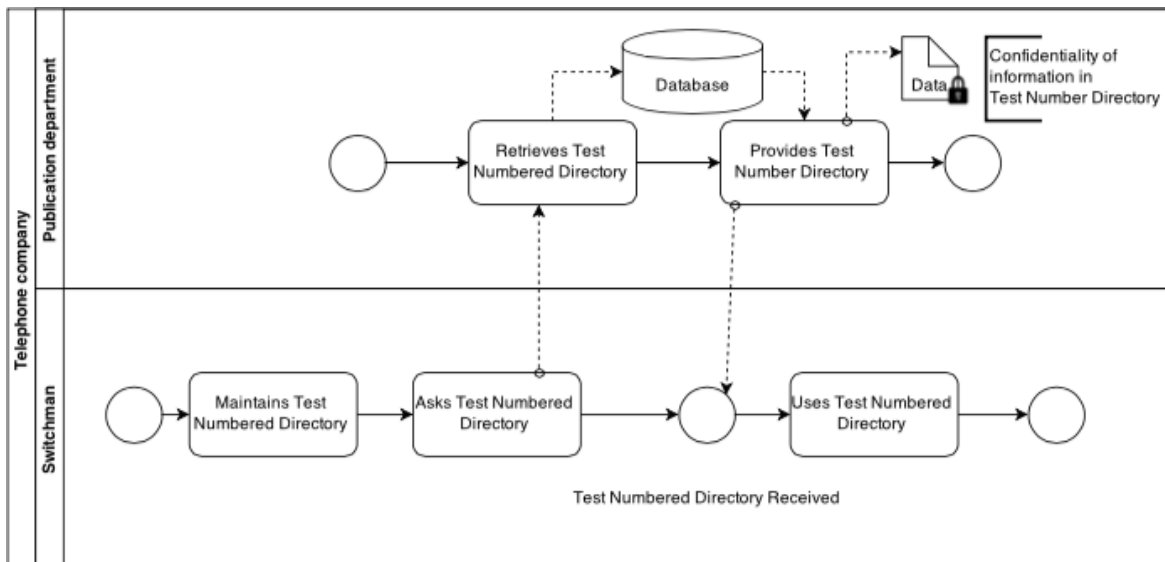


Figure 14. Search in recycle bin - BPMN assets identification

If consider the incident from **Risk-related concept** attacker called to the small central office telephone company building and said that for security reasons he cannot give employees copy until he gets old one. Next situation was where the potential attacker (pool *Attacker* in Figure 15) wished to get information from the switchman. An Attacker called (task *Asks for Test Numbered Directory*) to employee (task *Maintain for Test Numbered Directory*) then asked to leave its copy in order to get a new version. As employee trusted to the caller and sent back a copy (tasks *Uses Test Number Directory*). Then attacker received it (task *Test Numbered Directory received*).

In the final analysis from **risk treatment-related concept** presented how security flows can be mitigated. First of all switchman needed to verify from his colleagues that there has been issued a new version of Test Numbered Directory and to ask from security specialist is there mentioned something about exchange of published and printed out materials copies in security policy. To reduce the probability of providing internal information to the attacker, it has been introduced such task as ask for ID. When attacker provided fake ID employee could maintain task check ID and if it is wrong, reject request (task *Refuse to give data*).

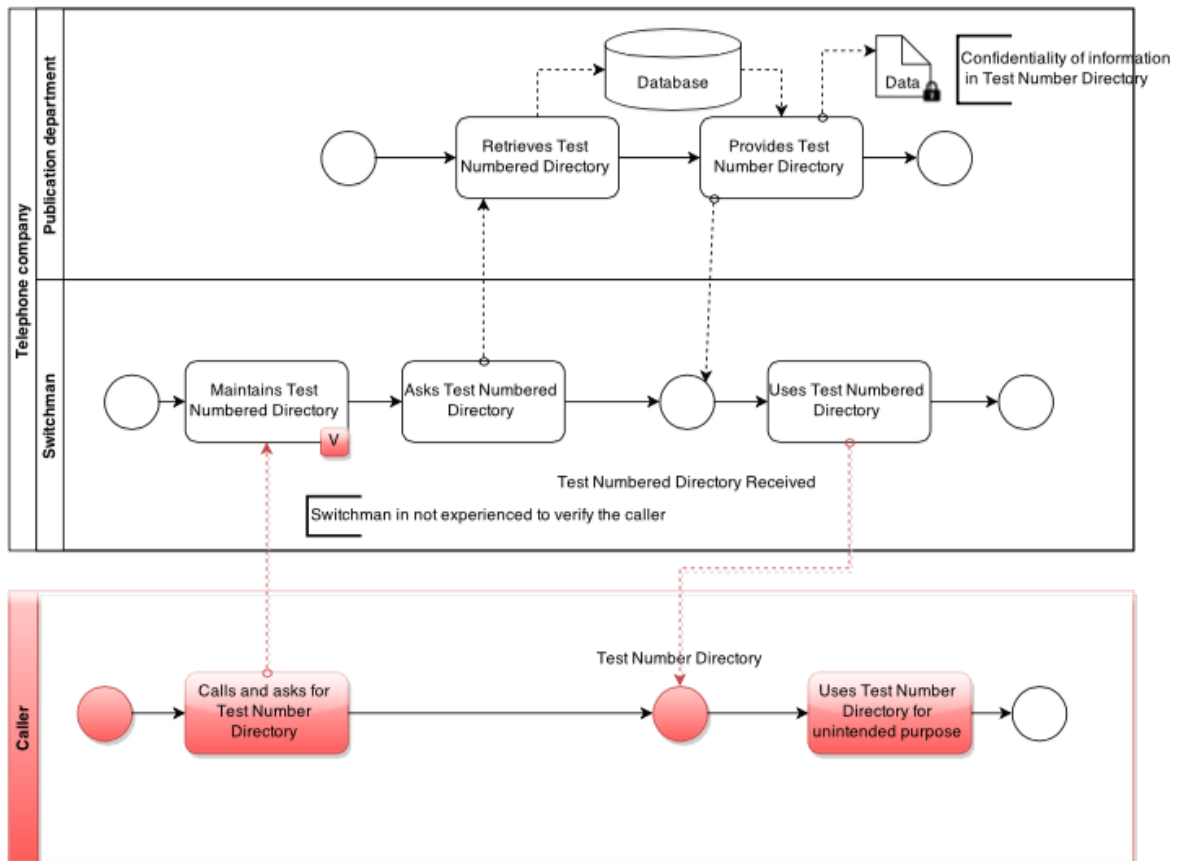


Figure 15. Search in recycle bin - BPMN risks identification

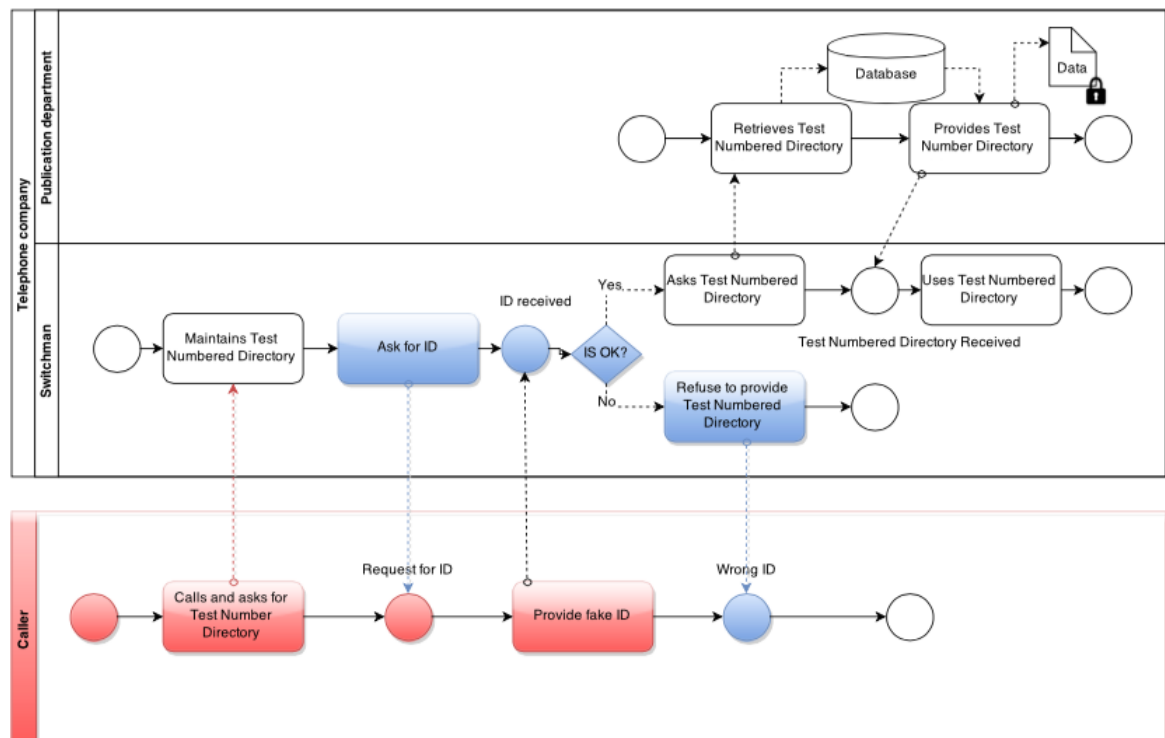


Figure 16. Search in recycle bin – BPMN risk treatment

Through Internet

Context and asset identification. Next situation was where the university's Registration office (pool *Registration office* in Figure 17) wished to get information about Michael Parker from university record's database. In order to get any information the Registration office checks it from the database (task *Requests for data*, *Maintains Login and password*, *Provides Login and Password*). Meanwhile the database performs following task *Retrieves data*, *Asks for Login and password*, *Login and password received*. If the Login and Password provided by Registration office is correct, database will extract necessary information and provide it to the Registration office (task *provided data*).

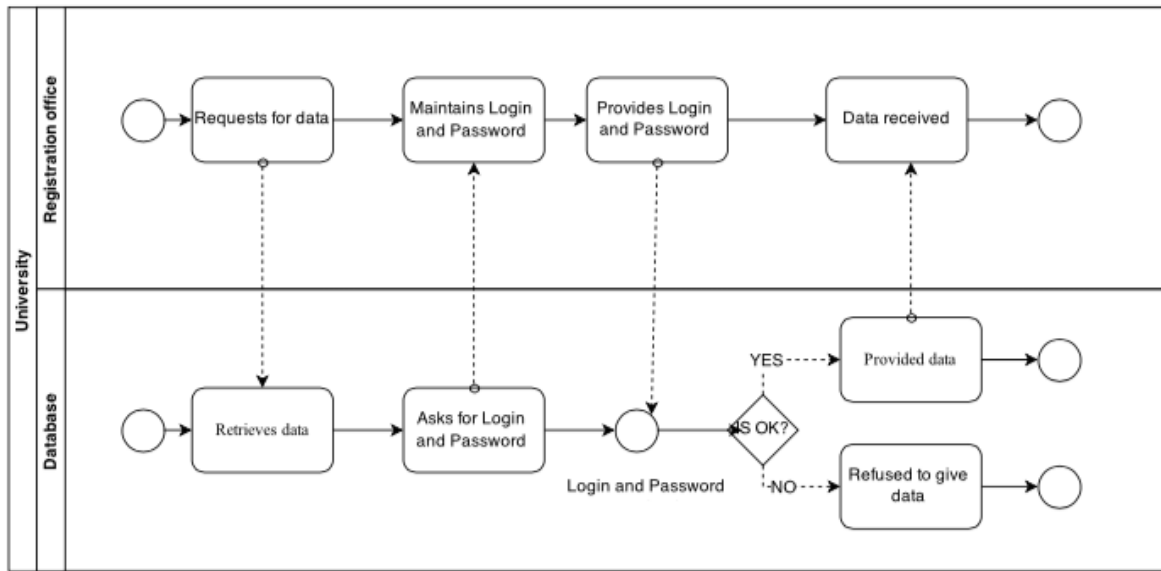


Figure 17. Through Internet – BPMN assets identification

In order to get required information, the Attacker/ Michael Parker did several necessary calls. During all calls the basic scheme of attack was the same. First of all the caller asks to provide some information from Registrar's office. In order to get it the attacker Request for data. After a message received (task *Maintain data*) Registration office checks it from the database (task *Ask data*, *Data received*) and provides received data (task *Uses data*). Michael Parker receives information (task *data received*) and uses it (task *Uses data*).

From **Risk-related concept** (see Figure 18) attacker went to the main library on the university campus, he sat down at a computer terminal, got up on the Internet, and accessed to the university's Web site. Then attacker called the Registrar's office. In order to get required information, the

Attacker/ Michael Parker did several necessary calls. During the process of obtaining necessary data the basic scheme of attack was the same. First of all the caller asked to provide some information from Registrar's office. In order to get information the attacker Request for data. After a message received (task *Maintain data*) Registration office checks it from the database (task *Ask for data*, *Data received*) and provides received data (task *Uses data*). Michael Parker receives information task data received and uses it (task *Uses data for unintended purpose*).

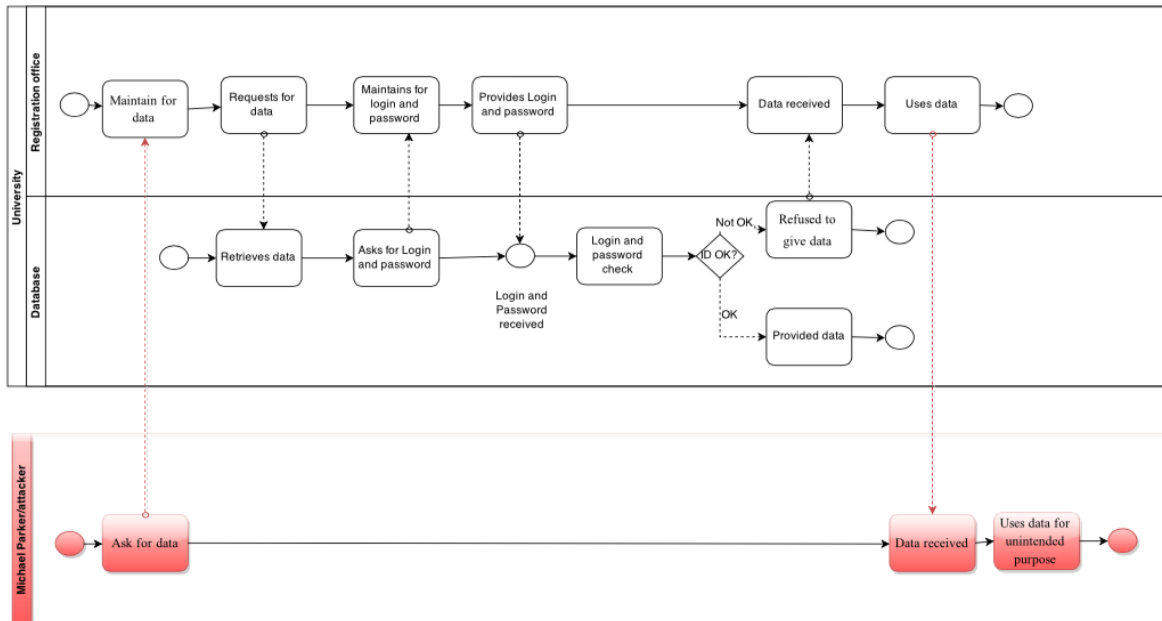


Figure 18. Through Internet - BPMN risks identification

Henceforth **Risk treatment concept** for all employees who are able to access any sensitive information have to know the importance of that information. University has to maintain a list of people who have been specially trained in the procedures and who are trusted to authorize sending out sensitive information. It is required that only these people are allowed to send information to anyone outside the workgroup. In this case it might be better to ask an ID beforehand in order to start the internal process of getting any sensitive information. Then Registration office has to ask an ID, check it (task *Ask for ID*, *ID received*, *check ID*) and only then provide data in case ID is correct.

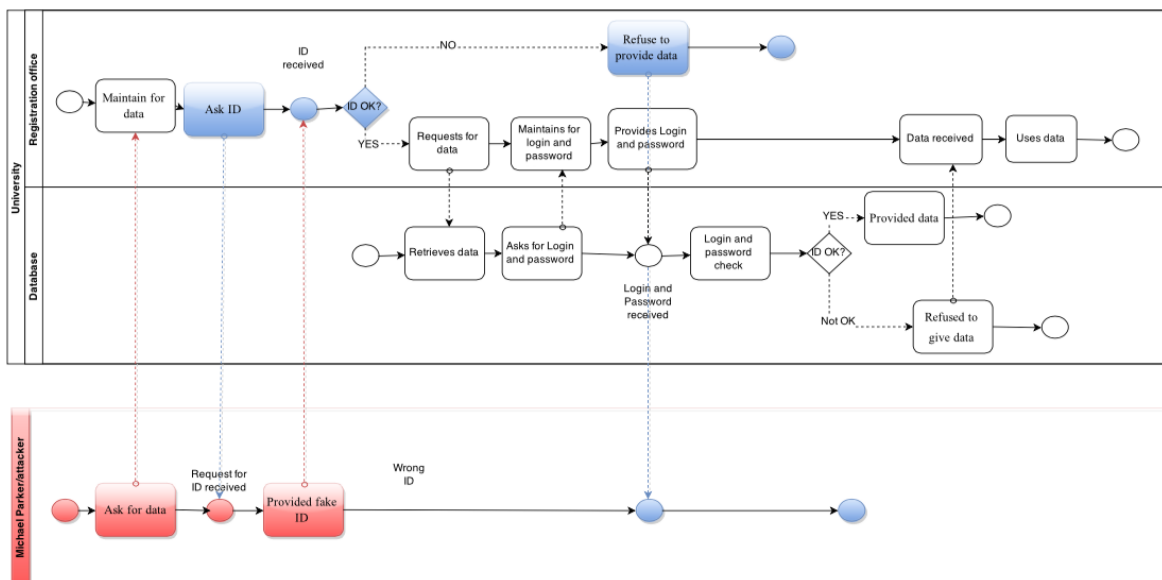


Figure 19. Through Internet – BPMN risk treatment

Through Persuasion

Context and asset identification. Next situation was where a user Steve (pool Steve in Figure 20) wished to get information from GeminiMed Medical Products. In order to get it, Steve requested that information from computer server. Firstly computer server asks to provide ID and password (task *Asked ID and password*) then Steve receives a request (task

Retrieved ID and password, Provided ID and password) and computer server receives ID (task *ID received*). If the provided data is correct, Steve receives data (task *Data received*) and can use it (task *Uses data*).

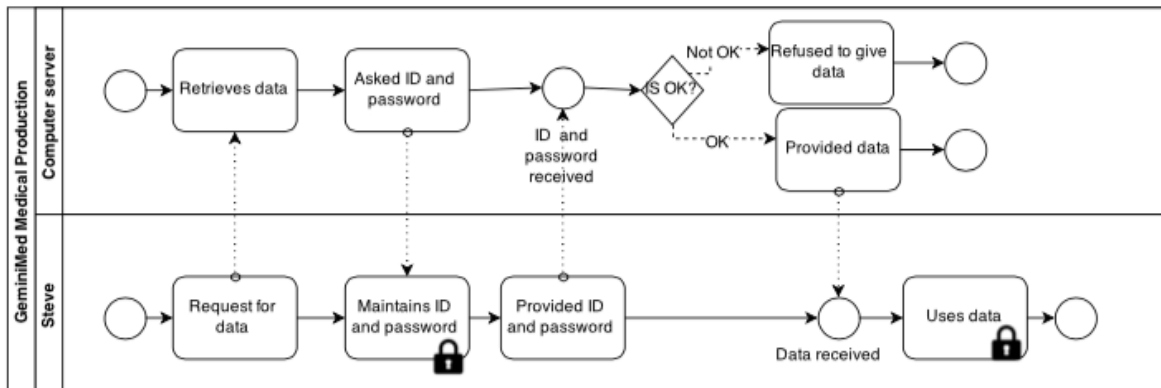


Figure 20. Through persuasion – BPMN assets identification

Risk related concept. Steve received a call from Ramon Perez from tech support with an information that three of the servers are not working and they'll need some time to reinstall the driver and restore all of their files. To have an access to his information as soon as possible Steven asked from tech support to deal with it urgently. Ramon Perez was pleased to help, but in order to help he needed to ask some verification questions. In Figure 21 the Caller requested a data (task *Calls and asks for data*) that has Steve (task *maintain data*). In order to provide any information Steve was suspicious that caller asked his private information (task *Asks to verify*). To sound authentic Caller gave old password (task *provided old ID and password*). Steve received it (task *ID Received*) and provided requested information (task *provided data*). Finally as data received, caller used it to his own purpose (task *Uses data for not intended purpose*).

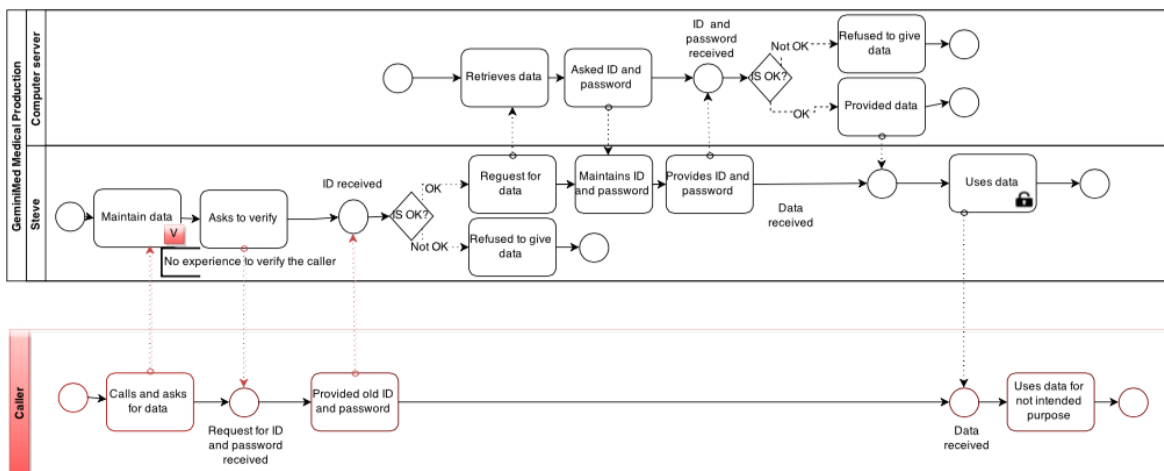


Figure 21. Through persuasion – BPMN risks identification

Risk treatment concept. Steve needed to verify that person who called is from technical support and taking into account that he got suspicious, not provide any information until a call to the boss or co-worker. To reduce the possibility of accepting the message Steve shouldn't accept old ID and password.

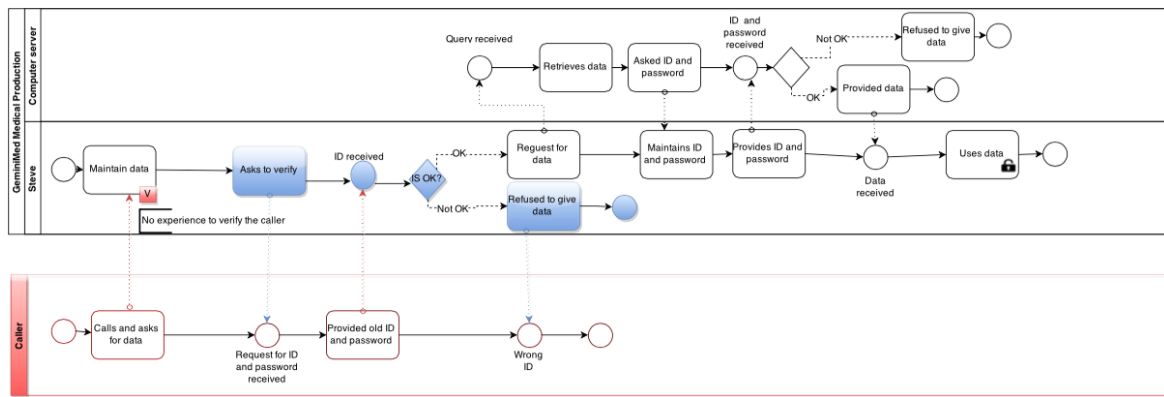


Figure 22. Through persuasion – BPMN risk treatment

Breaking Through Computer Network

Context and asset identification. Next situation was where one department of an organization (pool *IT Technical support* in Figure 23) wished to get some information. In order to get, first of all, IT technical support (task *Ask data*) called to the project leader (task *Retrieve data*). A project leader checked the availability of the information from servers to provide data (task *Provide data*) to IT support (task *Data received*). As soon as technical support received information, it can be used by that department.

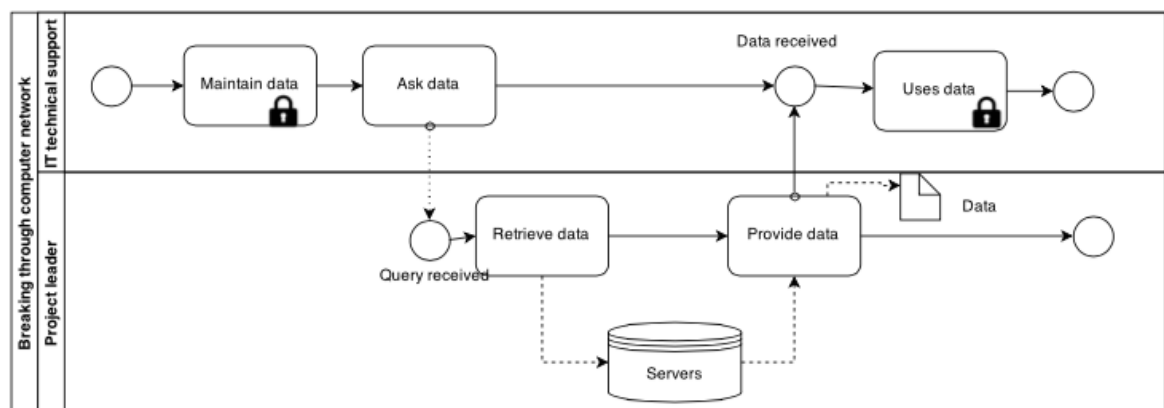


Figure 23. Breaking through computer network – BPMN assets identification

If consider the incident from **Risk-related concept** attacker noticed un-patched vulnerability in the Web-Server software. Called to IT technical support, claims to be a company employee, and asks phone number of project leader. Then called to project leader as a guy from IT and received name of servers. In both cases attacker performed called to the department (task *Calls and asks for data*) and received necessary information (task *Data received*). Using that data caller (task *Uses for not intended purpose*) was able to make a technical attacks on systems that provide remote access capability to identify weak password. When he was not able to find a password to ATM5, he figured out that some member might have chosen the same password for both machines and did further research in that area.

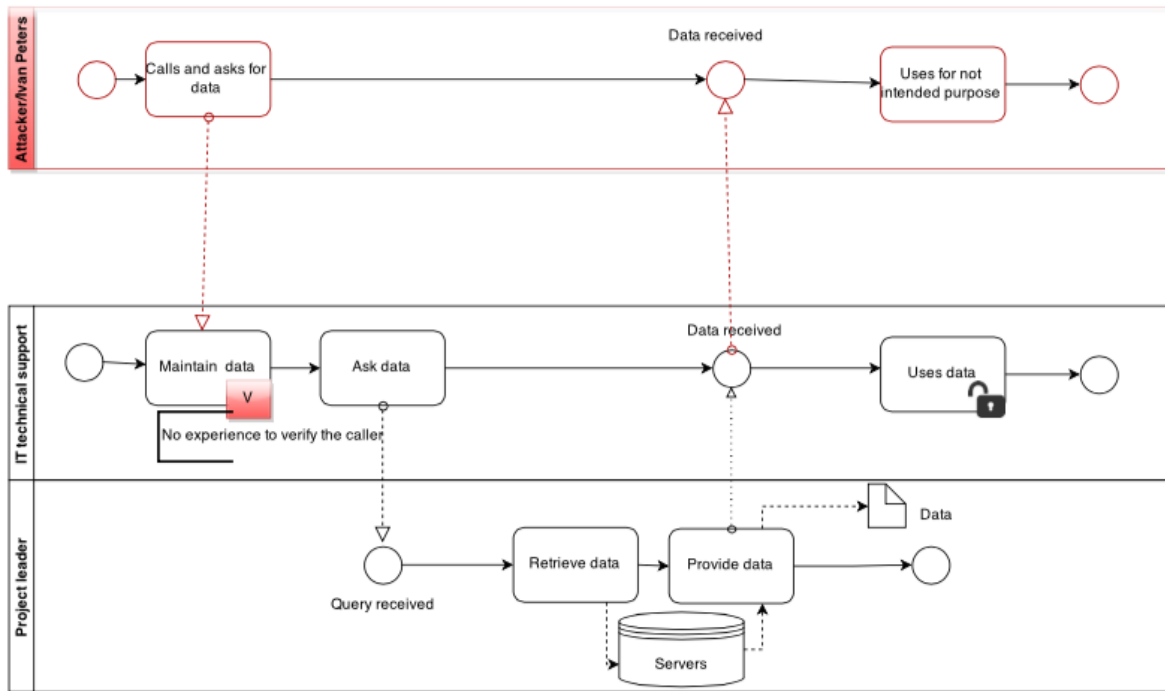


Figure 24. Breaking through computer network – BPMN risks identification

Henceforth **Risk treatment concept** typically involves taking steps on both human and technical levels. Because both commercial and public-domain hacking tools can be obtained by anyone for whatever purpose they have in mind, it's all the more important that you be vigilant in protecting enterprise computer systems and your network infrastructure. To do it any employee shouldn't speak valuable information of the organization and do no use easy passwords. In this case IT technical support should ask to verify caller's identity and provide ID (task *Asks to verify*).

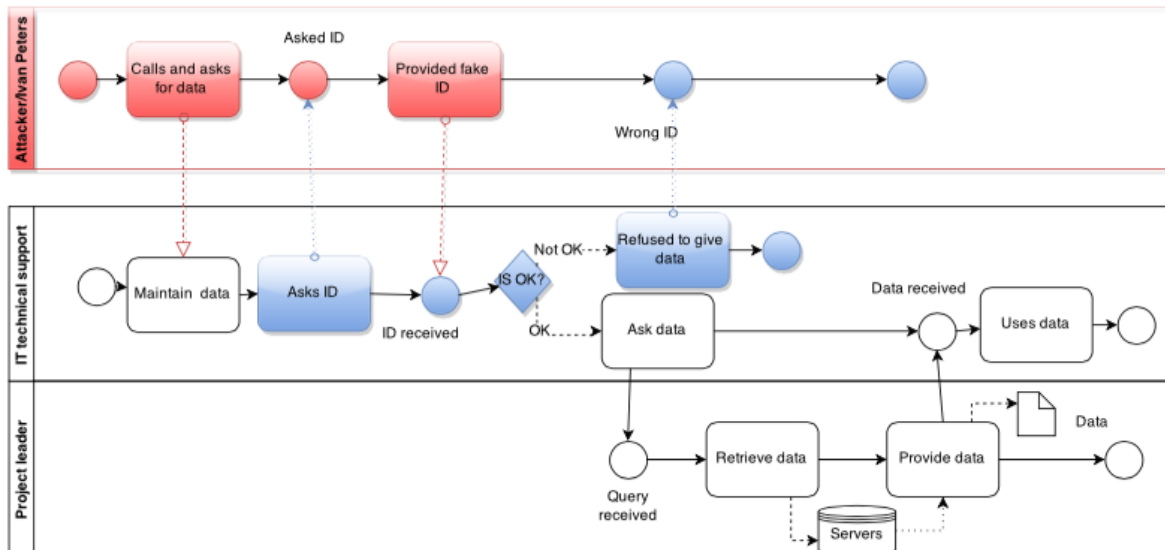


Figure 25. Breaking through computer network – BPMN risk treatment

III. Social Engineering Examples in MUC

Search in Recycle Bin

Asset Model. The case is focused on Switchman and the Test Number Directory system. An asset is only Switchman who is a user of the Test Number Directory. In order to get any information Switchman Asks for Test Number Directory and Uses Test Number Directory. The Ask for Test Number Directory includes Retrieve Test Number Directory. Test Number Directory provided has a security criterion Confidentiality of information in Test Number Directory represented as a hexagon. According to the ISSRM domain model Ask for Test Number Directory has been identified as a business asset that has a value to the organization. Retrieve Test Number Directory supports the business asset and is considered as an IS asset. The Asks for Test Number Directory and Uses Test Number Directory are business asset. Retrieve Test Number Directory are IS asset.

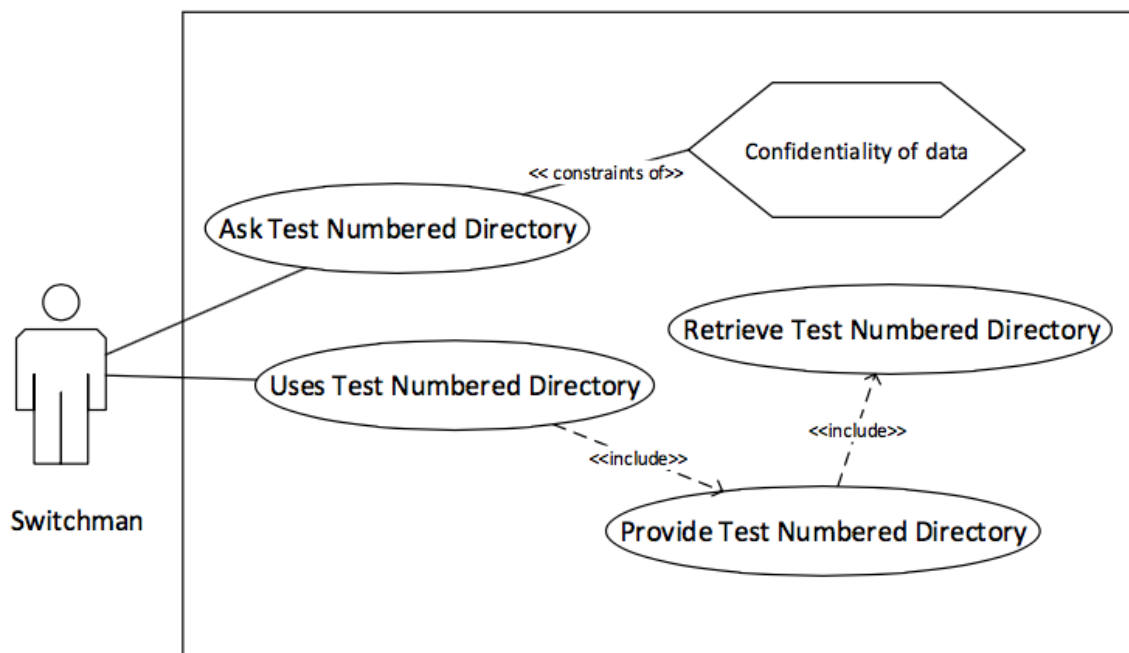


Figure 26. Search in recycle bin – misuse case assets model

Risk Model. In Figure 27 is presented security threat scenario. A misuser (i.e., *Attacker*) uses vulnerability (i.e., *User is not experienced, Switchman is not reliable*) to initiate misuse case (i.e., *Calls and asks for Test Number Directory*). In the picture Call for Test Number Directory exploits the fact that User is not experienced. Threat Calls and asks for Test Number Directory threatens Ask for Test Number Directory.

Risk treatment model. SROMUC does not support the risk treatment concept, but it is possible to model a security use case for identification of security requirement. In the Figure 28 represented security use case. It is shown by a use case diagram with a lock inside to mark security requirement for identified threats. The use case Switchman and Uses Test Number Directory (i.e., *IS Asset*) has to include a security use case (i.e., *Check ID*). The security use case mitigates the misuse case (i.e., *User is not experienced*). It ensures security criterion (i.e., *Confidentiality of Information in Test Number Directory*) imposed by business use case (i.e., *Provided Test Number Directory*).

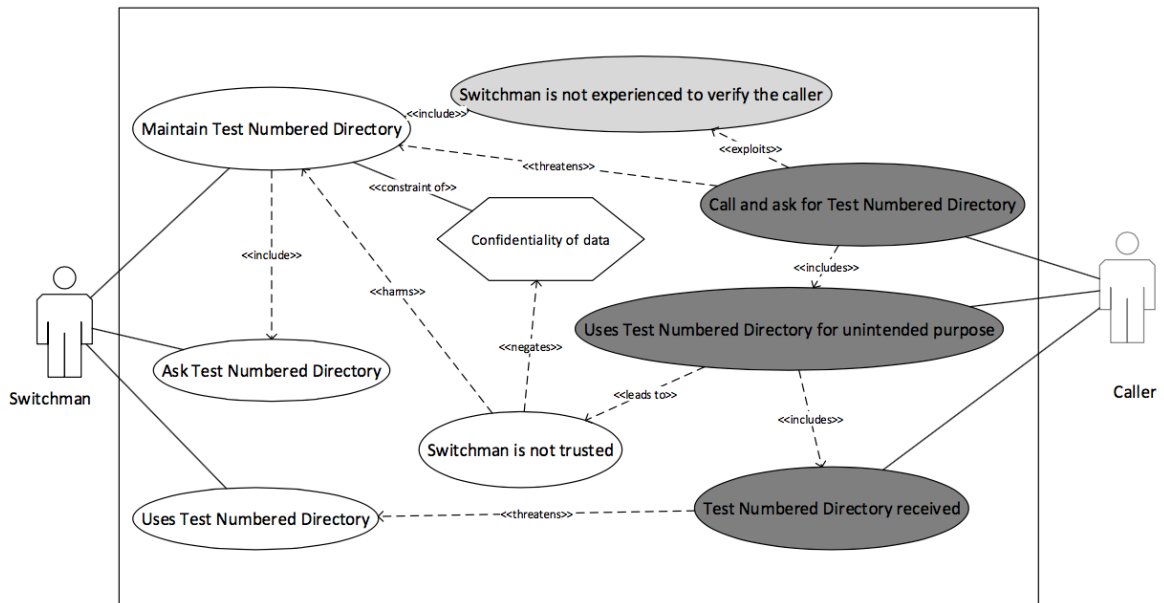


Figure 27. Search in recycle bin – misuse case risk model

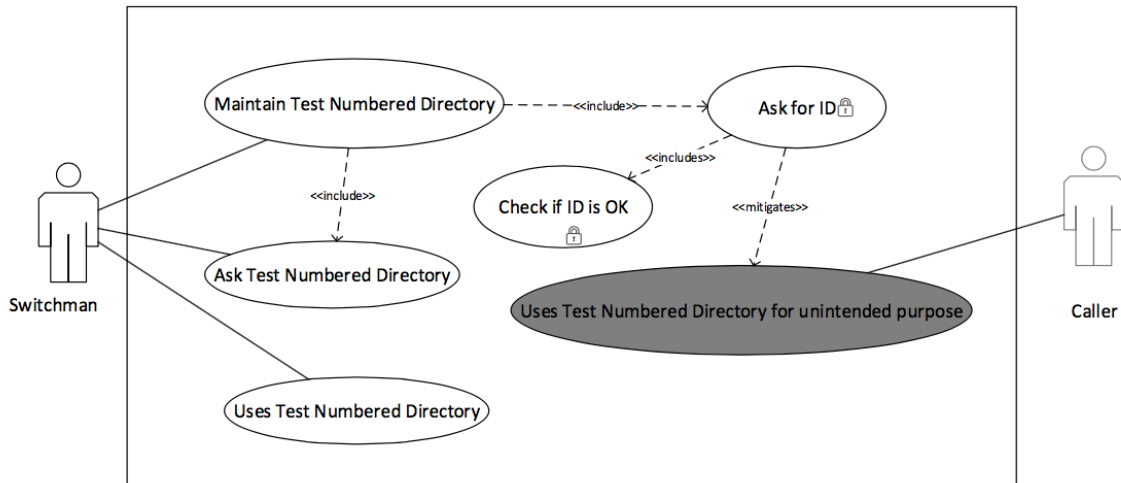


Figure 28. Search in recycle bin – misuse case risk treatment

Through Internet

Asset Model. An asset is only Registration office who has an access to the system. In order to get any information Registration office Requests for data, Maintains Login and Password, Provides login and password and Data received. The Request for data includes Asks for Login and Password and extends Maintain Login and Password. Retrieve data has a security criterion Confidentiality of data represented as a hexagon. The Provide data includes two use cases Login and Password Check and Data received. According to the ISSRM domain model Request for data has been identified as a business asset that has a value to the organization. Retrieve data supports the business asset and is considered as an IS asset. The Maintains Login and password, Ask for Login and Password are business asset.

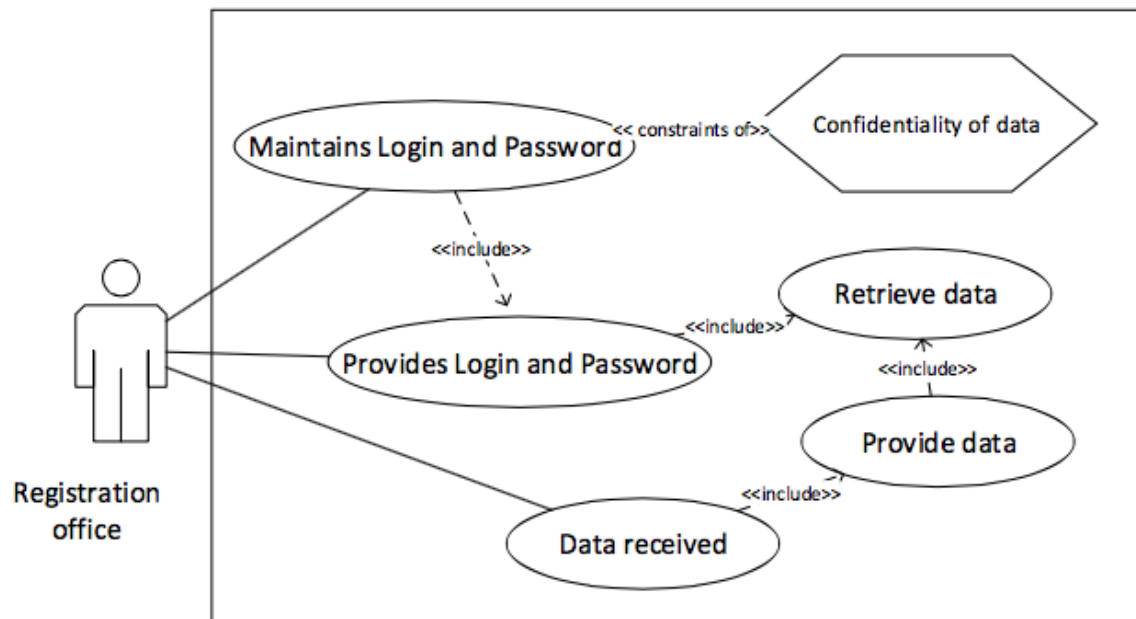


Figure 29. Through Internet – misuse case assets model

Risk Model. In Figure 30 is presented security threat scenario. A misuser (i.e., *Attacker*) uses vulnerability (i.e., *Registration office is not trusted*, *Registration office is not experienced to verify the caller*) to initiate misuse case (i.e., *Calls for data*). Request for data exploits the fact that User is not experienced. Threat User is not experienced threatens Request for data which includes retrieve data and disaffirms Confidentiality of data.

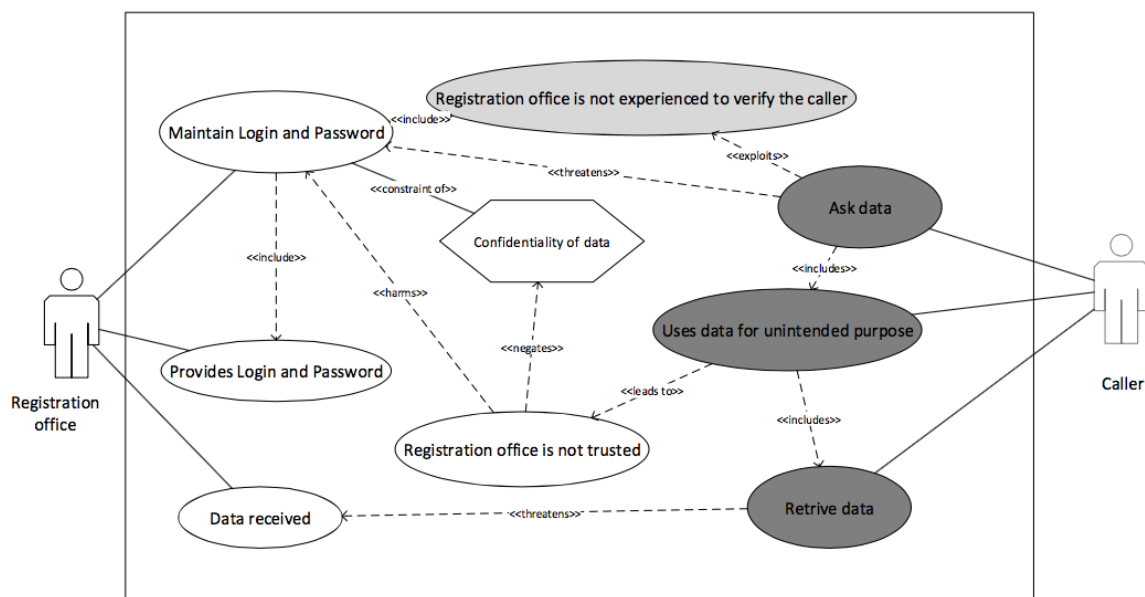


Figure 30. Through Internet - misuse case risk model

Risk treatment model. SROMUC does not support the risk treatment concept, but it is possible to model a security use case for identification of security requirement. In the Figure 31 represented security use case. It is shown by a use case diagram with a lock inside to mark security requirement for identified threats. The use case Registration office and Maintain data (i.e., *IS Asset*) has to include a security use case (i.e., *Check ID*). The security use case mitigates the misuse case (i.e., *Registration office is not experienced to verify the*

caller). It ensures security criterion (i.e., *Confidentiality of data*) imposed by business use case (i.e., *Maintain data*).

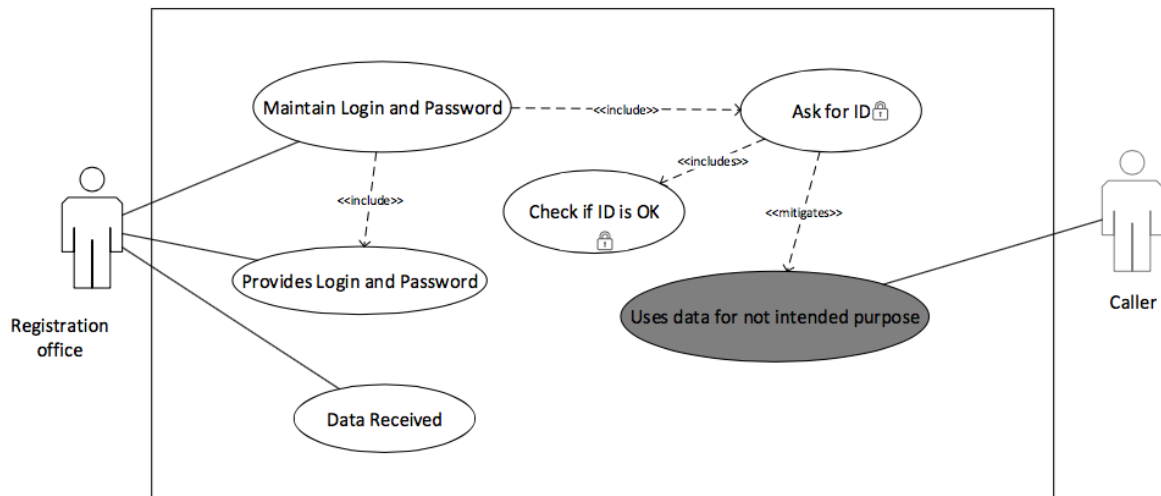


Figure 31. Through Internet – misuse case risk treatment

Through Persuasion

Asset Model. The case is focused on Steve and the computer server. In order to get any information Steve Calls and asks for data, retrieved ID and password, Uses data. The Maintains ID and password includes Provided ID and password. Asked ID and password has a security criterion Confidentiality of data represented as a hexagon. According to the ISSRM domain model Calls and asks for data has been identified as a business asset that has a value to the organization. Retrieved ID and password supports the business asset and is considered as an IS asset.

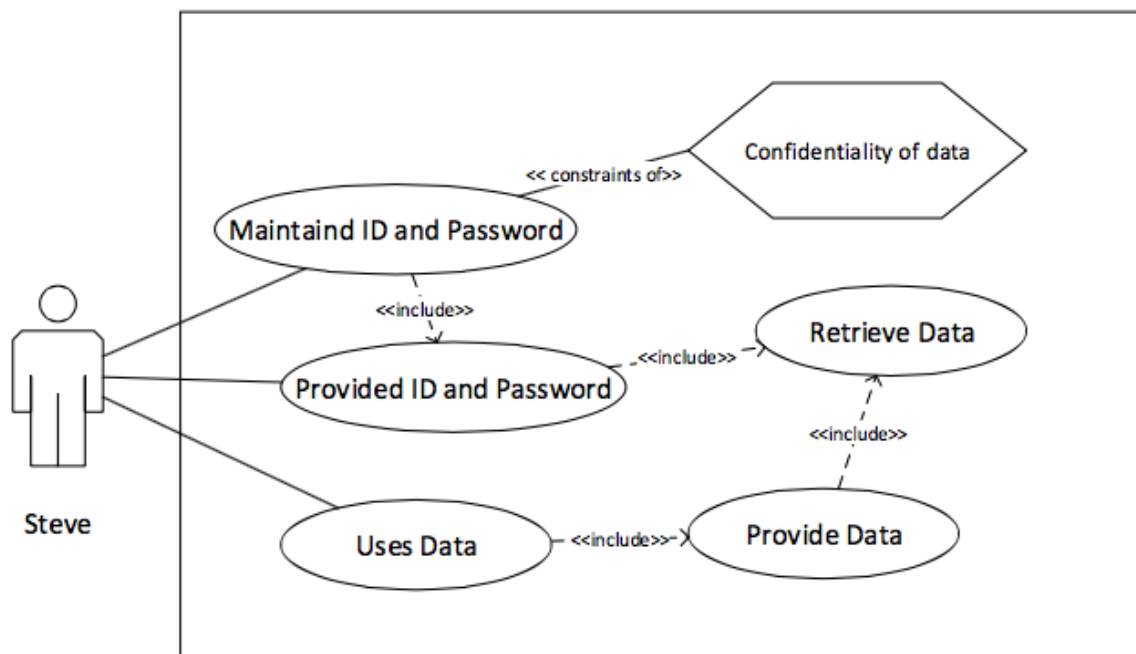


Figure 32. Through persuasion – misuse case assets model

Risk Model. In Figure 33 is presented security threat scenario. A misuser (i.e., *Caller*) uses vulnerability (i.e., *No experience to verify the caller, Steve is not trusted*) to initiate misuse case (i.e., *Calls for data*). Call for data exploits the fact that Steve is not experienced. Threat

Calls for data threatens Ask for data which extends Retrieve data and disaffirms Confidentiality of data.

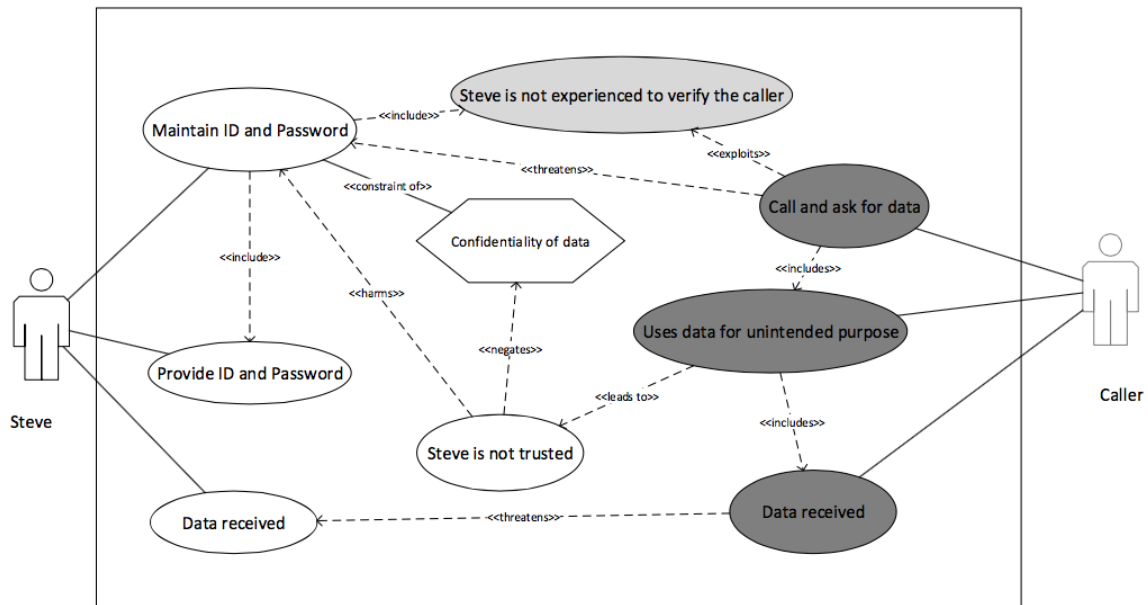


Figure 33. Through persuasion – misuse case risk model

Risk treatment model. SROMUC does not support the risk treatment concept, but it is possible to model a security use case for identification of security requirement. In the Figure 34 represented security use case. It is shown by a use case diagram with a lock inside to mark security requirement for identified threats. The use case Steve and Calls and asks for data (i.e., *IS Asset*) has to include a security use case (i.e., *Check ID*). The security use case mitigates the misuse case (i.e., *No experience to verify the caller*). It ensures security criterion (i.e., *Confidentiality of information*) imposed by business use case (i.e., provided data).

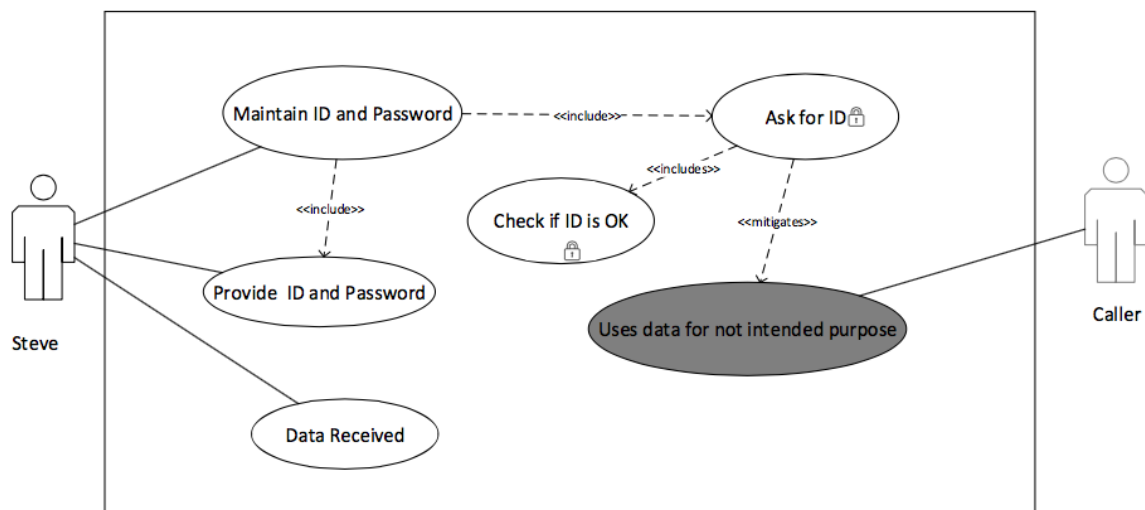


Figure 34. Through persuasion – misuse case risk treatment

Breaking Through Computer Network

Asset Model. An asset is IT Technical support and Project Leader who has an access to the system. In order to get any information IT Technical support Maintain data, Asks data and Uses data. The Ask for data includes Maintain data and extends Retrieve data. Retrieve data

has a security criterion Confidentiality of data represented as a hexagon. The Provide data includes two use cases Retrieve data and Uses data. According to the ISSRM domain model Ask for data has been identified as a business asset that has a value to the organization. Retrieve data supports the business asset and is considered as an IS asset. The Maintain data, Ask for data and Uses data are business asset. Retrieve data and Provide data are IS asset.

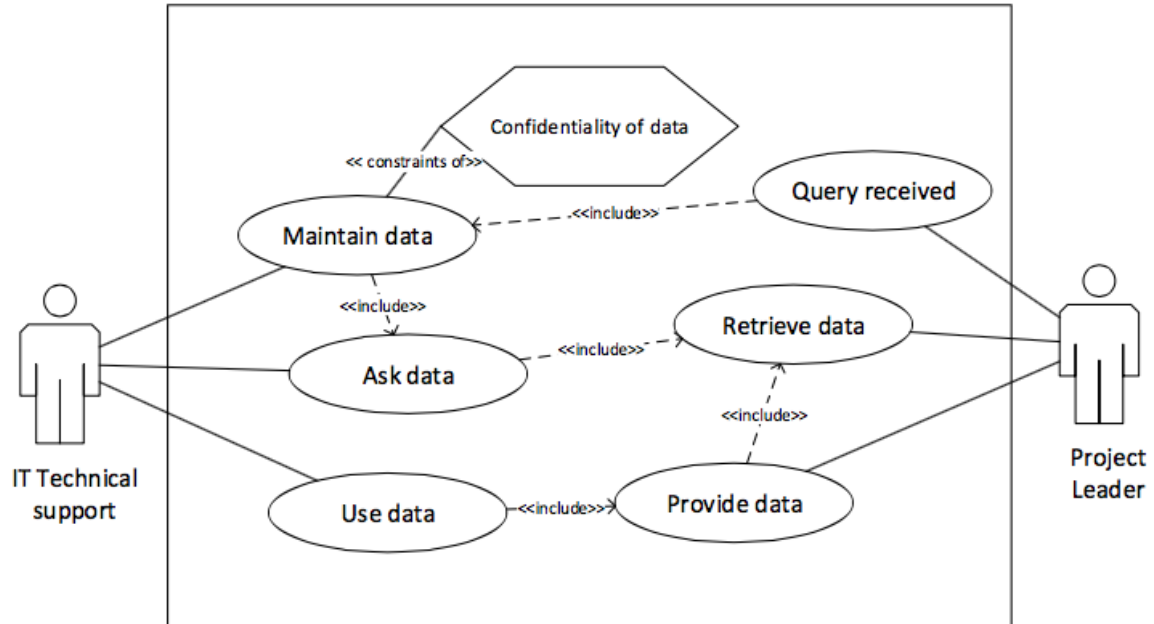


Figure 35. Breaking through computer network – misuse case assets model

Risk Model. In Figure 36 is presented security threat scenario. A misuser (i.e., *Attacker/ Ivan Peters*) uses vulnerability (i.e., *IT technical support is not trusted, No experience to verify the caller*) to initiate misuse case (i.e., *Calls for data*). Call and asks for data exploits the fact that No experience to verify the caller. Threat Calls for data threatens Ask for data which extends Retrieve data and disaffirms Confidentiality of data.

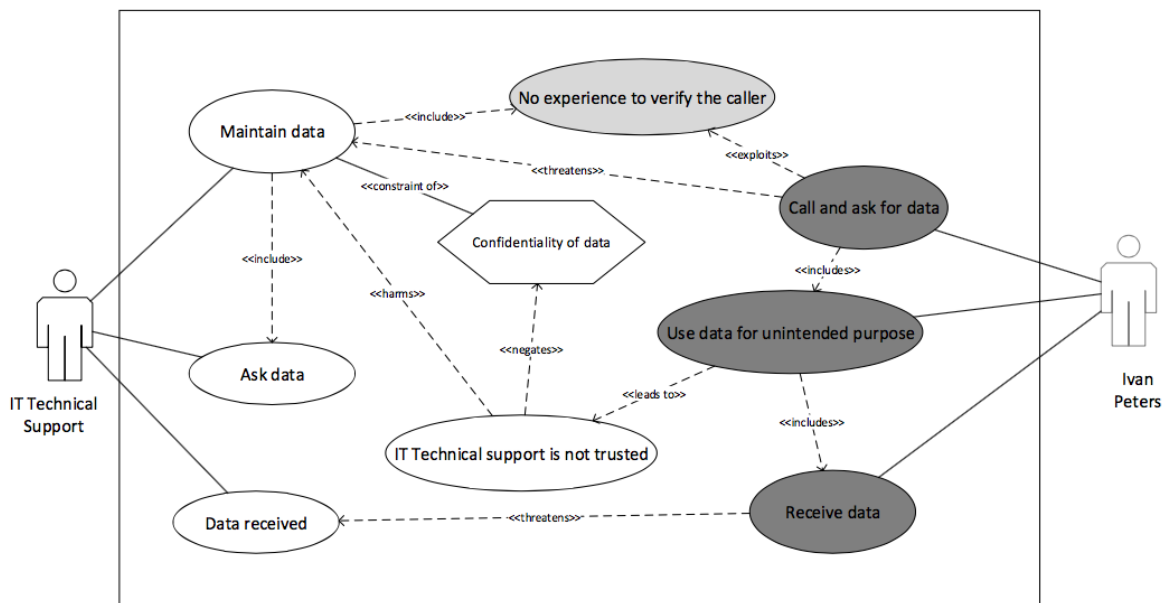


Figure 36. Breaking through computer network – misuse case risk model

Risk treatment model. SROMUC does not support the risk treatment concept, but it is possible to model a security use case for identification of security requirement. In the Figure 37 represented security use case. It is shown by a use case diagram with a lock inside to mark security requirement for identified threats. The use case IT technical support and Maintain data (i.e., *IS Asset*) has to include a security use case (i.e., *Check ID*). The security use case mitigates the misuse case (i.e., *IT technical support is not trusted*). It ensures security criterion (i.e., *Confidentiality of data*) imposed by business use case (i.e., *Maintain data*).

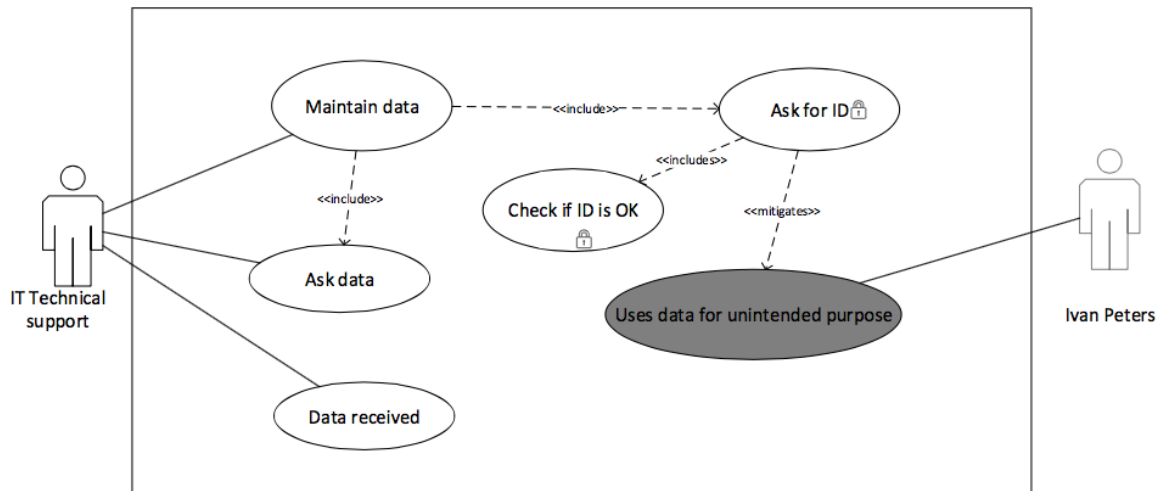


Figure 37. Breaking through computer network – misuse case risk treatment

IV. Social Engineering Examples in Secure Tropos

Search in recycle bin

Asset identification. Illustration to the applied Secure Tropos security extension to the case “Search in recycle bin” is presented in Figure 38. Here is represented only goals (e.g., Query received) and plans (e.g., *provide data*). In Secure Tropos security objectives are identified by softgoals (e.g., *Confidentiality*) and by security criteria which is communicated with security constraints (e.g., *Confidentiality of data*).

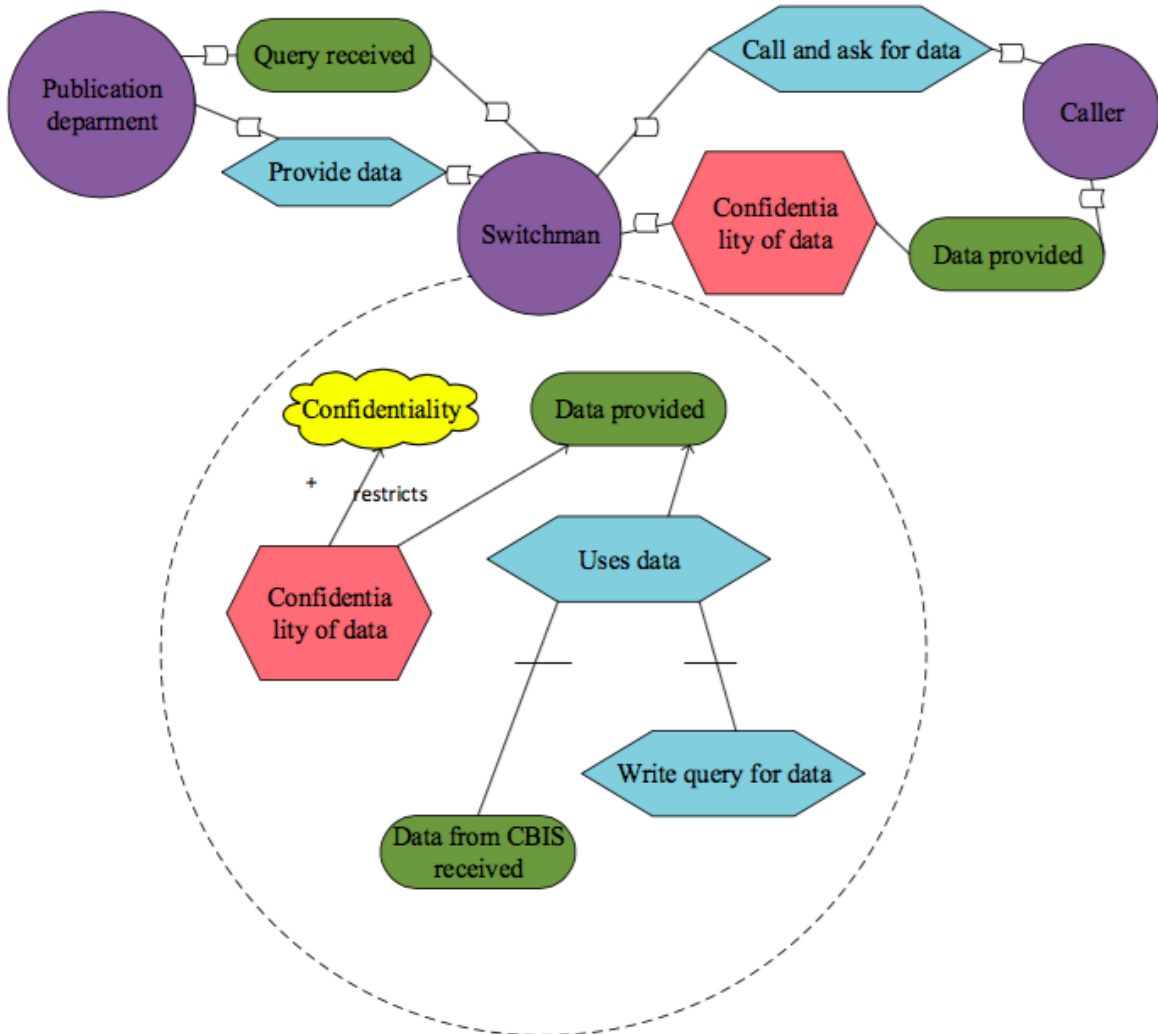


Figure 38. Search in recycle bin – Secure Tropos asset identification

Risk analysis. Next Figure 39 is focused on a possible event of the risk exposure. It describes a situation where a threat agent (e.g., *malicious caller*) wished to get an information from the switchman (e.g., *Switchman*). An attacker damages the Test Numbered Directory in the data provided. The Social engineering attack impacts Privacy. Malicious caller has a threat (*Use data for not intended purpose*) to support of data provided. Attacker attacks data provided through exploiting the vulnerability identified in uses data. The exploits link shows a relationship between an attack method (*Call and ask for data*) and a vulnerable IS asset (*Uses data*).

Security requirements definition. In order to mitigate risks, we have designed goals and plans. In current example plan is Check ID. It is shows in a dotted background pattern.

Through Internet

Asset identification. Illustration to the applied Secure Tropos security extension to the case “Through Internet” is presented in Figure 41. Here is represented only goals (e.g., *Query received*) and plans (e.g., *provide data*). In Secure Tropos security objectives are identified by softgoals (e.g., *Confidentiality*) and by security criteria which is communicated with security constraints (e.g., *Confidentiality of data*).

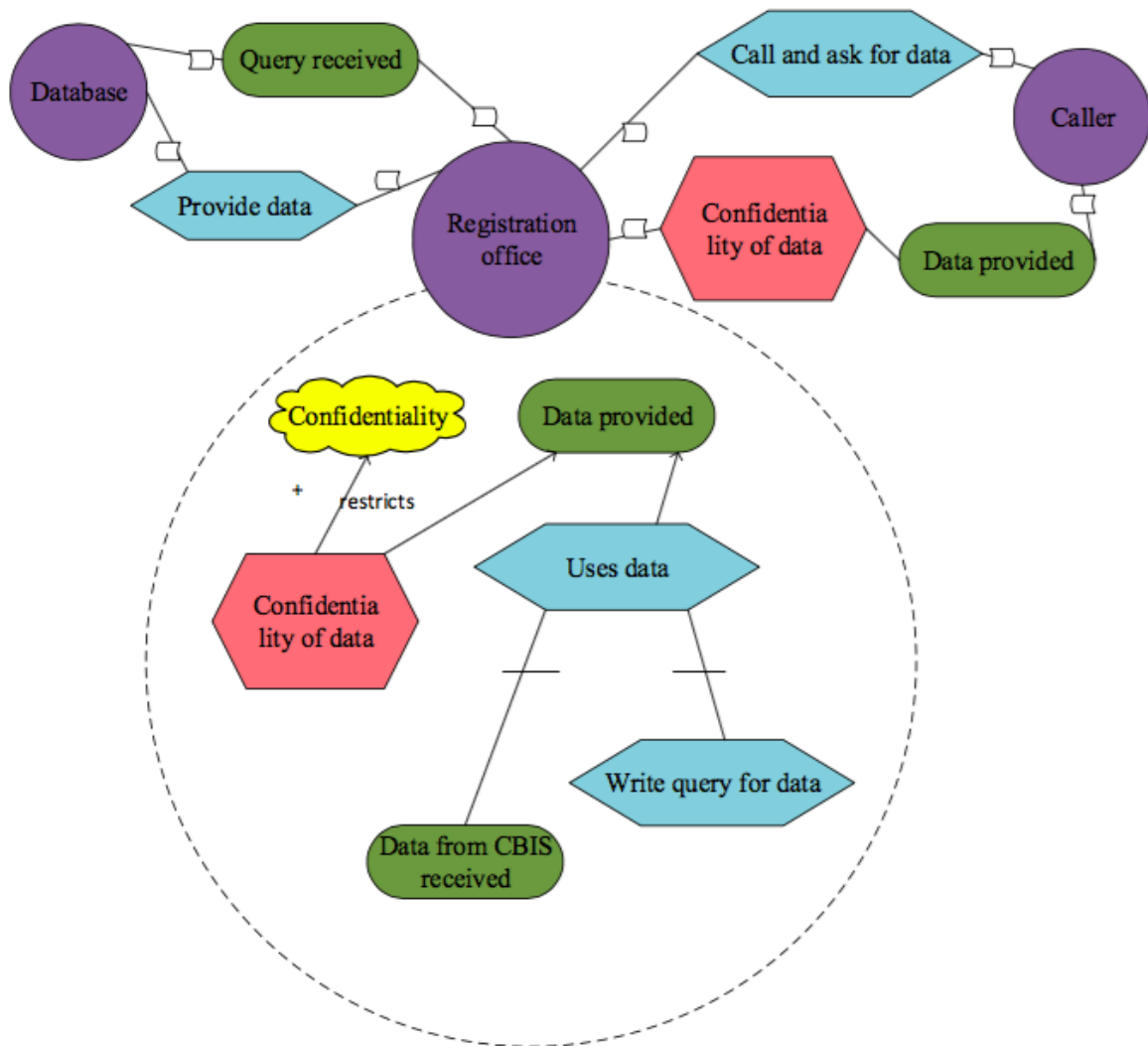


Figure 41. Through Internet – Secure Tropos asset identification

Risk analysis. Next Figure 42 is focused on a possible event of the risk exposure. It describes a situation where a threat agent (e.g., *malicious caller*) wished to get an information from the Registration office (e.g., *Registration office*). An attacker damages Data in the data provided. The Social engineering attack impacts Privacy. Malicious caller has a threat (*Use data for not intended purpose*) to support of data provided. Attacker attacks data provided through exploiting the vulnerability identified in uses data. The exploits link shows a relationship between an attack method (*Call and ask for data*) and a vulnerable IS asset (*Uses data*).

Security requirements definition. In order to mitigate risks, we have designed goals and plans. In current example plan is Check ID. It is shown in a dotted background pattern.

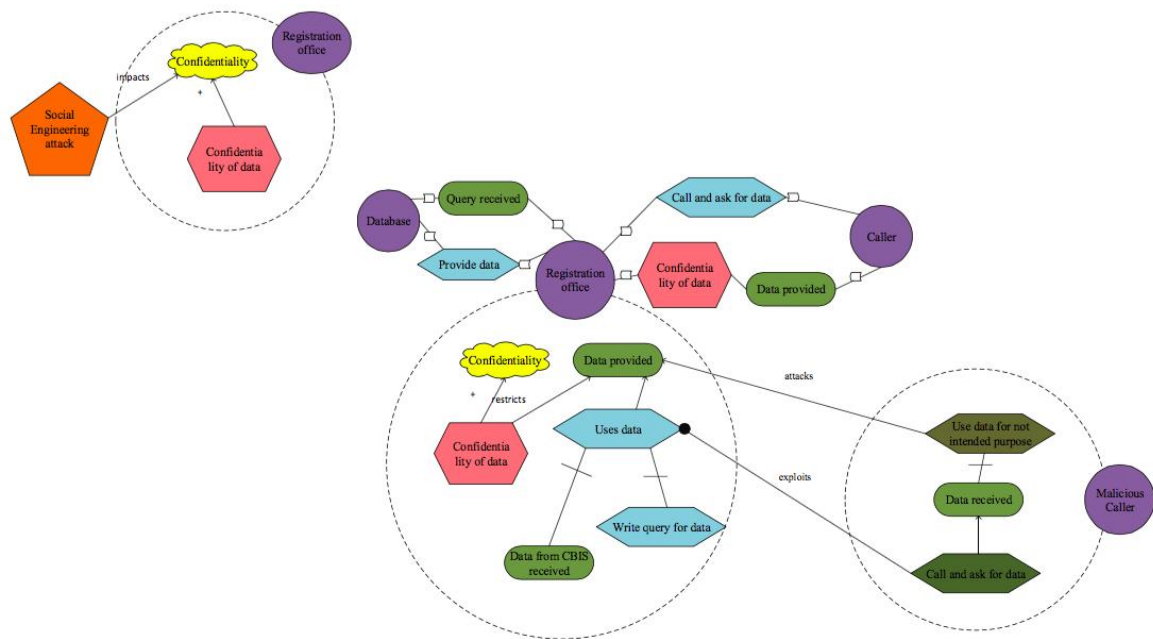


Figure 42. Through Internet – Secure Tropos risk identification

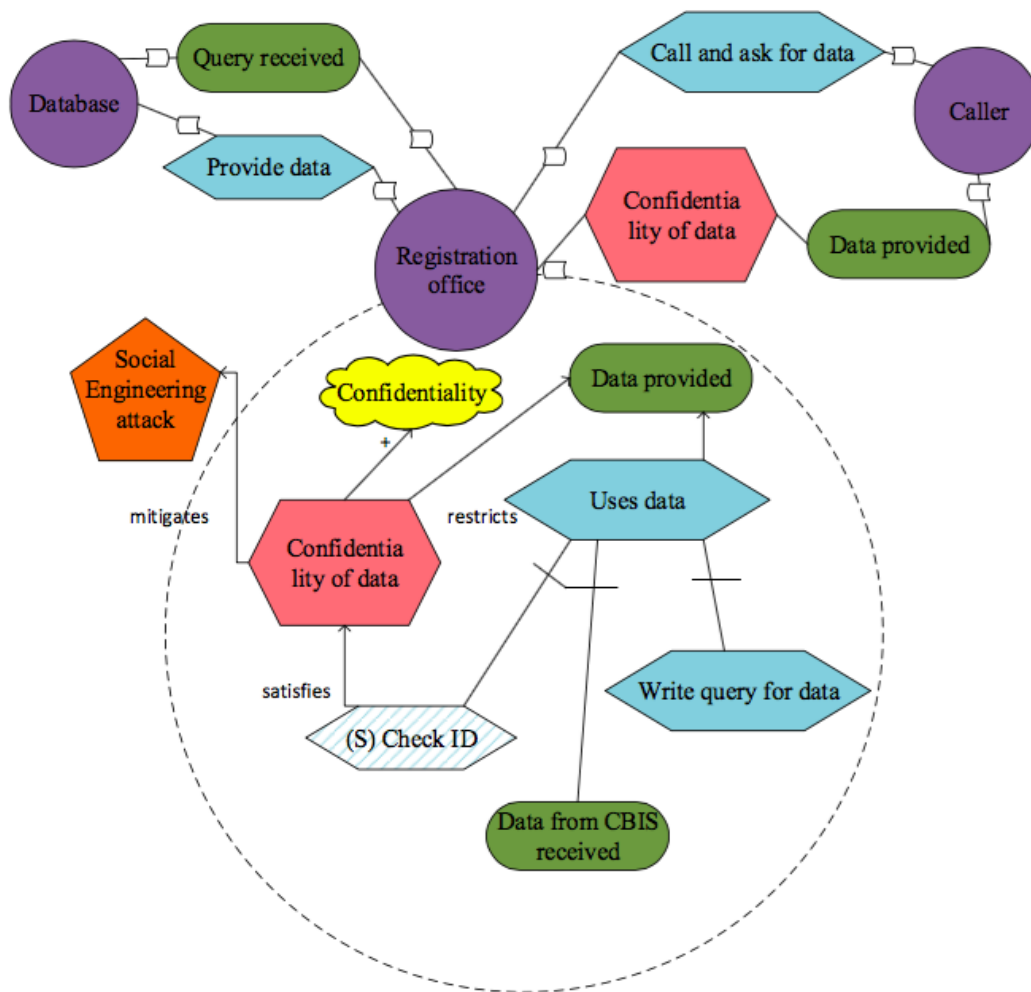


Figure 43. Through Internet – Secure Tropos risk treatment

Through Persuasion

Asset identification. Illustration to the applied Secure Tropos security extension to the case “Through persuasion” is presented in Figure 44. Here is represented only goals (e.g., *Query received*) and plans (e.g., *provide data*). In Secure Tropos security objectives are identified by softgoals (e.g., *Confidentiality*) and by security criteria which is communicated with security constraints (e.g., *Confidentiality of data*).

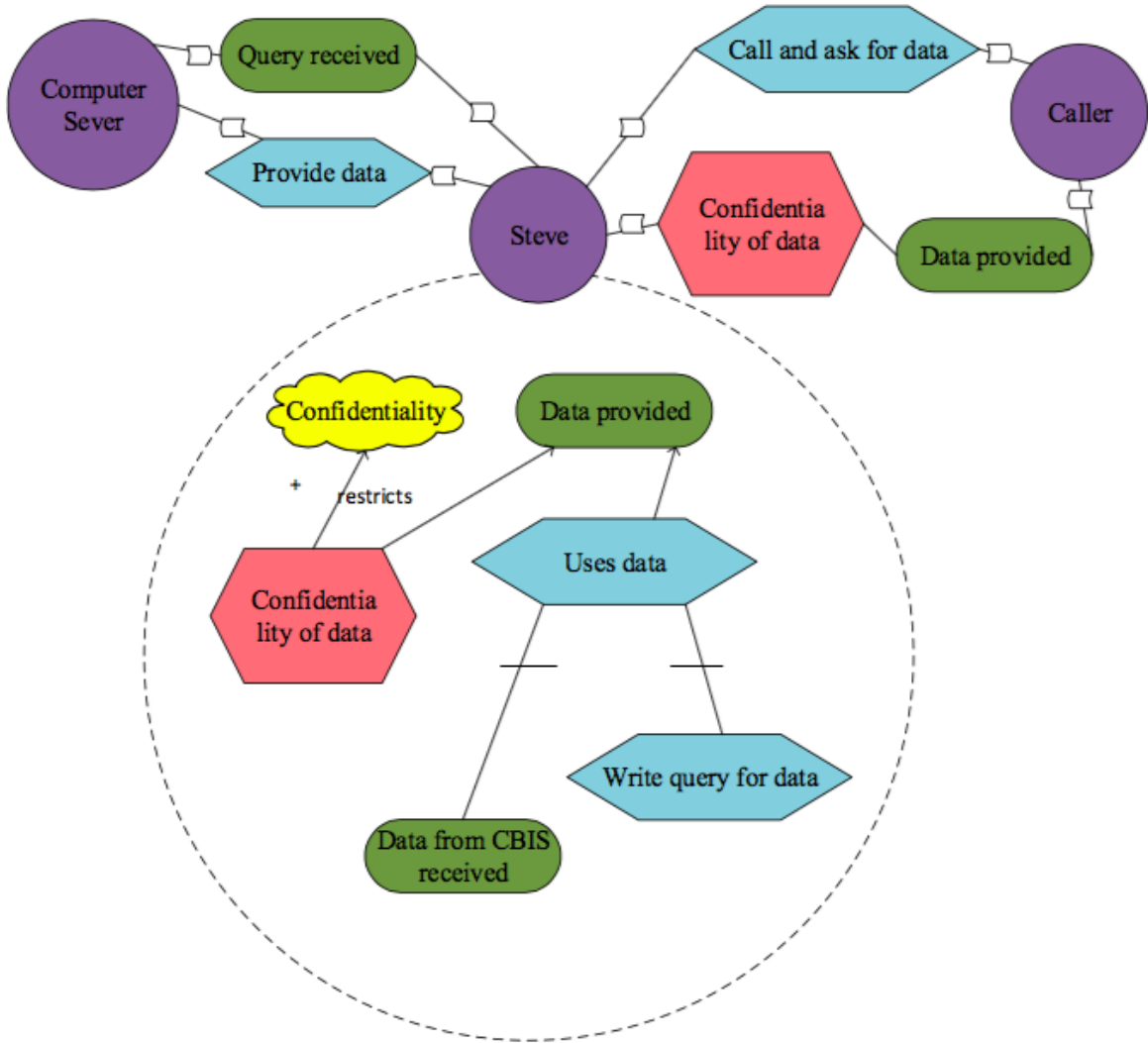


Figure 44. Through persuasion – Secure Tropos asset identification

Risk analysis. Next Figure 45 is focused on a possible event of the risk exposure. It describes a situation where a threat agent (e.g., *malicious caller*) wished to get an information from the Steve (e.g., *Steve*). An attacker damages Data in the data provided. The Social engineering attack impacts Privacy. Malicious caller has a threat (*Use data for not intended purpose*) to support of data provided. Attacker attacks data provided through exploiting the vulnerability identified in uses data. The exploits link shows a relationship between an attack method (*Call and ask for data*) and a vulnerable IS asset (*Uses data*).

Security requirements definition. In order to mitigate risks, we have designed goals and plans. In current example plan is Check ID. It is shows in a dotted background pattern.

Breaking Through Computer Network

Asset identification. Illustration to the applied Secure Tropos security extension to the case “Breaking through computer network” is presented in Figure 47. Here is represented only goals (e.g., *Query received*) and plans (e.g., *provide data*). In Secure Tropos security objectives are identified by softgoals (e.g., *Confidentiality*) and by security criteria which is communicated with security constraints (e.g., *Confidentiality of data*).

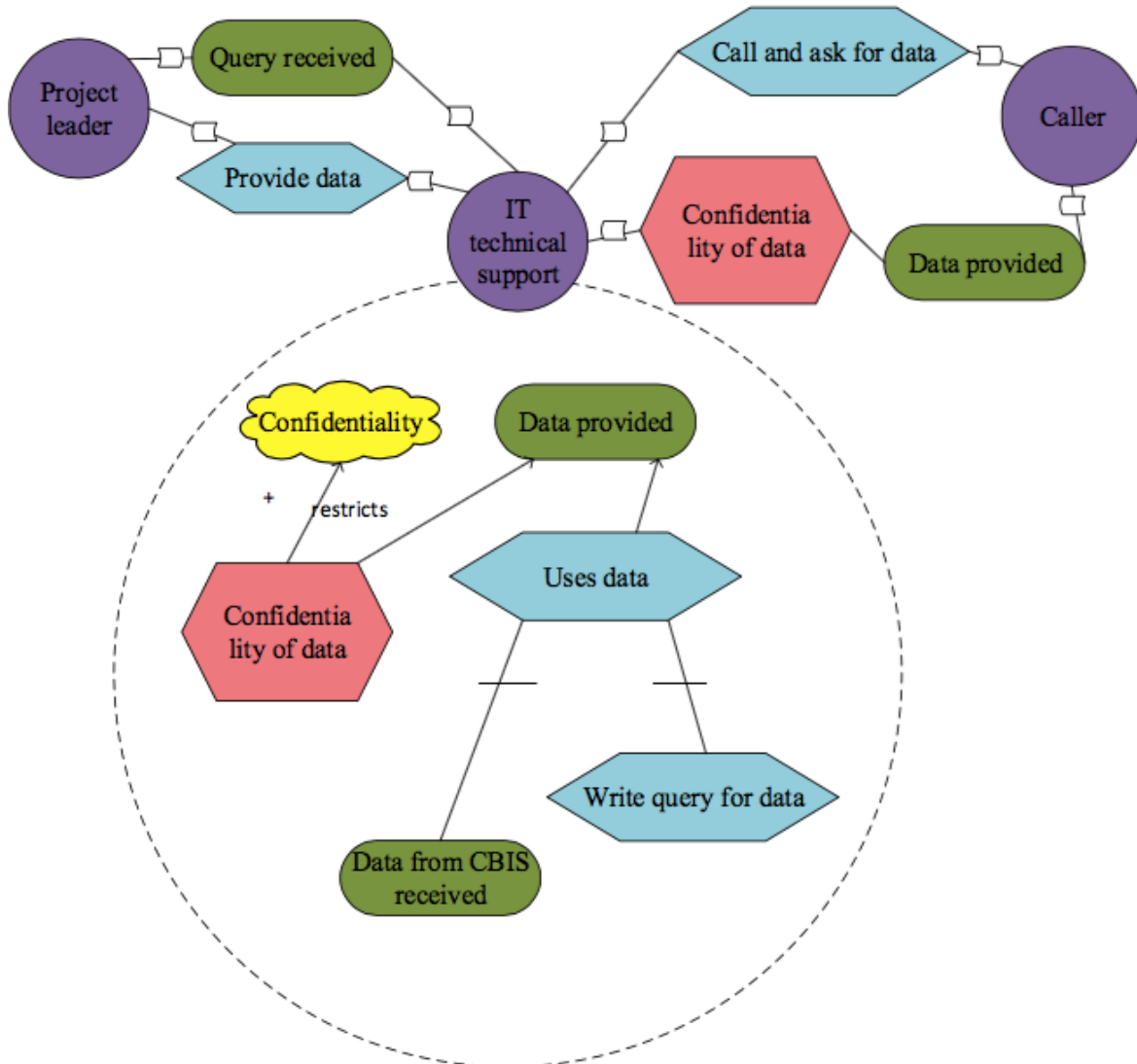


Figure 47. Breaking through computer network – Secure Tropos asset identification

Risk analysis. Next Figure 48 is focused on a possible event of the risk exposure. It describes a situation where a threat agent (e.g., *Ivan Peter*) wished to get an information from the IT technical support (e.g., *IT technical support*). An attacker damages Data in the data provided. The Social engineering attack impacts Privacy. Malicious caller has a threat (*Use data for not intended purpose*) to support of data provided. Attacker attacks data provided through exploiting the vulnerability identified in uses data. The exploits link shows a relationship between an attack method (*Call and ask for data*) and a vulnerable IS asset (*Uses data*).

Security requirements definition. In order to mitigate risks, we have designed goals and plans. In current example plan is Check ID. It is shown in a dotted background pattern.

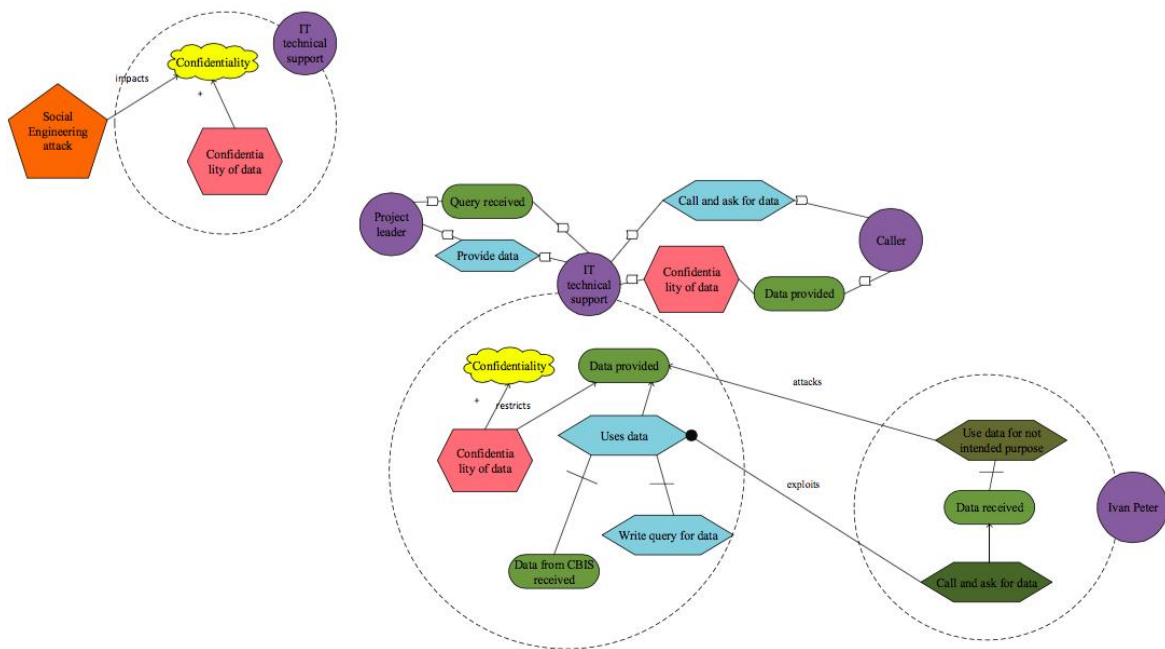


Figure 48. Breaking through computer network – Secure Tropos risk identification

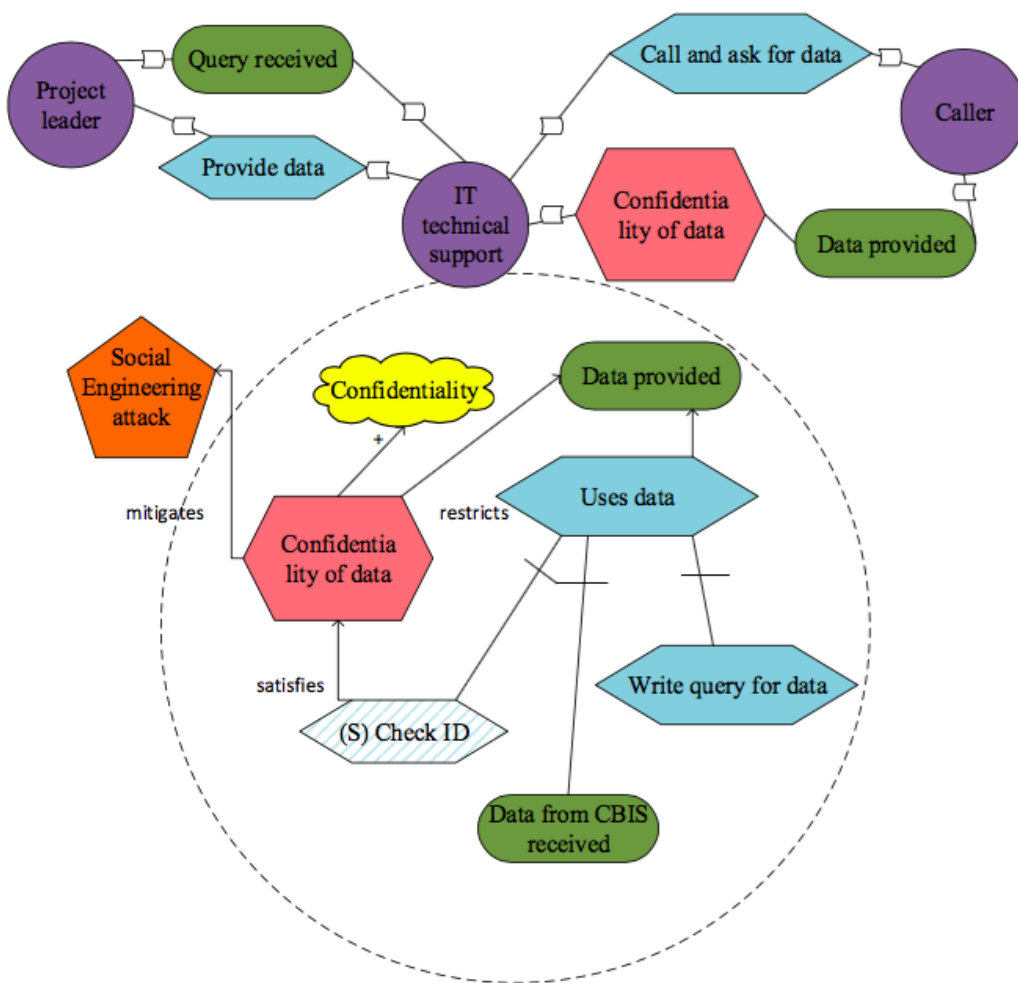
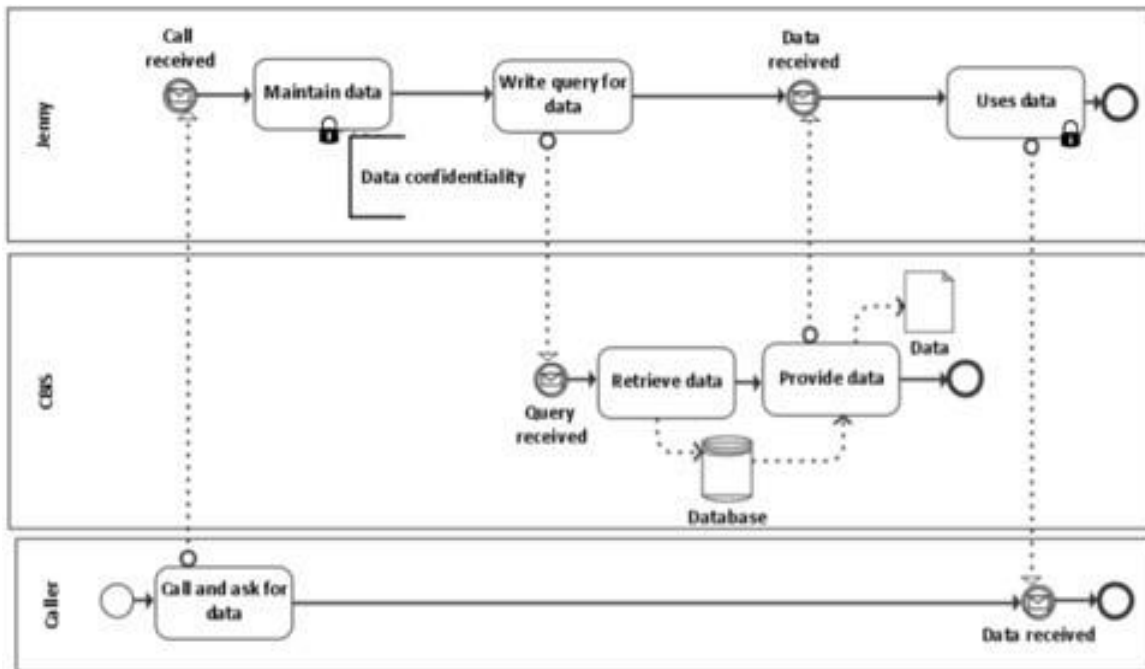
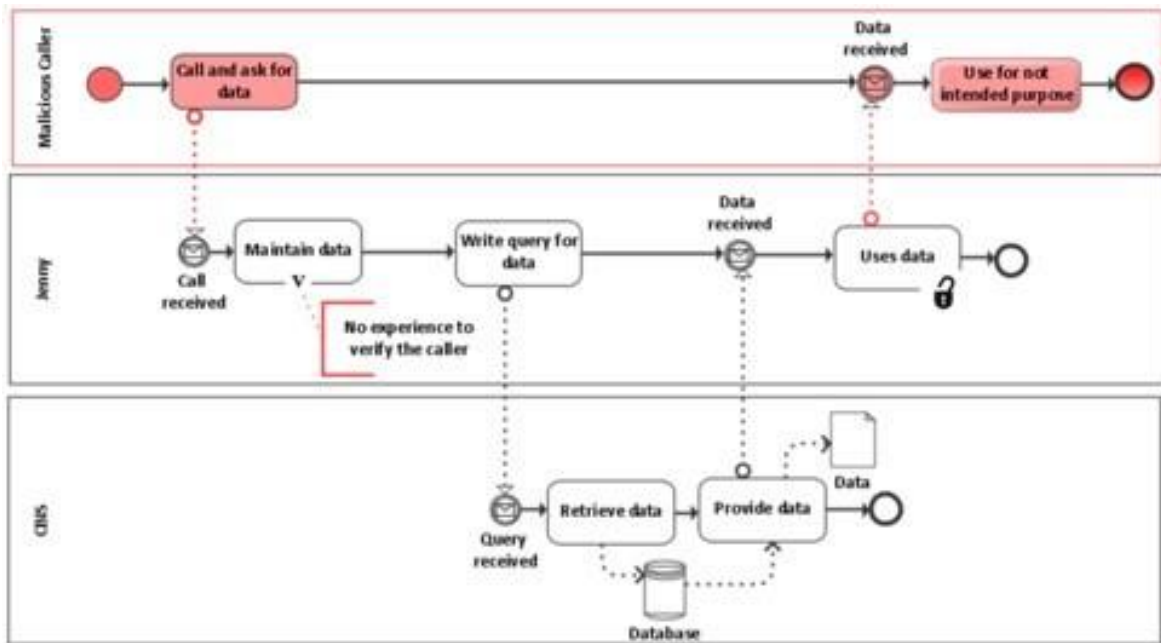


Figure 49. Breaking through computer network – Secure Tropos risk treatment

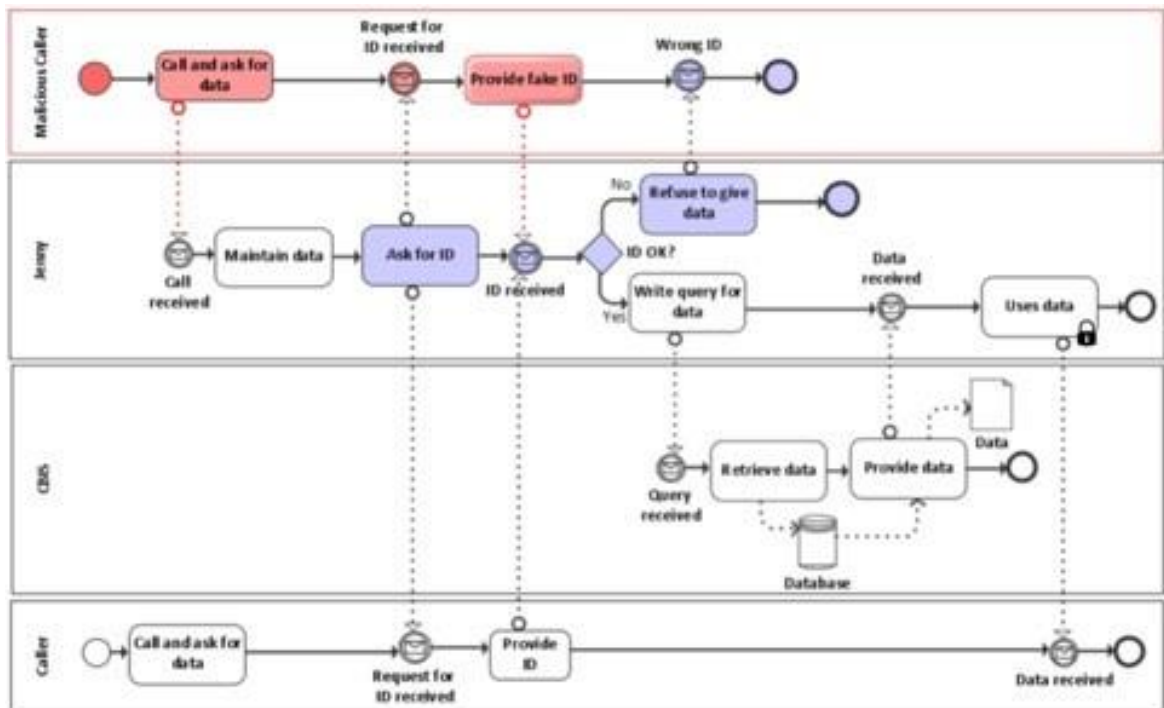
V. Questionnaire of BPMN



	What is ...?	Which language construct expresses ...?
Business Asset		
IS Asset		
Security criterion		

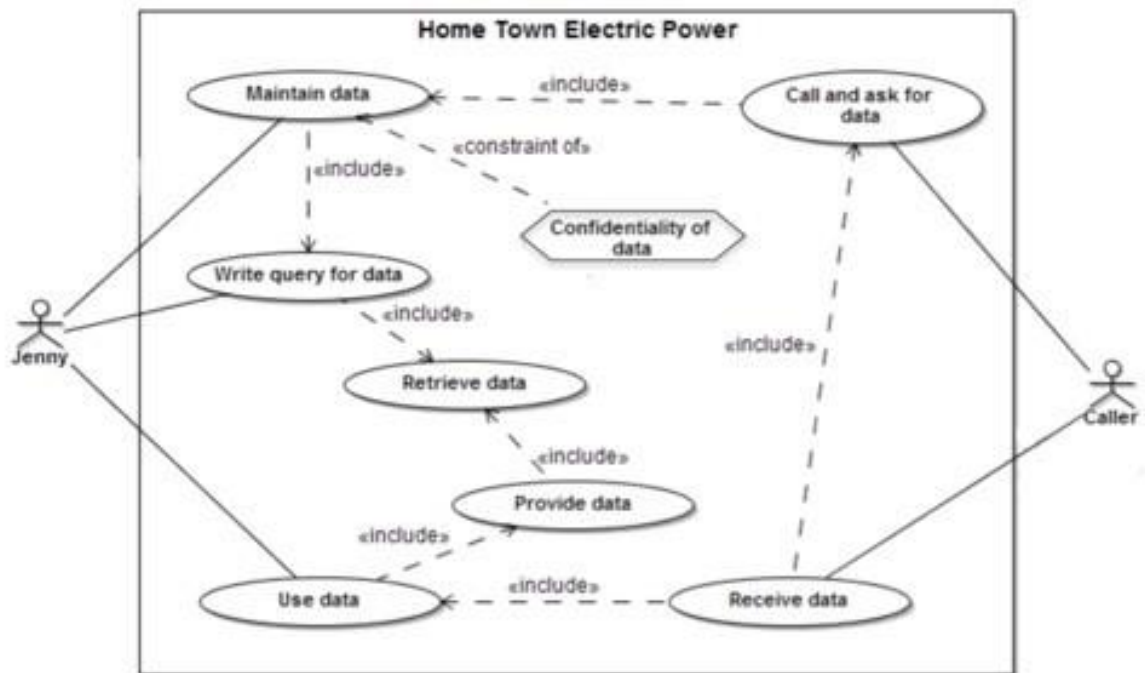


	What is ...?	Which language construct expresses ...?
Risk		
Impact		
Event		
Vulnerability		
Threat		
Threat agent		
Attack method		

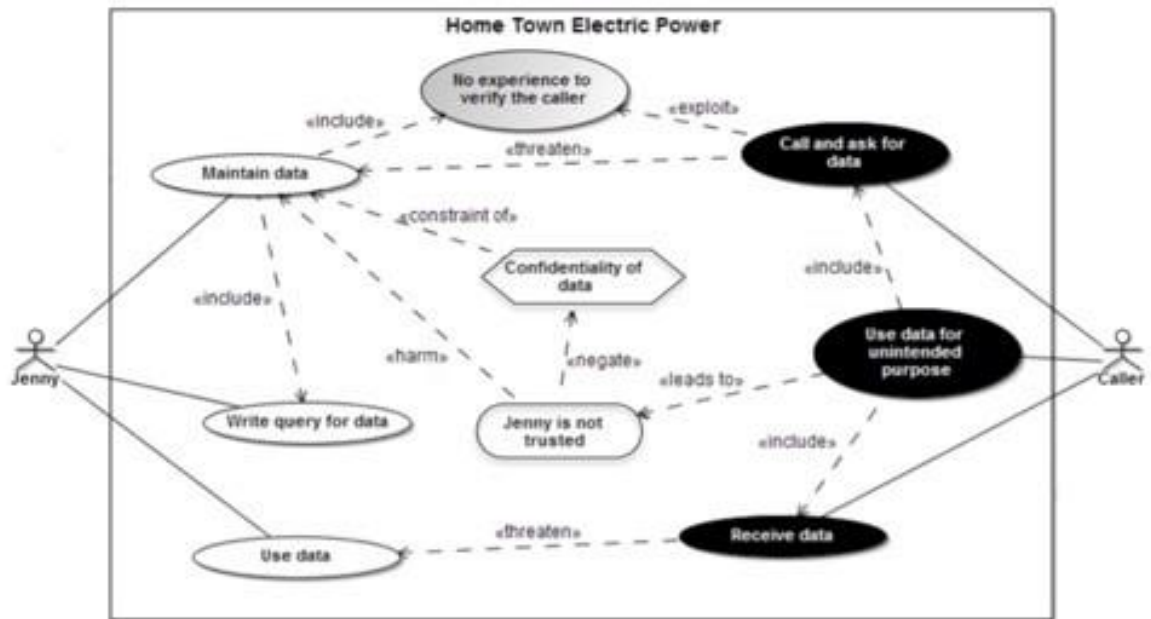


	What is ...?	Which language construct expresses ...?
Risk treatment decision		
Security requirement		
Control		

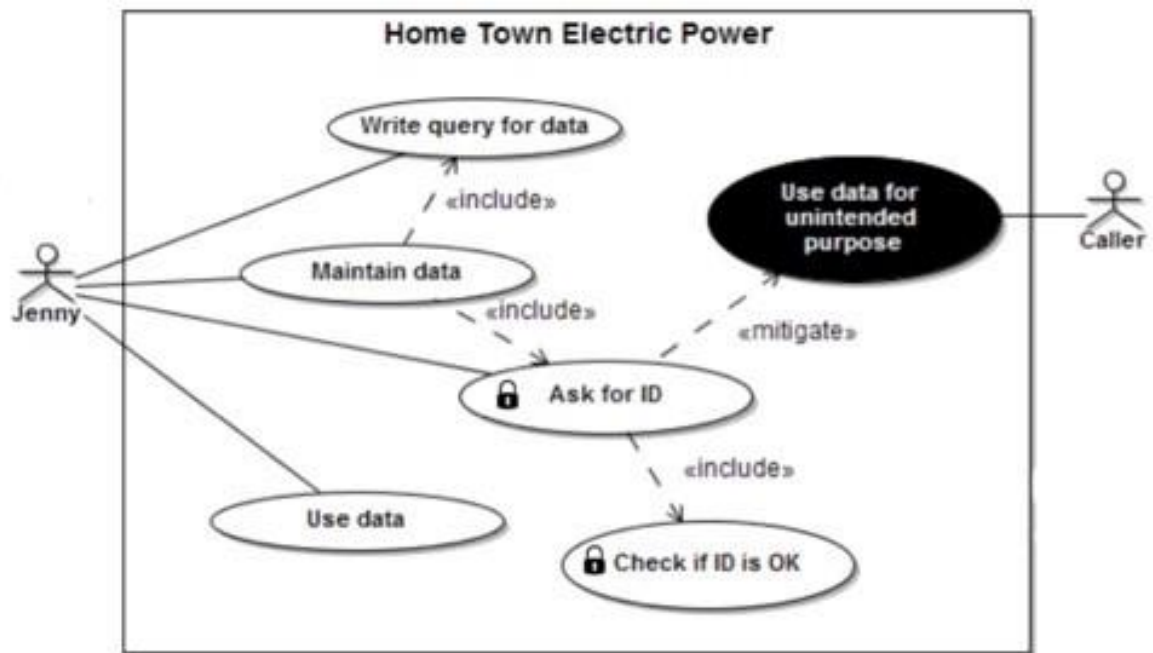
VI. Questionnaire of Misuse Case



	What is ...?	Which language construct expresses ...?
Business Asset		
IS Asset		
Security criterion		

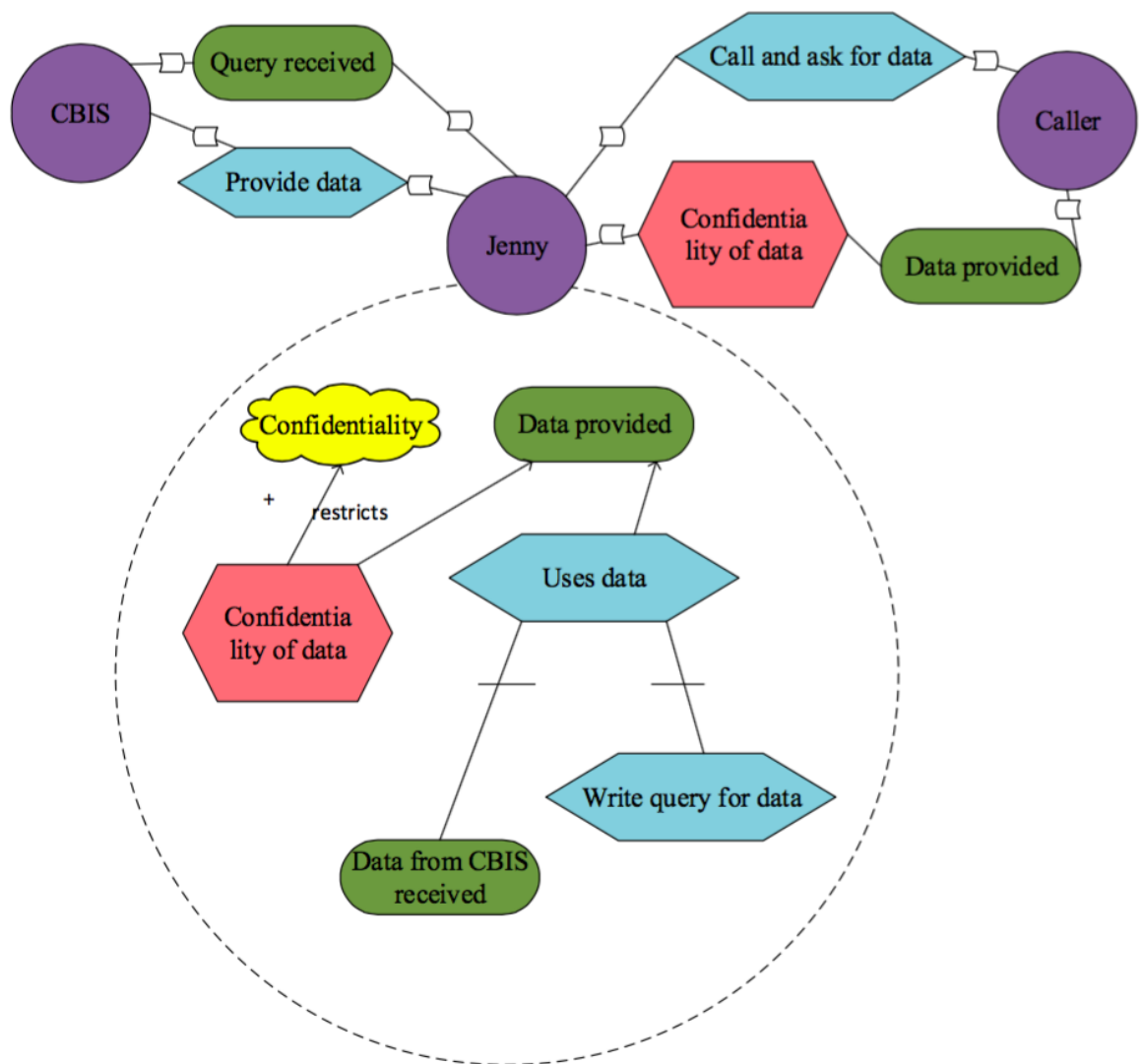


	What is ...?	Which language construct expresses ...?
Risk		
Impact		
Event		
Vulnerability		
Threat		
Threat agent		
Attack method		

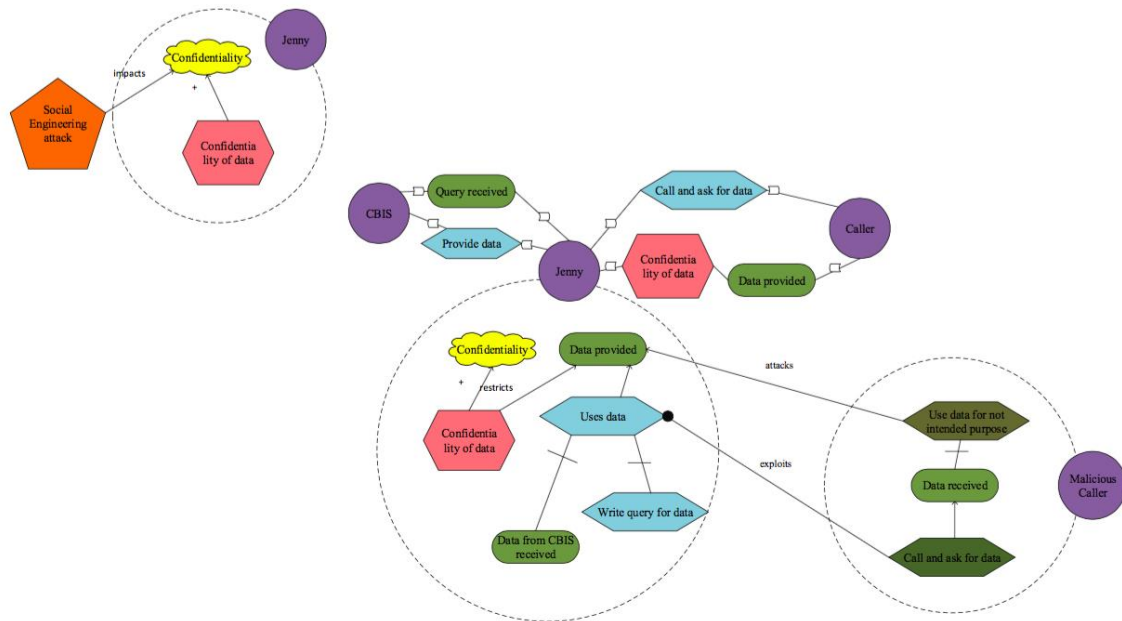


	What is ...?	Which language construct expresses ...?
Risk treatment decision		
Security requirement		
Control		

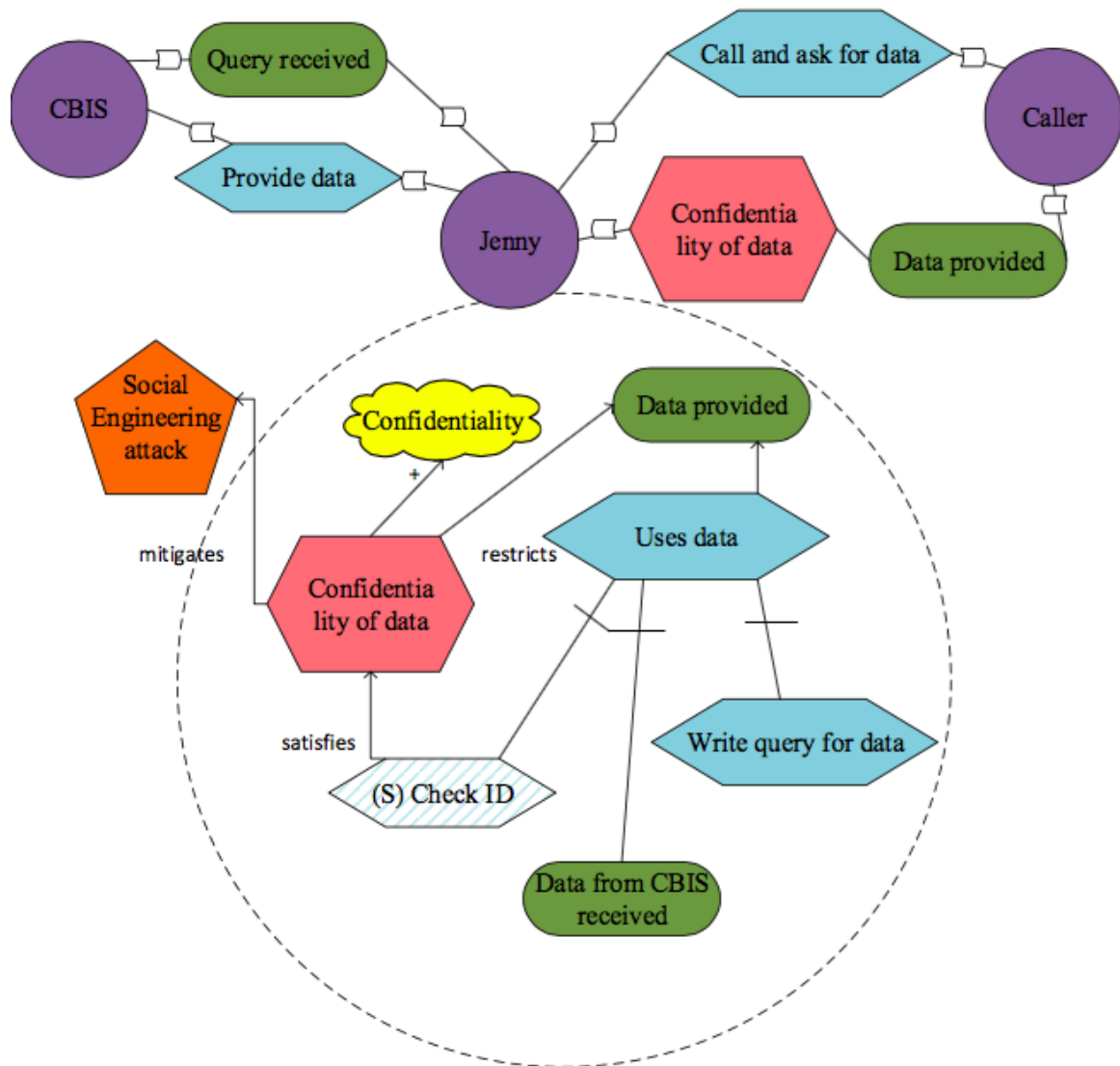
VII. Questionnaire of Secure Tropos



	What is ...?	Which language construct expresses ...?
Business Asset		
IS Asset		
Security criterion		



	What is ...?	Which language construct expresses ...?
Risk		
Impact		
Event		
Vulnerability		
Threat		
Threat agent		
Attack method		



	What is ...?	Which language construct expresses ...?
Risk treatment decision		
Security requirement		
Control		

VIII. Data upon BPMN Concepts and Constructs

BPMN concept results/ 'What is ...?'	Concept	1	2	3	4	5	6	7	8	9	10	11	12	Results
Business Asset	Data	-	-	+	+	+	-	+	+	+	-	+	+	4/12
	Caller and its business process including Call and ask for data and Data received	-	+	-	+	-	-	-	-	-	-	-	+	9/12
	Jenny tasks Maintain data and Uses data could be considered as business asset under some circumstance	+	+	-	+	+	+	+	-	-	+	-	-	5/12
IS Asset	Jenny	-	-	-	-	-	-	-	-	-	-	-	-	12/12
	Jenny's process write query for data, data received	-	-	+	-	-	-	-	-	-	-	-	-	11/12
	Process executed in CBIS	+	+	+	+	-	-	-	-	-	-	+	-	7/12
	Database	+	+	+	+	+	+	+	+	+	+	+	+	0
Security criterion	Confidentiality	+	+	+	+	+	+	+	+	+	+	+	+	0

BPMN concept results/ 'What is ...?'	Concept	1	2	3	4	5	6	7	8	9	10	11	12	Results
Risk	Malicious caller	+	+	+	-	-	+	+	-	+	+	+	+	3/12
	Malicious caller calls and asks for data, receives data, and uses data for not intended purpose	+	+	+	-	-	-	-	-	-	+	+	+	6/12
	Jenny has no experience to verify the caller	-	-	+	-	+	+	+	-	+	-	+	+	5/12
	Data confidentiality negation and data reception for unintended use.	+	+	+	-	+	-	-	-	-	+	+	+	5/12
Impact	Data confidentiality negated	+	+	+	-	-	-	+	-	+	-	+	+	5/12
	Data received	+	-	-	-	-	-	-	-	-	-	-	-	11/12
	Harm to Jenny is not indicated	-	-	-	-	-	-	-	-	-	-	-	-	12/12
Event	Malicious caller calls and asks for data, receives data, and uses data for not intended purpose	+	+	+	+	+	+	+	-	-	+	+	-	3/12
	Jenny has no experience to verify the caller	+	+	+	-	+	+	+	-	+	+	+	-	3/12

Vulnerability	Jenny has no experience to verify the caller	+	+	+	-	+	+	+	-	+	+	+	+	2/12
Threat	Malicious caller calls and asks for data, receives data, and uses data for not intended purpose	-	+	+	+	+	+	+	-	-	+	-	-	5/12
Threat agent	Malicious caller	+	+	+	+	+	+	+	-	+	+	+	+	1/12
Attack method	Call and ask for data	-	-	+	-	-	-	+	-	-	+	+	-	8/12
	Data received	-	+	-	-	-	-	-	-	-	-	-	-	11/12
	Use for not intended purpose	-	-	-	-	-	-	-	-	-	-	-	-	12/12

BPMN concept results/ 'What is ...?'	Concept	1	2	3	4	5	6	7	8	9	10	11	12	Results
Risk treatment decision	Data reduction	-	-	+	+	-	-	-	-	-	-	-	-	10/12
Security re-requirement	Ask for ID	+	-	+	+	+	+	-	-	+	+	+	+	3/12
	After ID is received check if ID is ok	+	-	+	+	+	+	-	-	+	-	+	+	4/12
	If not refuse to give data	+	-	+	+	+	+	+	-	+	-	+	+	3/12
Control	Not proposed	-	-	-	-	-	-	-	-	-	-	-	-	12/12

BPMN construct results	Concept	1	2	3	4	5	6	7	8	9	10	11	12	Results
Business Asset	Data store	-	-	-	-	+	-	-	+	+	-	+	-	8/10
	Combination of Flow objects (tasks, sequence flow and events)	+	+	-	+	-	-	-	-	-	-	+	-	8/10
IS Asset	Pool	-	+	-	+	+	+	+	+	-	-	-	-	6/10
	Combination of Flow objects (tasks, sequence flow and events)	-	-	-	+	-	-	-	-	-	-	-	-	11/10
Security criterion	Annotation	-	+	-	-	-	+	+	+	+	-	+	-	7/10

BPMN constructs re- sults	Concept	1	2	3	4	5	6	7	8	9	10	11	12	Results
Risk	Combination of event and impact	-	-	-	-	-	+	+	+	+	-	+	+	6/10
Impact	Unlock	-	-	-	-	+	+	+	+	+	-	+	+	5/10
	Event	-	-	-	-	-	-	-	-	-	-	-	-	12/10
Event	Combination of constructs for Threat and Vulnerability	+	-	-	-	+	+	+	+	+	-	+	+	4/10
Vulnerability	Annotation	+	+	-	-	+	+	+	+	+	-	+	+	3/10
Threat	Combination of constructs for Threat agent and Attack method	+	-	-	+	+	+	+	+	+	-	+	+	3/10
Threat agent	Pool	+	+	-	+	+	+	+	+	+	-	+	+	2/10
Attack method	Combination of flow objects (tasks and event) using sequence flow	+	+	-	+	+	+	+	+	-	-	+	+	3/10
Risk treatment decision	No constructs	-	+	-	+	-	+	+	+	+	-	+	+	4/10
Security requirement	Combination of Flow objects (tasks, gateways and events) using Sequence Flow	+	+	-	+	+	+	+	+	+	-	+	-	3/10
Control	No constructs	-	+	-	-	+	+	+	+	-	-	+	-	6/10

IX. Data upon Misuse Case Concepts and Constructs

MUC concepts results	Concept	1	2	3	4	5	6	7	8	9	10	Results
Business Asset	Data	+	-	-	+	-	-	-	+	+	+	5/10
	Call and ask for data, receive data	+	+	+	-	+	+	-	+	-	-	4/10
	Under some circumstance: use cases like Maintain data, Write query for data, Uses data	+	+	+	-	-	+	+	-	-	-	5/10
IS Asset	Combination of use cases, like Maintain data, Write query for data, Use data, Retrieve data, Provide data	-	+	-	-	-	+	+	-	-	-	7/10
	Home Town Electric Power	-	-	+	-	-	-	-	-	-	-	9/10
Security criterion	Confidentiality of data	-	+	+	+	+	+	+	+	+	+	1/10

MUC concepts results	Concept	1	2	3	4	5	6	7	8	9	10	Results
Risk	Malicious caller	+	-	+	-	+	-	-	-	-	-	7/10
	Malicious caller calls and asks for data, receives data, and uses data for not intended purpose	-	-	-	-	-	-	-	-	-	-	10/10
	Jenny has no experience to verify the caller	+	+	-	+	+	-	-	-	-	+	5/10
	Data confidentiality negation and data reception for unintended use.	+	+	+	-	+	-	+	+	-	-	4/10
Impact	Negate confidentiality of data	+	+	+	+	+	+	+	+	+	-	1/10
	Jenny is not trusted (harm to IS asset)	+	+	+	-	-	-	+	-	+	-	5/10
	Harm to maintain data (harm to business asset)	-	-	-	-	-	-	+	-	-	-	9/10
Event	Malicious caller calls and asks for data, receives data, and uses data for not intended purpose	+	-	-	-	+	+			+	-	4/10

	Jenny has no experience to verify the caller	+	+	-	+	+	-	-	-	+	+	2/10
Vulnerability	No experience to verify the caller when maintaining the data	+	+	+	--	+	+	+	-	+	+	2/10
Threat	Caller calls and asks for data, receives data, and uses data for unintended purpose	+	+	-	-	-	+	-	-	-	-	7/10
Threat agent	Malicious caller	+	+	+	+	+	+	+	+	+	+	0
Attack method	Call and ask for data	+	+	+	-	-	+	-	-	-	-	5/10
	Data received	+	+	-	-	-	-	-	-	-	-	8/10
	Use for not intended purpose	+	-	-	-	-	-	-	-	-	-	9/10

MUC concepts results	Concept	1	2	3	4	5	6	7	8	9	10	Results
Risk treatment decision	Data reduction	-	-	-	-	-	-	-	-	-	-	10/10
Security re-requirement	Ask for ID,	+	-	-	+	-	-	+	+		-	6/10
	check if ID is OK if not refuse to give data	-	-	-	+	-	-	+	+	-	-	7/10
Control	Not modelled	-	-	-	-	-	-	-	-	-	-	10/10

MUC constructs results	Concepts	1	2	3	4	5	6	7	8	9	10	Re-sults
Business Asset	Uses cases and appropriate link to express include	-	-	-	-	-	+	+	+	-	-	7/10
IS Asset	Use cases	-	-	-	-	-	+	+	-	+	-	7/10
	System boundary	-	-	-	-	-	-	-	-	+	-	9/10
Security Criterion	Construct for security criterion “hez-agon” and link express constraint of	-	-	-	-	+	+	+	+	+	-	5/10

MUC results	constructs	Concepts	1	2	3	4	5	6	7	8	9	10	Results
Risk		Combination of event and impact	-	-	-	-	-	-	-	+	-	-	9/10
Impact		Impact construct and appropriate links to express harm and negation of security criterion	-	+	-	-	-	-	+	-	+	+	6/10
Event		Combination of constructs used to express threat and vulnerability	-	-	-	-	-	+	+	+	+	-	6/10
Vulnerability		Vulnerability use case	+	-	-	-	-	+	+	-	+	+	5/10
Threat		Combination of misuser and misuse cases are linked by include	-	+	-	-	+	+	+	-	+	-	5/10
Threat agent		Misuser	-	+	-	-	+	+	+	-	+	-	5/10
Attack method		Misuse case construct and link include cases	-	-	-	-	-	+	-	-	-	-	9/10
Risk treatment decision		No construct	-	-	-	-	-	-	-	+	-	-	9/10
Security requirement		Security use case construct and link include	+	+	-	-	-	-	+	-	-	-	7/10
Control		No construct	-	-	-	-	-	-	-	+	-	-	9/10

X. Data upon Secure Tropos Concepts and Constructs

Secure Tropos concepts results	Concepts	1	2	3	4	5	6	7	8	9	10	11	12	Results
Business asset	Data	-	+	+	-	-	+	+	+	+	-	+	-	5/12
	Under some circumstances as business asset could be considered: write query for data and data provided	-	+	+	+	+	+	-	+	-	-	-	+	5/12
	Call and ask for data	+	+	+	+	+	+	-	+	+	-	+	+	2/12
	Caller and Jenny	-	+	-	+	+	+	-	+	-	-	+	-	6/12
IS asset	Jenny	+	-	+	-	-	-	+	-	-	+	-	+	7/12
	Jenny's process: write query for data, uses data, data provided	-	-	-	-	-	-	-	-	-	-	-	-	12/12
	Process executed in CBIS as query received, provided data, data from CBIS received	+	+	+	+	+	+	+	+	+	-	+	+	1/12
Security criterion	Confidentiality of data	+	+	+	+	-	+	+	+	+	+	+	+	1/12
	Confidentiality	+	-	-	+	+	-	-	+	-	+	-	-	7/12

Secure Tropos concepts results	Concepts	1	2	3	4	5	6	7	8	9	10	11	12	Results
Risk	Malicious caller calls and asks for data, receives data and uses data for not intended purpose	-	-	-	+	-	+	+	+	+	+	+	+	4/12
	to exploit use of data	-	+	-	-	-	+	+	-	-	-	-	-	9/12
	attack data	-	-	-	-	-	+	+	-	-	-	+	-	9/12
	social engineering attack has been used to negate confidentiality of data	+	-	+	-	+	+	+	+	-	+	-	+	4/12
Impact	Social engineering attack impacts confidentiality of data	+	-	+	+	+	+	-	+	+	+	+	+	2/12
Event	Malicious caller calls and asks for data, receives data and uses data for not intended purpose	+	+	+	+	-	+	+	+	-	-	+	+	3/12
	to exploit use of data	-	-	+	-	-	+	+	+	-	-	-	-	8/12
	attack data	-	+	-	-	-	+	+	+	-	-	-	-	8/12
	social engineering attack has been used to negate confidentiality of data	-	+	+	+	+	+	+	+	+	+	+	-	2/12

Vulnerability	Not clearly identified but points out that vulnerable is use of data	+	+	+	-	-	-	-	-	-	-	-	+	8/12
Threat	Malicious caller calls and asks for data, receives data and uses data for not intended purpose	-	-	+	+	+	-	-	-	-	+	+	+	6/12
Threat agent	Malicious caller	+	+	+	+	+	+	+	+	+	+	+	+	0
Attack method	calls and asks for data, receives data and uses data for not intended purpose	+	-	+	+	+	-	-	-	-	-	-	+	7/12
Risk treatment decision	risk reduction	-	+	+	-	+	+	-	+	-	+	-	+	5/12
Security re-requirement	check ID	-	+	-	+	+	+	+	-	+	+	-	-	5/12
Control	not proposed	-	-	-	+	-	-	-	-	-	-	-	-	11/12

Secure Tropos constructs re-sults	Concepts	1	2	3	4	5	6	7	8	9	10	11	12	Results
Business Asset	Actor supports hardgoal dependency and plan dependency	+	+	+	+	+	+	+	+	+	+	+	+	0
IS Asset	Actor	+	+	-	+	+	+	+	+	+	+	-	+	2/12
	composition of the plan, hardgoal using decomposition, mean-ends relationships	-	+	+	+	+	+	-	+	+	+	+	-	3/12
Security criterion	Security constraint contribution	+	+	+	+	-	+	+	+	+	+	+	+	1/12
	Softgoal	+	+	+	-	+	-	-	+	-	+	+	+	4/12
Risk	Combination of event and impact	+	-	+	-	-	-	+	-	-	+	-	+	7/12
Impact	Impacts	+	-	+	-	-	-	+	-	-	-	+	+	7/12
Event	Combination of an agent, goal, plan, exploits and vulnerability point	+	-	-	-	-	-	-	-	-	-	-	+	10/12
	Threat	-	+	+	-	+	+	+	+	+	+	+	-	3/12
Vulnerability	Vulnerability is not modelled, but vulnerability points can be identified by the attributes of the assets	-	-	-	-	-	-	+	-	-	-	-	-	11/12
Threat	Combination of construct for	-	+	+	+	+	+	-	+	+	+	+	+	2/12

	Threat agent and Attack method													
Threat agent	Agent	+	+	+	+	+	+	+	+	+	+	+	+	0
Attack method	Agent executes plan and goal using mean- ends, decompo- sition relation- ships	+	+	+	+	+	+	+	+	+	+	+	+	0
Risk treatment decision	No constructs	+	-	-	-	-	+	-	-	-	-	-	-	10/12
Security re- quirement	Plan that has dotted back- ground pattern	-	+	-	+	+	+	+	+	+	+	+	-	3/12
Control	No constructs	-	-	-	-	-	-	-	-	-	+	-	-	11/12

License

Non-exclusive licence to reproduce thesis and make thesis public

I, **Sarbar Tursunova** (date of birth: 08.12.1988),

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:
 - 1.1. reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and
 - 1.2. make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright, of my thesis

Comparing Security Risk-oriented Modelling Languages to Manage Social Engineering Risks,

Supervised by Raimundas Matulevičius,

2. I am aware of the fact that the author retains these rights.
3. I certify that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu, **25.05.2015**