A Review of Risk Identification Approaches in the Telecommunication Domain

Ahmed Seid Yesuf
Deutsche Telekom Chair of Mobile Business & Multilateral Security, Goethe University Frankfurt,
Frankfurt am Main, Germany
ahmed.yesuf@m-chair.de

Keywords: Risk Identification, Security, Telecommunication Service, Risk Assessment, Fraud Risk, Risk Management.

Abstract: Risks in the telecommunication (telco) domain are complex to identify due to the involvement of several independent stakeholders and the difficulty of predicting emerging threats to the services. This is costing the Telecom operators billions of dollars. We believe the little emphasis given to the important step of risk assessment process – risk identification (RI) – is the main reason for this loss. Unlike other domains, the proprietary nature of Telecom systems makes it challenging to show the risk assessment approaches in the domain. In this paper, we investigate the classifications of the RI approaches from the literature written on the telco and other related domains. We also investigate the research trends in the last 16 years when Telecom risks are evolving and the revenue loss of Telecom operators is largely affected. Based on our review, we also show future research directions in the domain.

1 INTRODUCTION

The lives of people are changing through time since the beginning of telecommunication (telco) services. Individuals able to communicate with their families, friends and relatives from almost anywhere using data, voice or video communication services. Companies and organisations facilitate their tasks better than ever using the telco services. Telecom companies strive to deliver their services considering customers' information security and privacy requirements into consideration. It is also obvious that they want to protect their revenue stable and profitable. The responsibilities of a Telecom companies include accepting, delivering and transmitting the message from a sender to a recipient. Typical telco services are roaming, VoIP, PBAX service, national and international messaging and call services. Unfortunately, attackers or fraudsters are working to deform the telco services to gain individual or organised benefit, for instance, using the service without payment.

According to the Communication Fraud Control Association (CFCA)(CFCA, 2015), fraud is the use of telco services or products with no intention of payment. Thus, fraud *negatively* affect the global telco revenue. In 2015, fraud affect the global Telecom revenue by almost $38.1 billion USD. It is lower from the previous reporting years because the Telecom operators outsource their fraud risk management to the third party companies. Even though there is momentum in reduction of fraud loss from 2009, it requires a lot of work in risk reduction from the Telecom operators' perspective. The estimated global loss from 2000 is shown in Table 1. The two top most sustainable fraud categories from the year 2000 are subscription and PBX hacking, where the loss in 2013, for instance, is $5.22 and $4.42 billion USD respectively.

Despite the fact that the Telecom industry loses billions of dollars every year due to several types of risks (socio-technical-economic risks), the control measures are not handling to stop risks from happening. The reasons are due to the following problems: 1) risks in the Telecom industry are not straight forward to identify how they could happen, 2) the existing risk assessment process in the Telecom industry couldn't cope up with those complex, dynamic and sophisticated attacks/fraud, and 3) researches on risk assessment techniques are limited in the telco domain to handle those risks. In this paper, we are interested in business related and socio-technical risks, but we use the general term risk to indicate also other types of risks - fraud risks, performance and security risks.

In order to address problems, the risk assessment process – specifically the risk identification (RI) stage - plays an important role. There are different types of RI approaches in the research community specific to the field of studies. In this paper, we perform a systematic review to find out the existing RI approach-

Yesuf, A.
A Review of Risk Identification Approaches in the Telecommunication Domain.
DOI: 10.5220/0006197603890396
In *Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP 2017)*, pages 389-396
ISBN: 978-989-758-209-7

Table 1: Yearly fraud loss (in billion USD) based on CFCA(CFCA, 2015).

Year	2003	2006	2009	2011	2013	2015
Loss	$35.0	$54.6	$72.8	$40.1	$46.3	$38.1

es/techniques available in the domain. This helps us to identify the research landscape and shape future research directions. Section 2 describes the scope and methodology used for the review; Section 3 discusses the findings including the research trends in the last 16 years. Finally, Section 4 highlights open issues and future research directions of risks identification in the domain.

2 SCOPE AND METHODOLOGY

Scope. To shape the scope of the review process, we use Coopers literature review taxonomy (von Brocke et al., 2009). The focus of the review is to investigate and analyse the research outcomes and applications of the RI approaches. This happens by exhaustively searching publications in the telco domain and related domains. The goals of the review are: 1) identifying and classifying the RI approaches with their applicability to the telco domain: the review mainly focuses on the RI methods, frameworks or approaches of the telco domain. But we also investigate the RI approaches from related domains, e.g. e-commerce, communication systems and network systems, in order to find out approaches that are applicable to the telco domain. 2) Finding out the research trends in the domain: in order to understand the trends of the literature, we exhaustively search the selective keywords in each database for publications from 2000 to 2016. This is because since 2000 risks in the domain get sophisticated and costs the Telecom operators billions of dollars (CFCA, 2015).

The general audience of the review include experts, scholars or practitioners in the telco sector. Therefore, the selection of databases and keywords is based on the above taxonomy.

Methodology: Search Resources. In order to span several databases of literature in the selected domains, we use well-known publishers in several disciplines: IEEE, Springer, and ACM from the area of Computer Science; AiSeL from the areas of Information Systems; Elsevier from several disciplines spanning from Computer Science, Engineering, E-commerce, and Telecommunication. The combined search results from these databases provide the big picture of the domain. The keywords are carefully selected to span the problem domain. Besides, we include keywords related to e-commerce and communication systems in order to observe how the problem is addressed in the related field of studies. Even though the searching mechanism varies from one database to another, we kept the main scheme of our keywords in all of the selected databases. The main query keywords are shown below.

```
{("risk identification" or "risk
  analysis" or "risk analyses" or
  "risk  assessment" or "risk
  management")
and (method or approach or framework)
and (e?commerce or
  electronic?commerce or
  "communication system" or
  telecommunication)
not (agriculture or oil or volcanic)}
```

3 FINDINGS

By searching the keywords in the databases above, 44 *representative* papers are filtered after fifth iterations. The summary of iterations is listed in Table 2.

3.1 Classes of RI Approaches

RI is the process of finding out several types of risks in an enterprise before, and after the system is developed or the service is released to the customers. The RI approaches of the telco domain are limited in number from the literature identified above but the fact that we extended the search to the related domains (e.g. e-commerce, communication networks and systems) provide several other types of approaches which can be extended and applicable to the telco domain. From this, nine different RI classes of approaches are identified which allow us to classify the 44 papers observed above. As the classes are produced considering the perspective and emphasis of each paper (the input for RI, the model leveraged, the security standard they use), it can be extended to be used to observe papers in similar domains. The following classes are produced. The classification of RI approaches with respect to the selected literature is shown in Table 3.

Model-based security engineering (MBSE): is a strategy of assessing risks against the security requirements/policies based on different types of system models (e.g. system architecture, use-cases, sequence, deployment diagrams). These models provide the possibility to understand the context of the risky environment, which in the end need to be analysed. Some of the *MBSE* approaches identified in the literature include CORAS(Aagedal et al., 2002; Gran

Table 2: Number of publications in each database.

Databases	IEEE	ACM	Springer	Elsevier	AiSeL	Total
1st iteration (first search)	657	749	694	582	284	2966
2nd iteration (filtered by the titles)	128	40	61	40	22	291
3rd iteration (filter by the abstracts)	55	20	8	11	11	105
4th iteration (filter by the contents)	42					42
5th iteration (with backward search)	44					44
Total number of publications observed						44

et al., 2007), UMLsec(Jurjens et al., 2008; Vinnakota, 2011), and goal-oriented analysis modelling.

Threat modelling: provide the capability of analysing a system based on standardised threat models. Through understanding the context of target of analysis, threats can be identified structurally using threat models. STRIDE[1](Zalewski et al., 2013; Prasad, 2007), for instance, is a threat model from Microsoft, which allows categorising threats of a target of assessment. This threat categorisation provides an indication to the available weaknesses of the system and helps decision makers design countermeasures.

Structural analysis: is the conventional way of structural analysis through identifying assets, vulnerabilities, threats and the probability of an attack against identified assets.

Business process-based RI: is an approach that business process models are used to identify risks in an enterprise.

Data mining: analysing large amount of data (e.g. usage characteristics of mobile call subscribers) to identify the associated risks. Data mining is mainly used to identify fraud related risks perpetrated in the telecommunicaiton services.

Game theory: is a situation where the risk assessment process is considered as a game, involving two players: an attacker and a defender. The RI process involves understanding the behaviour of the attacker, i.e., the cost of the attack and the benefit from it. The decision of the defender to defend the attack is, therefore, based on the attacker behaviour.

Methods and standards: Using different standards, some of the papers propose a risk management approaches mainly to deal with security risks. ISO 27001 (Information Security Management), ISO27011 (Information security management guidelines for telecommunications organizations based on ISO/IEC 27002) and ISO 31000 (Risk Management principles and guidelines)(ISO, 2009). Some other risk management methods, for instance, CRAMM and HazOp are used to identify security risks in telco.

Survey and Brainstorming: helps to understand the context of the environment to be analysed through preparing question-answer sessions, focus groups, and continuous discussions. This is a classical approach that happens mostly when there is no sufficient data to perform the risk assessment process.

Probabilistic analysis: analyses probabilities of, for example, failure of a system to provide reliable service to customers. Based on identified probabilities, preventive measures take place.

Discussion: The Result. Model-based risk assessment approach is proposed for telco domain in (Jurjens et al., 2008) and (Vinnakota, 2011). UMLsec - one of model-based approaches and the extension of UML modelling - is used to identify and analyse risks in mobile communication systems (Jurjens et al., 2008). It provides the possibility of integrating security requirements (basically security policies) of a Telecom enterprise into the development of a secured system. In (Vinnakota, 2011), Cybernetics Risk Influence Diagraming (CRID) is used to identify interconnected, interrelated and emerging risks in a software project, which is applicable to the Telecom domain. CRID begins its process by identifying risk influencers - events or conditions - that lead for a risk to happen. With the involvement of project manager and team members of a project, the influence of each risk influencers will be identified. This process iterates at each stage of the project life cycle to identify and evaluate risks of the project. Some papers from the related domains have proposed security risk modelling and assessment approaches of their IT systems and services (Mounzer et al., 2010), (Dantu et al., 2004), (Aagedal et al., 2002), (Sadiq et al., 2010), (Zalewski et al., 2013), (Nostro et al., 2014), (Cholez and Feltus, 2014), by which some of them are applicable in the telco domain. To mention some of the others, the RI process in (Mounzer et al., 2010) is a structural way of identifying threats and the corresponding attacks against the crucial assets of a system, even though the main focus is given to the assessment and mitigation stages of the risk management process. Based up

[1] STRIDE: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege (msdn.microsoft.com).

Table 3: Classification of RI approaches.

Classes of RI approaches	Known approaches from the selected literature	Literature
Model-based security engineering	UMLsec, Archimate, ISRM, Mission tree, goal-oriented, use case diagram, multi-layer tree, CRID, graphs, attack graph, CRID technique, CORAS	(Jurjens et al., 2008) (Vinnakota, 2011) (Mounzer et al., 2010) (Dantu et al., 2004) (Aagedal et al., 2002) (Sadiq et al., 2010) (Zalewski et al., 2013) (Nostro et al., 2014) (Cholez and Feltus, 2014) (Gran et al., 2007) (Ariss, 2011) (Clark et al., 2008) (Prasad, 2007) (Wu and Wang, 2011)
Threat modelling	STRIDE, DREAD, fault tree	(Prasad, 2007) (Zalewski et al., 2013)
Structural analysis	Identification of assets, internal/external risk factors	(Prasad, 2007) (La Corte and Scatà, 2010) (Rossebø et al., 2007) (Yu and Wu, 2010) (Iannicca et al., 2013) (Rippon, 2006) (Tsai and Huang, 2011)
Business process based RI	Mapping business process with the probabilities of failure, impact analysis	(Ernawati et al., 2012) (Mayer and Aubert, 2014) (O'Donnell, 2005) (Rohde et al., 2016)
Data mining	Fraud detection algorithms	(Harmantzis and Malek, 2004) (Bihina Bella et al., 2009) (Brucker et al., 2010) (Subudhi and Panigrahi, 2015) (Tseng et al., 2015) (Subudhi and Panigrahi, 2015) (Tseng et al., 2015)
Game Theory	Attacker-defender model	(He et al., 2008)
Methods and standards	based on CRAMM, HazOp, NIST, ISO 27001, ISO 31000, ISO 27011	(Mounzer et al., 2010) (Aagedal et al., 2002) (Ernawati et al., 2012) (Mayer and Aubert, 2014) (Stoneburner et al., 2002) (Vahl et al., 2009) (Seify and Bijani, 2009) (Bojanc and Jerman-Blažič, 2008)
Survey and Brainstorming	Questions-Answers, discussions, SWOT analysis, SJT, existing literatures	(Mounzer et al., 2010) (Sadiq et al., 2010) (Rippon, 2006) (Martinez-moyano et al., 2006) (Esteves et al., 2004) (Herzfeldt et al., 2012) (Macwan, 2004) (Sutton et al., 2008) (Rohde et al., 2016)
Probabilistic analysis	Bayesian networks; Failure of system, router	(Dantu et al., 2004) (Vidalenc and Ciavaglia, 2010) (Sherif et al., 2003) (Wickboldt et al., 2011) (Cortellessa et al., 2005)

on the preliminary RI process, the risk modelling and control/mitigation is performed through graph-based approach and mathematical optimisation respectively. In order to estimate risks of a critical resources in an enterprise, (Dantu et al., 2004) argues that identifying the behaviour of attackers play an important role. A behaviour-based attack graph is used to show their argumentation. Another model-based enterprise risk assessment approach called CORAS (Aagedal et al., 2002; Gran et al., 2007) uses modelling of unwanted incidents, vulnerabilities and threat scenarios of a system to identify risks against the target of assessment.

Threat modelling is also used as an approach to identify risks. It is the process of identifying threats structurally using standard threat models, e.g. STRIDE, DREAD (Prasad, 2007) or fault trees (Prasad, 2007); in this regard, besides integrating other model-based risk assessment models, (Zalewski et al., 2013) and (Prasad, 2007) leveraged Microsoft STRIDE threat model and fault trees to analysis the security of cyber-physical systems and enterprise risks respectively. Even though some of the literature above follows structural analysis together with the model-based approach, there exist literature which only used the structural analysis - identify assets, vulnerabilities, threats to find out security risks (La Corte and Scatà, 2010) (Rossebø et al., 2007) (Yu and Wu, 2010) (Iannicca et al., 2013) (Rippon, 2006) (Tsai and Huang, 2011). The approaches from (La Corte and Scatà, 2010), (Rossebø et al., 2007), (Yu and Wu, 2010), and (Rippon, 2006) are applied in the telco domain.

Some of the RI approaches use business processes to identify risks in an enterprise (Ernawati et al., 2012), (Mayer and Aubert, 2014) and (O'Donnell, 2005), where the first two papers applied the approach for the telco domain. Some others, (Harmantzis and Malek, 2004) (Bihina Bella et al., 2009) and (Brucker et al., 2010) describe and use approaches of data mining for identifying fraud risk in the telco domain.

Under the class of Standards and Methods, security standards and other known methods (e.g. HaZop) are used in the risk assessment and management process including RI (Mounzer et al., 2010) (Aagedal et al., 2002) (Ernawati et al., 2012) (Mayer and Aubert, 2014) (Stoneburner et al., 2002) (Vahl et al., 2009) (Seify and Bijani, 2009) (Bojanc and Jerman-Blažič, 2008).

Discussions, SWOT analysis, existing literature and survey are also considered as a way to identify different types of risks in (Mounzer et al., 2010) (Sadiq et al., 2010) (Rippon, 2006) (Martinez-

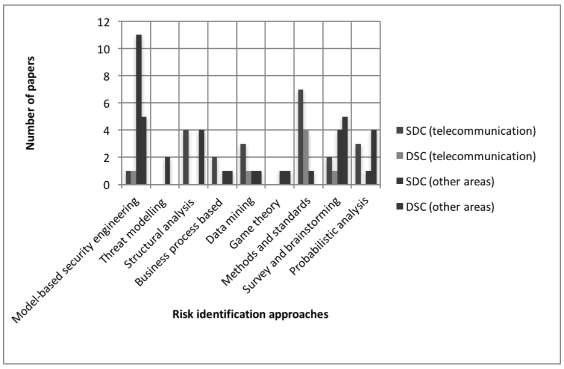

Figure 1: The distribution of papers to the RI approaches for different types of domains. SDC (Single Domain Case), DDC (Double Domain Case).

moyano et al., 2006) (Esteves et al., 2004) (Herzfeldt et al., 2012) (Macwan, 2004) (Sutton et al., 2008).

Research Focus of the Selected Papers. We show the results using the RFC 2904 requirements (Vollbrecht et al., 2000) that helps to categorise the focus of the selected papers based on the authorisation level - single domain case (SDC) and distributed domain case (DDC). In a single domain case (SDC) there exists only one administration domain that put decisions on different aspects; everything else is grouped into a distributed domain case (DDC). Considering the context of the telco as a system or a service released to customers, we further have three subcategories of applicability: *before, at real-time* and *after* a system is developed or a service is released to customers. The distribution of the selected papers in the telco and other related domains is shown in Figure 1. Open research gaps in SDC domain include threat modelling approaches, game theory and data mining. In addition to these, structural analysis, business process based RI, and probabilistic analysis are the research gaps in the domain of DDC. This helps to understand the research landscape of the telco domain and other domains (specifically e-commerce and communication systems).

In general, we draw the following key points: 1) Risks in the telco domain are continuous and happen in variety of forms, but the RI approaches only apply to specific domains. 2) The review based on public researches on this area only reveals the partial image of the problem. The challenges include lack of enough publication resources, difficulty of getting real telco data to do researches and willingness of the Telecom operators for external researchers.

3.2 The Research Trend

In the first five years, mobile applications, the development of application software for smart phones and the next generation networks (NGN) were the topic of discussion. The risk management and assessment approaches were, therefore, targeting such trend to identify risks, analyse the impacts and provide countermeasures of different types of risks (including human factors).

From the beginning of 2006, IP-based telco services, as the main part of NGN, were widely adopted to provide the complementary functionalities to the classic audio, messaging and data services. Since then the research trend were extended to risk assessment of the NGN networks and associated elements that go together with it, including risks of network infrastructures, mobile applications development, fraud risks and leakage of customers information. Several risk assessment and management approaches were proposed. More than 30% of the selected telco papers lied between 2006 and 2010.

In continuation to the above trend, due to the introduction of NGN, the Telecom enterprise have enforced to work together with other enterprises including banks. This relationship also produced new business and security risks. The regulatory bodies modify the existing regulations on the telco services based on the new types of services. So flexible ways of risk management and assessment approaches were the main focus of discussions. Table 4 summarises the main focus of the selected papers and the types of telco risks with in different years of time.

4 CONCLUSION AND FUTURE RESEARCH DIRECTIONS

The RI approaches identified above cover some of the telco risks in the domain. We believe telco risks can be minimised through investigation of specific problems and researching suitable approaches, which can prevent risks before occurring or before the damage escalates beyond a threshold. From this perspective the following are future research directions on identification of telco risks.

Usage of *model-based security engineering (MBSE)* for several types of risks: *MBSE* is applicable to many of risk assessment problems in the telco domain. From the review, (Jurjens et al., 2008) shows how the security policies of a company can be enforced and verified on telco network architectures and communications. This is the effort of involving *MBSE*

Table 4: The research trends between 2000 and 2016, based on the selected papers.

Years	Types of risks	Main focus	Literature
2000 - 2005	Security risks, enterprise risks (business process performance risks) and Human vulnerabilities	Vulnerability identification of network-based systems, Model-based risk assessment, Event (negative) identification of an enterprise, Risk management approaches, Performance risk assessment	(Aagedal et al., 2002) (Cortellessa et al., 2005) (Dantu et al., 2004) (O'Donnell, 2005) (Sherif et al., 2003) (Stoneburner et al., 2002) (Harmantzis and Malek, 2004) (Esteves et al., 2004) (Macwan, 2004)
2006 - 2010	Security risks (of mobile applications, software, network infrastructure, mobile network), Risks of NGN (next generation networks), IP-based voice systems, Fraud risks (of NGN), Data leakage (of customer information)	Risk management approaches (using model-based security risk assessment, considering business objectives), Model-based software risk analysis and evaluation, Game theory as security risk assessment paradigm, Determination of investment in information security, Fraud management systems	(Clark et al., 2008) (Vahl et al., 2009) (Vidalenc and Ciavaglia, 2010) (Yu and Wu, 2010) (Prasad, 2007) (Rippon, 2006) (Buhr et al., 2007) (Iannicca et al., 2013) (Sadiq et al., 2010) (Seify and Bijani, 2009) (Rossebø et al., 2007) (La Corte and Scatà, 2010) (He et al., 2008) (Gran et al., 2007) (Bihina Bella et al., 2009) (Bojanc and Jerman-Blažič, 2008) (Brucker et al., 2010) (Mounzer et al., 2010) (Jurjens et al., 2008)
2011 - 2016	Security risks, Performance risks, Risks because of telco regulations, Integrated risks (business, technology and social risks), Fraud risks	Risk Management (based on IT security standards, Systematic assessments of a project (e.g. telco software) risks, Model-based risk assessment, Vulnerability management, Fraud detection	(Zalewski et al., 2013) (Ariss, 2011) (Wu and Wang, 2011) (Vinnakota, 2011) (Wickboldt et al., 2011) (Tsai and Huang, 2011) (Nostro et al., 2014) (Mayer and Aubert, 2014) (Iannicca et al., 2013) (Cholez and Feltus, 2014) (Ernawati et al., 2012) (Herzfeldt et al., 2012) (Subudhi and Panigrahi, 2015) (Tseng et al., 2015) (Rohde et al., 2016)

in the development of mobile applications. An interesting development could go beyond enforcement of security requirements. For instance, *MBSE* can itself help in identifying other security, transaction, and privacy risks. The combination of *MBSE* models can also represent other risks as shown from some of the papers from related fields (e.g. (Dantu et al., 2004) shows how behaviour based attack graph can be used in assessing enterprise risks). In this regard, the EU project TREsPASS (Montoya, 2013; Pieters et al., 2014) strives to come up with a modelling approach which identifies, analyse and prioritize socio-technical risks covering the telco domain.

Unlike for other domains, *real-time RI approaches* of the telco domain identify risks after the damage has occurred. In a call service, for instance, a real-time RI approach detects only after some amount of call traffic has been inflated. Unfortunately, the damage has already been done even though the risk has been detected. Therefore, a RI and assessment approach that takes the call payment plan, telco services architecture and surrounding context into consideration is an interesting research direction which prevent risks before happening.

Risks in distributed domain case, for instance roaming, involve multiple operators where the authorisation level for each of operators is different. Risks emerge not only from the weaknesses of the home operators but also due to existing settings of other operators. A new requirement of a RI approach from this regard is that it should engage the existing settings of the surrounding environment. From our review, we identified data mining approaches and business process based approaches are open issues that could address such problems when they are designed to a specific set of problems involving *several authorization levels*. Other types of RI approaches including game theory, threat modelling and probabilistic analysis are also the potential approaches that can be applicable together with other types of approaches.

Data mining approaches are observed strong in RI and real-time risk detection. Through identifying patterns of the risky situation, this approach detects risks at real-time. The fact that risks are detected after the damage has been done limits the full functionality of this approach. Instead, preventive RI approaches (e.g. analysis of service contracts and policies) can help develop the maximum possible prevention and detection capabilities.

As new technologies get increased, the risk assessment approach should also adopt the changes to prevent emerging risks. Fraud risks could emerge due to the tariff plan of operators, social engineering attacks, flawed business processes and transaction failures. A RI approach, therefore, should consider internal and external *risk motivating factors* (e.g. the security level of employees and market competition respectively).

In general, due to the complication of risks in the telco domain, the risk assessment steps should also be designed taking such complication into consideration. In this regard, this paper provides an overview of classes of RI approaches, investigate the research trends and future research directions of risk assessment steps in the telco domain.

ACKNOWLEDGEMENTS

Part of the research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007- 2013) under grant agreement no. 318003 (TREsPASS). This publication reflects only the authors' views and the Union is not liable for any use that may be made of the information contained herein.

REFERENCES

Aagedal, J., Braber, F. D., Dimitrakos, T., Gran, B., Raptis, D., and Stolen, K. (2002). Model-based risk assessment to improve enterprise security. In *Proceedings. Sixth International Enterprise Distributed Object Computing*, pages 51–62. IEEE.

Ariss, O. E. (2011). Modeling Security Attacks with Statecharts. In *Security*, pages 123–132, New York, New York, USA. ACM Press.

Bihina Bella, M. A., Eloff, J. H. P., and Olivier, M. S. (2009). A fraud management system architecture for next-generation networks. *Forensic science international*, 185(1-3):51–8.

Bojanc, R. and Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management*, 28(5):413–422.

Brucker, A. D., Petritsch, H., and Weber, S. G. (2010). *Fraud Detection for Voice over IP Services on Next-Generation Networks*, volume 6033 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, Berlin, Heidelberg.

Buhr, R., Nel, A., and Dos Santos, M. (2007). Laying the foundation of a sector wide risk model for the telecommunications industry. In *IEEE International Engineering Management Conference*, pages 366–370. IEEE.

CFCA (2000-2015). Global telecom fraud report. Technical report, Communications Fraud Control Association.

Cholez, H. and Feltus, C. (2014). Towards an Innovative Systemic Approach of Risk Management. In *Proceedings of the 7th International Conference on Security of Information and Networks - SIN '14*, pages 61–64, New York, New York, USA. ACM Press.

Clark, K., Singleton, E., Tyree, S., and Hale, J. (2008). Strata-Gem. In *Proceedings of the 4th ACM workshop on Quality of protection - QoP '08*, page 51, New York, New York, USA. ACM Press.

Cortellessa, V., Goseva-Popstojanova, K., Appukkutty, K. A. K., a.R. Guedem, Hassan, a., Elnaggar, R., Abdelmoez, W., and Ammar, H. (2005). Model-based performance risk analysis. *IEEE Transactions on Software Engineering*, 31(1):3–20.

Dantu, R., Loper, K., and Kolan, P. (2004). Risk management using behavior based attack graphs. In *International Conference on Information Technology: Coding Computing*, volume 1, pages 445–449. IEEE.

Ernawati, T., Suhardi, and Nugroho, D. R. (2012). IT risk management framework based on ISO 31000:2009. In *System Engineering and Technology (ICSET), 2012 International Conference on*, pages 1–8. IEEE.

Esteves, J., Rodriguez, N., Pastor-Collado, J., and Roy, R. (2004). Extending The SEI Risk Management Approach With Organizational Factors: An Action-Research Project.

Gran, B. A., Fredriksen, R., and Thunem, A. P.-J. (2007). Addressing dependability by applying an approach for model-based risk assessment. *Reliability Engineering & System Safety*, 92(11):1492–1502.

Harmantzis, F. and Malek, M. (2004). Security risk analysis and evaluation. In *2004 IEEE International Conference on Communications*, volume 4, pages 1897–1901 Vol.4. IEEE.

He, W. H. W., Xia, C. X. C., Zhang, C. Z. C., Ji, Y. J. Y., and Ma, X. M. X. (2008). A Network Security Risk Assessment Framework Based on Game Theory. In *2008 Second International Conference on Future Generation Communication and Networking*, volume 2, pages 249–253. IEEE.

Herzfeldt, A., Hausen, M., Briggs, R. O., and Krcmar, H. (2012). Developing a Risk Management Process and Risk Taxonomy for Medium-Sized It Solution Providers.

Iannicca, D. C., Young, D. P., Thadhani, S. K., and Winter, G. a. (2013). Security risk assessment process for UAS in the NAS CNPC architecture. In *Integrated Communications, Navigation and Surveillance Conference, ICNS*, pages 1–9. IEEE.

ISO, I. (2009). ISO 31000:2009, risk managementprinciples and guidelines.

Jurjens, J., Schreck, J., and Bartmann, P. (2008). Model-based security analysis for mobile communications. In *2008 ACM/IEEE 30th International Conference on Software Engineering*, page 683, New York, New York, USA. ACM Press.

La Corte, A. and Scatà, M. (2010). A process approach to manage the security of the communication systems with risk analysis based on epidemiological model. In *Proceedings - 5th International Conference on Systems and Networks Communications, ICSNC 2010*, pages 166–171. IEEE.

Macwan, A. (2004). Approach for identification and analysis of human vulnerabilities in protecting telecommunications infrastructure. *Bell Labs Technical Journal*, 9(2):85–89.

Martinez-moyano, I. J., Conrad, S. H., Rich, E. H., and Andersen, D. F. (2006). MODELING THE EMERGENCE OF INSIDER THREAT VULNERABILITIES. *Engineering*, pages 562–568.

Mayer, N. and Aubert, J. (2014). Sector-Specific Tool for Information Security Risk Management in the Context of Telecommunications Regulation (Tool demo). In *Proceedings of the 7th International Conference on Security of Information and Networks - SIN '14*, pages 85–88, New York, New York, USA. ACM Press.

Montoya, L. (2013). The trespass project.

Mounzer, J., Alpcan, T., and Bambos, N. (2010). Integrated security risk management for IT-intensive organizations. In *2010 6th International Conference on Information Assurance and Security, IAS 2010*, pages 329–334. IEEE.

Nostro, N., Ceccarelli, A., Bondavalli, A., and Brancati, F. (2014). Insider Threat Assessment. *ACM SIGOPS Operating Systems Review*, 48(2):3–12.

O'Donnell, E. (2005). Enterprise risk management: A systems-thinking framework for the event identification phase. *International Journal of Accounting Information Systems*, 6(3):177–195.

Pieters, W., Hadžiosmanović, D., Lenin, A., Montoya Morales, A., and Willemson, J. (2014). Trespass: Plug-and-play attacker profiles for security risk analysis (poster).

Prasad, N. R. (2007). Threat model framework and methodology for Personal Networks (PNs). In *Proceedings of the 2007 2nd International Conference on Communication System Software and Middleware and Workshops, COMSWARE 2007*, pages 1–6. IEEE.

Rippon, W. (2006). Threat assessment of IP based voice systems. In *1st IEEE Workshop on VoIP Management and Security, 2006.*, pages 17–26. IEEE.

Rohde, M., Peko, G., and Sundaram, D. (2016). Mindful Routines in the Face of Fraud. *AMCIS 2016 Proceedings*.

Rossebø, J. E. Y., Cadzow, S., and Sijben, P. (2007). ETVRA, a threat, vulnerability and risk assessment method and tool for eEurope. In *Proceedings - Second International Conference on Availability, Reliability and Security, ARES 2007*, pages 925–933. IEEE.

Sadiq, M., Rahmani, M., Ahmad, M., and Jung, S. J. S. (2010). Software risk assessment and evaluation process (SRAEP) using model based approach. In *Networking and Information Technology (ICNIT), 2010 International Conference on*, pages 171–177. IEEE.

Seify, M. and Bijani, S. (2009). A Methodology for Mobile Network Security Risk Management. In *2009 Sixth International Conference on Information Technology: New Generations*, pages 1572–1573. IEEE.

Sherif, M., Hoeflin, D., and Recchia, M. (2003). Risk management for new service introduction in telecommunications networks. In *Proceedings of the Eighth IEEE Symposium on Computers and Communications. ISCC 2003*, pages 597–601. IEEE Comput. Soc.

Stoneburner, G., Goguen, A. Y., and Feringa, A. (2002). SP 800-30. Risk Management Guide for Information Technology Systems.

Subudhi, S. and Panigrahi, S. (2015). Quarter-Sphere Support Vector Machine for Fraud Detection in Mobile Telecommunication Networks. *Procedia Computer Science*, 48:353–359.

Sutton, S. G., Hampton, C., Khazanchi, D., and Anrold, V. (2008). Risk Analysis in Extended Enterprise Environments : Identification of Critical Risk Factors in B2B E- Commerce Relationships.

Tsai, H.-Y. and Huang, Y.-L. (2011). An Analytic Hierarchy Process-Based Risk Assessment Method for Wireless Networks. *IEEE Transactions on Reliability*, 60(4):801–816.

Tseng, V. S., Ying, J.-C., Huang, C.-W., Kao, Y., and Chen, K.-T. (2015). FrauDetector. In *Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining - KDD '15*, pages 2157–2166, New York, New York, USA. ACM Press.

Vahl, M., Boehmer, S., and Oestreich, T. (2009). Probability Based Risk Analysis for a VoIP System. In *2009 Fifth Advanced International Conference on Telecommunications*, pages 441–446. IEEE.

Vidalenc, B. and Ciavaglia, L. (2010). Proactive fault management based on risk-augmented routing. In *IEEE Globecom Workshops, GC'10*, pages 481–485. IEEE.

Vinnakota, T. (2011). Systemic assessment of risks for projects: A systems and Cybernetics approach. In *2011 IEEE International Conference on Quality and Reliability, ICQR 2011*, pages 376–380. IEEE.

Vollbrecht, J. R., Calhoun, P. R., Farrell, S., Gommans, L., Gross, G. M., Bruijn, B. D., Laat, C. T. D., Holdrege, M., and Spence, D. W. (2000). AAA Authorization Framework Status. pages 1–35.

von Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., Cleven, A., Brocke, J. V., and Reimer, K. (2009). Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process.

Wickboldt, J. A., Bianchin, L. A., Lunardi, R. C., Granville, L. Z., Gaspary, L. P., and Bartolini, C. (2011). A framework for risk assessment based on analysis of historical information of workflow execution in IT systems. *Computer Networks*, 55(13):2954–2975.

Wu, B. and Wang, A. (2011). A multi-layer tree model for enterprise vulnerability management. In *Proceedings of the 2011 conference on Information technology education - SIGITE '11*, page 257, New York, New York, USA. ACM Press.

Yu, Z. and Wu, Y. (2010). Risk assessment of customer information in telecommunication industry. In *Proceedings - 2010 International Conference of Information Science and Management Engineering, ISME 2010*, volume 2, pages 341–344. IEEE.

Zalewski, J., Drager, S., McKeever, W., and Kornecki, A. J. (2013). Threat modeling for security assessment in cyberphysical systems. In *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop on - CSIIRW '13*, page 1, New York, New York, USA. ACM Press.