UNIVERSIDADE DE LISBOA

INSTITUTO SUPERIOR DE ECONOMIA E GESTÃO

Value focused assessment of cyber risks to gain benefits from security investments

Sérgio Rodrigues Nunes

Orientadores: Prof. Doutor Gurpreet Singh Dhillon

Prof. Doutor Mário Fernando Maciel Caldeira

Tese especialmente elaborada para obtenção do grau de Doutor em Gestão

2018

UNIVERSIDADE DE LISBOA

INSTITUTO SUPERIOR DE ECONOMIA E GESTÃO

Value focused assessment of cyber risks to gain benefits from security investments

Sérgio Rodrigues Nunes

Orientadores: Prof. Doutor Gurpreet Singh Dhillon

Prof. Doutor Mário Fernando Maciel Caldeira

Tese especialmente elaborada para obtenção do grau de Doutor em Gestão

Júri:

Presidente: Doutor Nuno João de Oliveira Valério, Professor Catedrático e membro do Conselho Científico do Instituto Superior de Economia e Gestão da Universidade de Lisboa

Vogais:

Doutor Mário Fernando Maciel Caldeira, Professor Catedrático do Instituto Superior de Economia e Gestão da Universidade de Lisboa

Doutor Mário José Batista Romão, Professor Associado do Instituto Superior de Economia e Gestão da Universidade de Lisboa

Doutor José Filipe Sá Rodrigues Soares, Professor Auxiliar da Escola de Engenharia da Universidade do Minho

Doutor Carlos José Corredoura Serrão, Professor Auxiliar do Departamento de Ciências e Tecnologias da Informação do ISCTE-Instituto Universitário de Lisboa

2018

Resumo

Com a multiplicação de dispositivos tecnológicos e com as suas complexas interacções, os ciber riscos não param de crescer. As entidades supervisoras estabelecem novos requisitos para forçar organizações a gerir os ciber riscos. Mesmo com estas crescentes ameaças e requisitos, decisões para a mitigação de ciber riscos continuam a não ser bem aceites pelas partes interessadas e os benefícios dos investimentos em segurança permanecem imperceptíveis para a gestão de topo. Esta investigação analisa o ciclo de vida da gestão de ciber risco identificando objectivos de mitigação de ciber risco, capturados de especialistas da área, prioritizando esses objectivos para criar um modelo de decisão para auxiliar gestores de risco tendo em conta vários cenários reais, desenvolvendo um conjunto de princípios de gestão de risco que possibilitam o estabelecimento de uma base para a estratégia de ciber risco aplicável e adaptável às organizações e finalmente a avaliação dos benefícios dos investimentos em segurança para mitigação dos ciber riscos seguindo uma abordagem de melhoria contínua. Duas frameworks teóricas são integradas para endereçar o ciclo de vida completo da gestão de ciber risco: o pensamento focado em valor guia o processo de decisão e a gestão de benefícios assegura que os benefícios para o negócio são realizados durante a implementação do projecto, depois de tomada a decisão para investir numa solução de segurança para mitigação do ciber risco.

Palavras-chave: ciber risco, gestão de risco, investimentos em segurança, VFT, gestão de benefícios

Abstract

With the multiplication of technological devices and their multiple complex interactions, the cyber risks keep increasing. Supervision entities establish new compliance requirements to force organizations to manage cyber risks. Despite these growing threats and requirements, decisions in cyber risk minimization continue not to be accepted by stakeholders and the business benefits of security investments remain unnoticed to top management. This research analyzes the cyber risk management lifecycle by identifying cyber risk mitigation objectives captured from subject matter experts, prioritizing those objectives in a cyber risk management decision model to help risk managers in the decision process by taking into account multiple real scenarios, developing the baseline of cyber risk management principles to form a cyber risk strategy applicable and adaptable to current organizations and finally evaluating the business benefits of security investments to mitigate cyber risks in a continuous improvement approach. Two theoretical frameworks are combined to address the full cyber risk management lifecycle: value focused thinking guides the decision process and benefits management ensures that business benefits are realized during project implementation, after the decision is taken to invest in a security solution to mitigate cyber risk.

Keywords: cyber risk, risk management, security investments, value focused thinking, benefits management

Acknowledgments

I wish to thank both my advisors Professor Gurpreet Dhillon and Professor Mário Caldeira for their support and advice, that allowed me to complete this work and to gain knowledge to grow as a better person. I also wish to thank all participants that contributed to this work.

Lisboa, May 2017

Dedicated to all my friends and family.

Contents

List of Figures

List of Tables

Nomenclature

AHP	Analytic Hierarchy Process
ALE	Annual Loss Expectancy
APT	Advanced Persistent Threats
CIA	Confidentiality, Integrity, Availability
ERM	Enterprise Risk Management
ICT	Information Communication Technologies
IRR	Internal rate of retun
IS	Information System
IT	Information Technology
KPI	Key Performance Indicator
MIS	Management Information Systems
NDA	Non disclosure agreements
NFC	Near Field Communication
NPV	Net present value
RBV	Resource Based View
RFID	Radio Frequency Identification
ROSI	Return of Security Investment
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SOX	Sarbanes Oxley

VFT Value Focused Thinking

WITI Why Is iT Important

Chapter 1

Introduction

"You have to believe in yourself."

—Sun Tzu, the Art of War

Nowadays most enterprises have requirements to protect the information security from outsiders, competitors and even between employees from different departments. It has been proven that disgruntled employees are seen as a massive threat to information security as they have access to sensitive information that can put the company's reputation at stake, although they are frequently perceived by management as trusted personnel that follow safeguards (Dhillon, 2001). The enforcing of regulatory requirements like Basel II or SOX by supervision entities force enterprises to conduct risk assessments and perform strict management of information security (Damianides, 2005; Locher, 2005). Information security due care should be established not only in large enterprises, but also in small and medium enterprises, taking into account the information criticality for business (Dimopoulos et al., 2004). This urge of information security relies on the accomplishment of three basic pillars: confidentiality, integrity and availability of information. Other information security principles that are always useful to be present in the information security manager's mind when evaluating security situations are Saltzer and Schroeder (1975) protection of information principles and RITE principles (Backhouse and Dhillon, 1999; Dhillon and Backhouse, 2000).

The data classification process helps to focus security investments according to information criticality, but the classification of information should be driven by business and most of those ongoing projects are performed without business support and the information security manager is left alone

as information custodian without any clear defined business requirements. Even with these multiple security principles and the assurance of the requirements, how does an information security manager transmit the added value of information security to top management? The model of fear, uncertainty and doubt can not be forever used to justify security investments (Salmela, 2008). The attacker also weights the retribution factors of being caught as well as cost to break in while balancing incentives such as value of information and deterrent factors such as a visible strict company security posture. The security strength of controls is not always directly measured because it is a function of the attacker's cost (Schechter, 2004).

Top management recognizes the need of information security, but how much of information security investment is enough? (Stewart, 2004) The information security budget is seen by top management as a black hole that sucks resources and investment without any returns. What are the return benefits of security investments? Although the information security manager is fighting daily to align business objectives with security objectives, it is not always possible to achieve a direct alignment between them. A key factor in influencing top management to expand the information security budget is cyber risk.

Risk is the common language between information security and the business, by translating the technical details into business losses and bringing top management long term commitment to the security strategy (Baskerville, 1991; Vitale, 1986). Security investments, most of the times, do not bring tangible added value to business, but they mitigate risk to an acceptable level by management by following a cost-benefit approach. The security budget lives from those detected risks, based on the importance of the critical business assets that it protects. Critical information resides on the assets that are part of complex technological environment and are targeted by multiple threats with a probability of being exploited that consequently results in multiple risks. Top management is flooded with these multiple risks and is urged by stakeholders to decide on the best alternative as soon as possible. Should the decision be focused in an alternative based approach?

Keeney (1992) argues that alternative focused thinking limits the decision criteria by focusing only on the alternatives rather that concentrating on company's objectives that are driven by values. Alternatives are pushed by others to force a decision among measures that are not aligned with business objectives and can result on the least damaging alternative being chosen by top management without appropriate reflection on business values (Ramanujam et al., 1986). Values should drive decision making as they influence intrinsically everything we do. Deciding on alternatives without understanding the values behind them and without matching the alternatives towards company's

values will constrain the decision process. The right approach is value focused thinking where values articulate different alternatives that achieve them, thus identifying better decision situations and changing a reactive decision process into a proactive process (Keeney, 1996).

Deciding on risk to drive the benefits from security investments entails the same phenomenon, decisions must be made as soon as possible and there might always be a better alternative that was not thought beforehand, as risks can always be further reduced. Decisions on risk can be critical because they might influence the business continuity in case of a major disaster or limit a sensitive information leak that causes stocks to fall abruptly (Goel and Shawky, 2009; Khansa and Liginlal, 2009). Nowadays we read news that enterprises go bankrupt or lose high amounts of money because of these damaging events and that's why this research is vital to achieve an adequate understanding of this problem as more and more information is managed within the corporate environment without appropriate due care by top management regarding cyber risks (Zetter, 2011).

How do we evaluate the benefits of a security investment? Investments should not be guided by poor decision management that uses creative accounting by assigning arbitrary values to benefits and costs and see benefits management as an act of faith (Irani and Love, 2013). This poor decision management hinders critical security investments that can be beneficial in the long term of the organization. The measures used to evaluate benefits from information technology (IT) are usually vague in nature and only linked to business performance, although IT nowadays plays a vital part in multiple business areas with qualitative benefits such as product quality improvement and competitive advantage for example (Jurison, 1996). Benefits from IT investments were initially directly linked to cost reduction, but as the IT implementation in enterprises becomes mature, the benefits from IT investments move from tangible financial gains to business value creation (Bradley, 2010). The time lag between the investment decision and the benefits recognition also plays a hindering force to develop a benefits management approach that continuously monitors the realization of benefits during project implementation and also after project closing. For example if we look at a project that changes a company's network, the benefits realization is difficult to measure to a simple metric due to the shared nature of infrastructure. In this case benefits are not perceived after project closure, but in future implementations of information systems on top of that infrastructure that are able to deliver increased capacity.

Ward and Daniel (2006) developed a benefits management approach that provides guidance on defining benefits a priori while evaluating the feasibility of the investment and later revisiting those benefits to see if they were really realized. They define a benefit as "an advantage on behalf

of a particular stakeholder or group of stakeholders" (p. 70). Although this approach is drawn on a model for strategic change and is linked in that research directly to IT investments, security investments are being more and more linked to IT and share the same problem of being regarded as a cost center that brings no added value to the business in the accomplishment of its strategic goals and its costs are difficult to justify, so this approach can be used out of the box to maximize the realization of security investment benefits that were drawn by a risk management strategy. Some of the implications of poor benefits management are: lack of alignment with the business strategy, inability to set priorities, inappropriate investment decisions, poor benefits identification and planning and lack of proven benefits realized from the investments performed. As it can be seen security investments suffer exactly from the same problems, which lead to poor decision making and underinvestment in projects with no clear and quick tangible benefits. Security spending is increasing and benefits are not being realized with data breaches continuing to occur (Dhillon, 2004).

Most of the investments are pushed by consultants that show low direct costs and miracle benefits that will revolutionize the current market, but hidden or unnoticed remain the indirect costs that tend to rise and the miracle benefits, that enable the investment in the first place, are vague in the end (Alshawi et al., 2003). Security investments are even more difficult to evaluate, as their goal is not to enable competitive new products or improve service quality, but a mitigation of a risk formed as the product of a threat and a vulnerability that might never be triggered. Due to these intangible benefits of security investments, a benefits management approach throughout the whole project is a vital step in enabling value for business from security investments.

Making the decision using value focused thinking based on risk management is a contribution towards the right path but is only a partial step, because only after a post implementation review of the benefits is the risk mitigation effective. This periodical benefits review approach assures that the benefits that triggered the investment decision are continually followed and project management adjustments are made to maximize benefits realization, not focusing only on the return of investment approach that reduces spending without benefits maximization. The necessary organizational changes to maximize security investment benefits must be continually monitored, because most of the investments in security involves not only technology, but require a change in the organizational processes and a shift in the employee's behaviour (Peppard et al., 2000). A mature benefits management approach leads to clearer planning of the activities and changes necessary to provide the necessary security capabilities, reduce the communication gap between information

technology, business management and the security risk department, and promote wiser decisions based on value focused thinking aligned with benefits continual monitorization to maximize benefits realization. Moreover, this research contributes for the methodology for evaluating management decision behavior by using a value focused thinking approach and controls quality changes after the decision is taken by using a benefits management approach (Fenz and Ekelhart, 2010).

1.1 Concepts and definitions

This section defines the main concepts of this research to leverage a common understanding of the phenomenon under analysis.

1.1.1 Information system

The UK Academy of Information Systems (UKAIS) defines information systems as ”the means by which people and organizations, utilizing technology, gather, process, store, use and disseminate information” (Ward and Peppard, 2002). Another definition of information system by Laudon and Laudon (1995) is: ”interrelated components working together to collect, process, store, and disseminate information to support decision making, coordination, control, analysis, and visualization in an organization“ (p.15). Information systems are composed by people, technology and processes, normally used in an organizational context. Information systems should not be viewed only with a technological lens, as processes and people play a vital part in their success. As Lee (2004) explains: ”an information system is not the information technology alone, but the system that emerges from the mutually transformational interactions between the information technology and the organization” (p.11). Moreover, Hirschheim et al. (1995) explains that information systems have two perspectives: functional and structural. The structural perspective of information systems is formed by people, data, processes, models and technology to serve an organizational purpose. The functional perspective deals with recording, storing and disseminating information. This ability to work and communicate information within the organization is a vital part of an information system and is not dependent on technology (Liebenau and Backhouse, 1990). People should be trained to maximize the information systems usage and they should be developed with adequate usability in mind (Davis, 1989). Current business processes will be adapted to mirror the new reality of change management with the adoption of the new system. Some legacy processes will end, new

processes will be discovered and others will be adapted to maximize benefits for business (Ward and Daniel, 2006).

1.1.2 Information security

Merrian-webster dictionary defines information as: ”knowledge that you get about someone or something, facts or details about a subject” and security as: ”the state of being protected or safe from harm”. Information is considered a main driver to achieve competitive advantage in the e-business age (Porter and Millar, 1985) and this mindset is borrowed from the resource based view (RBV) in which information and the knowledge obtained from that valuable resource foment the intangible capabilities that allow an organization to achieve competitive advantage over its competitors (Bharadwaj, 2000; Caldeira and Ward, 2003; Wade and Hulland, 2004). Critical business information should be protected from harm and that's the purpose of information security with its 3 base pillars: protect the confidentiality, integrity and availability of information. The confidentiality of information deals with information not being disclosed to unauthorized people and is normally accomplished by the use of encryption. Integrity of information invalidates the tampering and destruction of data. Some security measures allow information to be changed or corrupted while traveling in electronic format, but they preserve the integrity by detecting it and requesting the information replay, until it arrives with its integrity intact. The availability of information requires that when such information is needed, it can be accessed in a timely manner. Inside information confidentiality pillar two other concepts must be explained: anonymity and privacy. Anonymity is the possibility of not being identified, when performing actions, preserving the identity's confidentiality and privacy entails the confidentiality of personal data. Inside the integrity pillar there's authentication, accountability, authorization and non-repudiation. Authentication is the integrity of the origin that proves the identity in some information system, accountability deals with the integrity of the responsibility that tracks user's actions, authorization deals with the permissions of an authenticated identity across objects and finally non-repudiation assures the integrity of communications. When designing security controls there are three main focus areas: technology, formal controls, namely policies and procedures and informal controls focused on changing people's behavior with awareness (Chowdhuri and Dhillon, 2012; Dhillon, 1995). Focusing the controls on a single area leaves the others as the low hanging fruit, waiting to be exploited by an attacker.

Saltzer and Schroeder (1975) present a set of principles for the protection of information in the secure design of information systems:

- Economy of mechanism: this principle deals with simplicity and a simple information system that is easy to be understandable and tested is more secure;
- Fail safe defaults: denying an access should be the default action and every permitted access should be detailed explicitly. When a system fails it should deny all access in order to be quickly detected;
- Complete mediation: every access should be checked by a central monitor for the adequate authorization in order to function as the main gate of access that has the complete vision;
- Open design: the security of a design should not be its obscurity, but be positioned by the strength of its public protection mechanisms;
- Separation of privilege: sometimes named dual men control, this mechanism ensures that it is not possible to perform a critical operation with only one credential. Two credentials are needed at the same time or an additional validation by another person is required to complete the task;
- Least privilege: the system should give users only the privileges necessary for the fulfilment of the user's tasks;
- Least common mechanism: shared mechanisms should be minimized, has they have the power to influence several users or modules;
- Psychological acceptability: it is important to balance usability with security otherwise there will be resistance from people to accept the security mechanism, it will be turned off or someone will find a way to bypass it.

Another set of principles in information security is RITE (Backhouse and Dhillon, 1999; Dhillon and Backhouse, 2000). This set of principles is focused on people rather than information systems:

- Responsibility: Each employee should clearly know his roles and responsibilities within the organizational structure, to prevent gray areas were responsibility is dissolved without clear accountability;
- Integrity: Integrity of a person within an organization plays a fundamental role, as most employees have access to sensitive information on a daily basis. Most data breaches arise from disgruntled internal employees and their organizations should prevent the leakage of information to competitors;

- Trust: As organizations move to a virtual environment with geographically disperse physical boundaries, the close control and supervision tends to become weaker. Nevertheless the trust from close face to face relations has to prevail within the organizational peers and the organization expects from each employee a trusted behavior despite the absence of control;
- Ethicality: Beyond the organizational rules lie the ethical principles of each person and culture. These ethical principles are critical when an employee faces an unexpected organizational situation that is not applicable to existing rules and has to behave according to his own principles.

1.1.3 Risk

Risk is defined in the Oxford dictionary as: ”a situation involving exposure to danger” or in the merrian-webster dictionary as: ”the possibility that something bad or unpleasant will happen”. Slovic et al. (2004) differentiates two types of risks: risks as feelings and risks as analysis. The first type “refers to our fast, instinctive and intuitive reactions to danger” and the other “brings logic, reason and scientific deliberation to bear on hazard management”. NIST (2010) defines risk as: ”a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of the adverse impacts that would arise if the circumstance or event occurs; and the likelihood of occurrence”. ISO (2009) defines risk generically as an ”effect of uncertainty on objectives”. Being the effect, in this definition, a positive or negative deviation from the expected. Dubois et al. (2010) strive to define the domain of information system security risk management and explain that ”risk is the combination of a threat with one or more vulnerabilities leading to a negative impact harming one of more of the assets. Threats and vulnerabilities are part of the risk and impact is the consequence of the risk.” The authors define vulnerability as: ”the characteristic of an IS asset or group of IS assets that can constitute a weakness or a flaw in terms of cyber security” and threat as: ”potential attack, carried out by an agent, that targets one or more IS assets and that may lead to harm to assets”. NIST (2010) defines risk management as ”coordinated activities to direct and control an organization with regard to risk”.

Renn (1998) synthesizes multiple approaches to risk management. He describes risk in economic theory as a method to limit losses but also as a window of opportunity. From a social perspective, risks are viewed as deviation of human actions that bring consequences to human values. There are also multiple risks that are always present in mother nature and provoke undesirable states of

reality as result from natural incidents. From a technical perspective, risk assessments calculate probabilities of unwanted consequences multiplying by the magnitude of their impact. The major focus is to reduce risks to an acceptable level that can be tolerated, controlled and monitored. When considering risks of information systems there are two major types of risks. The first deals with project management risk when developing or implementing information systems. The second one deals with security risks of information systems. What is the risk to information security that top management is willing to accept? Risk is, most of the times, not possible to be eliminated without affecting the continuity of the business. Information security risk should be mitigated with security measures until it reaches a point, when top management is willing to accept it. Could be, for example, that additional risk mitigation measures are more expensive than purchasing an insurance, so the transference of the risk to an external entity would be the best decision. The cost of a risk mitigation measure should not be higher than the risk it mitigates, but the uncertainty in risk assessment is always present as information technology (IT) is increasing in complexity everyday and business dependency from IT rises (Longstaff et al., 2000). People tend to underestimate common, natural, familiar and anonymous risks that can be controlled and are well understood, while exaggerating in personified, rare and intentional risks that are beyond their control and are surrounded by uncertainty (Schneier, 2008). Fischhoff et al. (1979) argue that the extend of a full risk analysis is surrounded with multiple uncertainties, because it is not possible to enumerate all possible events and their consequences in advance, even if that was possible it is also very difficult to estimate the accurate probability of occurrence. The acceptability of a risk can be influenced by multiple factors: the weighing of the benefits may smoother any residual risks, risks from voluntary activities are more likely to be accepted than risks from involuntary activities due to the false sense of control and the level of acceptability of a risk depends also from the number of targets that it affects.

Risk is the common language between information technology and business management, the information security manager should change its technical speech of bits and bytes to a common language understood by management. Risk serves that function in clarifying threats and vulnerabilities in a common sense, so that management is able to understand the problem at hand and take a decision to mitigate the risk and still enable the business changes necessary to achieve business goals. This achieves an alignment between business, information security and information technology objectives and as the organizational risk management strategy evolves, it will be present in every management process. With this continuous presence, risk management culture, as an op-

portunity for business, will spread across the multiple departments from outside of the information security context (Doherty and Fulford, 2006; Westerman, 2009). This common language serves as a technique for justifying a baseline of information security controls in a predictive manner, although some of its values are interpretative (Fitzgerald, 1995). The main power of risk management relies in acting as a facilitator of speech that involves multiple departments and creates awareness of harmful consequences (Baskerville, 1991).

When talking about a risk assessment strategy two approaches appear: qualitative or quantitative risk management. The qualitative risk management approach relies on labels of prioritization taking into account the probability of loss and criticality of information to quantify the risk into low, medium and high or another defined scale. The qualitative approach includes expert judgment with the discussion of common risk scenarios among subject matter experts. The quantitative approach follows a similar approach but takes into account the financial impact of losing information from a company asset, by measuring the loss in monetary values. According to Bandyopadhyay et al. (1999) risk analysis divides the IT environment in 3 levels. The application level deals with the risks of the failure of IT applications. The organizational level concerns the impact of IT across business areas and the inter organizational level entails risks across organizations that share IT networked assets. A generic risk assessment process is divided among 4 phases. The first phase evaluates current business assets and the severity of information they entail. The second phase details the threats that each asset is exposed to and determines its probability of exploit. After the risk analysis phase is completed, risks not accepted by management have to be mitigated with security measures. The last phase ensures the continuous improvement approach with the monitorization of the risks to alert business if some residual risks increase due to business or context changes.

1.1.4 Cyber

The word cyber is defined in the Oxford dictionary as: ”relating to or characteristic of the culture of computers, information technology, and virtual reality” or in the Merriam-webster dictionary as: ”of, relating to, or involving computers or computer networks (as the Internet)”. It has its origins in the term cybernetics. NIST glossary defines cybersecurity as (Kissel, 2013): ”The ability to protect or defend the use of cyberspace from cyber attacks.” In the same document, a cyber attack is defined as: ”an attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.” ISO (2012) 27032 defines

cybersecurity as: ”preservation of confidentiality, integrity and availability of information in the cyberspace”. Cyberspace is defined in that document as: ”the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form”.

Von Solms and Van Niekerk (2013) argue that cyber security is not the exactly the same as information security, because cybersecurity embraces the need to protect societal values that have migrated into cyberspace such as cyberbullying and cyberstalking for example, instead of focusing solely on the protection of information. World problems, like for example cyber terrorism or cyber warfare, are also part of the cybersecurity domain. The objective is to protect the legitimate actions from individuals, organizations or nations that function in the cyberspace from cyber attacks. Barzilay (2013) explains that cyber risks or risks of cybersecurity, extend the information security risks with the rise of new technical risks of low probability and high impact.

In this document we use the term cybersecurity and information security interchangeably with exactly the same meaning.

1.1.5 Value

Merrian-webster dictionary defines value as: ”usefulness or importance” and the Oxford dictionary uses the definition: ”the regard that something is held to deserve; the importance, worth, or usefulness of something”. Catton (1959) defines value as ”a conception of the desirable which is implied by a set of preferential responses to symbolic desiderata”. These values influence everything we do, even if these value weights are performed intrinsically. Keeney (1992) explains that ”values are what we care about” and that ”values should be the driving force for our decisionmaking” (p. 3). This research regards values in a value-focused-thinking approach (Keeney, 1992) to be able to decide and justify alternatives in security investments based on risk management values from stakeholders.

1.1.6 Benefit

Oxford dictionary defines benefit as: ”an advantage or profit gained from something” and Merrian-webster dictionary uses the definition: ”a good or helpful result or effect”. Just as a good result characterizes a benefit, a bad result characterizes a disbenefit. Irani and Love (2013) define disbenefit as: ”an impact, direct or indirect of ICT, which has an unwanted and negative effect on the

performance of an individual or organisation". Ward and Daniel (2012) define business benefits as: "an advantage on behalf of a particular stakeholder or group of stakeholders" (p. 70). They note that business benefits have owners according to the value obtained from the investment. This owner, which normally is a senior member of the organization, ensures that the necessary changes to realize the benefit are actually implemented according to the plan. Serra (2016) explains that "benefits realization is a process to make benefits happen and also to make people fully aware of them throughout the entire process of realization in order to ensure the creation of strategic and measurable value to the business". This research uses the term benefit in a benefits management approach (Ward and Daniel, 2006), that plans and monitors a security investment to assure the maximization of the business benefits with the implementation of that investment.

1.2 Problem statement

In current organizations security investments are normally driven by a risk management process that prioritizes security initiatives. Risks are identified by security managers that face the risk mitigation decision towards multiple security measures or safeguards. Most of the times the cyber risk management approach is reactive when problems are detected, although this approach should be planned based in the organization's values in a preventive attitude. The main objective of risk management is to mitigate risks to a level that is acceptable by top management. The decision to accept a designated risk should be based on the values from management and stakeholders. Even if the risk is not acceptable, then the decision on how to prioritize security investment alternatives to reduce the risk should also be based on values. The explicit approach of discussing, writing down these values and transforming them into strategic objectives has not been carefully researched in a risk decision situation.

Another factor to take into account is how do these decisions are able to enhance the benefits from security investments, as return on security investments are not easily quantifiable per se. Even if the right decision is executed towards an investment, the expected benefits are usually not controlled. Most of the times, the security investments fail to meet the desired objectives by not realizing the benefits that were the initial reason for choosing that investment. Without benefits management, security investments do not assure risk mitigation, as they should be aligned with business objectives. Security investments are driven by technological vendors pushing the latest trend or by consultant agents documenting multiple policies and procedures that do not represent

the company's values and are not adopted and understood by its employees (Kolkowska and Dhillon, 2013). Most of the times these technological or business changes are not achieved or are underexploited by organizations and do not generate the initial benefits that were the cause of the investment decision process.

This problematic raises the following research questions:

- What are the objectives based on values for cyber risk management decision making?
- How do those objectives influence a cyber risk management strategy?
- How can an organization maximize the benefits from security investments to mitigate cyber risks?

1.3 Objectives

This research has the following main objectives:

- Identify value based objectives for cyber risk management;
- Evaluate the contribution of cyber risk management objectives for a risk management strategy;
- Evaluate the benefits realization of security investments to mitigate cyber risks.

1.4 Structure

This section describes the thesis structure summarizing each chapter regarding its focused themes and contributions.

Chapter 2 presents the literature review, focusing in two main themes: information security risk management and security investments. The main goal of this chapter is to present the status quo of the academic research in both fields. The inclusion factors in the search criteria for the first theme was information security risk management or cyber risk management and the exclusion factors were project management risk management, physical security risk management, energy risk management, safety risk management, law risk management, ethics risk management, medical

risk management and financial risk management. For the second theme the search criteria was cybersecurity investments or security investments. The researcher reviewed both academic and professional articles, including articles in journals and proceedings of conferences.

Chapter 3 details the research methodology, taking into account the philosophical perspective adopted. It presents the two main theoretical frameworks that are used in this thesis: value focused thinking and benefits management. It reviews multiple studies that use those theories to demonstrate the applicability of the chosen theories to multiple diversified fields of research. It provides also the best practices of case study research. The chapter is finalized with the design of the research.

Chapter 4 details the gathering of values in the form of objectives for cyber risk management. It uses the value focused thinking approach to gather and prioritize objectives to accomplish the main goal of minimizing cyber risk. The data is collected in the form of interviews with specialists in the field. It relates means and fundamental objectives in a graphical network. All the objectives are discussed and related back to the literature.

Chapter 5 presents a decision model for cyber risk management using the objectives collected in chapter 4. Multiple workshops were conducted to evaluate the consequences of the objectives in real world scenarios. Within those workshops the multiple objectives were prioritized and weighted using the swing method. The results were discussed among participants. Measures were defined to evaluate the performance of the multiple objectives. The decision model simplifies the process of the decision maker when evaluating multiple security investments for risk mitigation. The decision based on accepted values allows the simple justification of the investment across the multiple stakeholders.

Chapter 6 details the cyber risk strategy captured within a case study from a public organization. Objectives for planning a cyber risk management strategy are weighted, taking into account their business importance and achievable level. Principles for cyber risk management are presented, taking into account the objectives and decision model detailed in the previous chapters. These principles serve as a basis for managers planning a cyber risk management strategy, being able to be adapted to the needs of an organization.

Chapter 7 presents the cyber risk benefits management approach from an analyzed organization. It details the benefits of a risk management practice that evaluates security investments to mitigate cyber risk. The investment objectives are the same objectives from the previous chapters and this approach allows the fitting of the two theories: value focused thinking focuses on the decision

making process and benefits management focuses on realizing the benefits, that were the basis for the decision process.

Chapter 8 concludes this thesis by synthesizing the main theoretical and practical contributions. It details current research limitations and future work that is not in the context of this document.

Chapter 2

Literature review

"If ignorant both of your enemy and yourself, you are certain to be in peril."

—Sun Tzu, the Art of War

This chapter summarizes what is being researched in the multiple areas of information security risk and security investments benefits, by enlightening the researchers methodology and conclusions. It enumerates the multiple advantages and limitations of each research approach along with its main practical and theoretical contributions. The literature review process situates the existing literature in a broader scope and context (Boote and Beile, 2005). It justifies the decisions of the researcher of what demarcates the boundaries of the study and allows the researcher to examine critically the status quo of the researched area. Webster and Watson (2002) argues that ”an effective review creates a firm foundation for advancing knowledge”. It defines the areas where research already exists and unexplored areas with knowledge gaps, while facilitating theory development. Levy and Ellis (2006) summarize the main literature review characteristics:

- Analyzes methodologically and synthesizes the quality of the literature;
- Provides firm foundation to the research;
- Provides firm foundation to the selection of research methodology;
- Demonstrates that the proposed research contributes something new to the overall body of knowledge or advances the existing knowledge base.

2.1 Information Security Risk Management

Regarding security risk research, there are multiple models, frameworks and methods to deal with information security risk in organizations along with different studies that summarize them (Eloff et al., 1993; Tiganoaia, 2012; Vorster and Labuschagne, 2005). These studies are mainly divided among three groups: statistical probabilistic or economic risk management, maturity or standards focused risk management and people focused behavioral risk management. Transversal to these three groups, the research can be focused on the risk of a specific technological solution, adapting risk management to the requirements of an industry or business sector or changing an accepted risk assessment model or methodology to address specific needs.

2.1.1 Statistical risk management

In this subsection we analyze the literature that is based on statistical, probabilistic economical theories. Butler (2002) introduces a cost-benefit analysis technique that helps managers in the evaluation process of security initiatives. The Security Attribute Evaluation Method (SAEM) requires that a risk assessment is performed previously to list the threats and their impact to the organization (Butler and Fischbeck, 2001). The risk assessment is conducted in four phases: the first phase consists of the enumeration of impact outcomes and next it is necessary to estimate the frequency of the outcome and its measuring scale. The third phase uses the swing weight method to determine the weights of the outcome attributes and the final step is the normalization of weights between 0 and 1 to provide the sum of 1. Then it uses value functions to compute the threat index for each attribute. SAEM picks up that risk assessment and performs a benefit assessment on how much does a technology safeguard contribute to risk mitigation. It uses the previously calculated thread index and evaluates how the threat index is affected with the implementation of the safeguard. The next step is to consider the coverage of the safeguard among best practice engineering principles and the evaluation of the solution's cost. A final sensitivity analysis is performed to see if the manager committed errors during the process based on his beliefs and if he took a pessimistic or optimistic point of view to assess the technological benefits.

In et al. (2005) researched a security risk analysis model that consists of 4 steps. The first step involves the identification and evaluation of assets, threats and vulnerabilities. It is followed by the risk analysis phase taking into account the vulnerabilities, threats and asset values. After the risks are exposed, the next phase is to list the countermeasures and evaluate them in terms of risk

mitigation. The final step consists on the evaluation of the residual risk that remains after applying the countermeasure and documents those results in a report. The CCTA Risk Analysis and Management Method (CRAMM) follows a similar approach with 3 steps (Yazar, 2002): identifying and valuing assets, identifying threats and vulnerabilities, calculating risks and identifying and prioritizing countermeasures. This method simplifies the prioritization of security countermeasures, provides a structured approach to risk management and assists contingency planning while allowing compliance with mandatory standards.

Sun et al. (2006) present a new model for security risk assessment based on Dempster-Shafer Theory of Belief Functions. The Dempster-Shafer Theory of Belief Functions helps to model the uncertainties in the assessment process and provides the notion of plausibility of a negative outcome. Another benefit from this model is the incorporation of impact measuring when countermeasures involve the mitigation of multiple risks, thus limiting various threats. It finalizes by discussing how to conduct a cost-benefit analysis under the evidential reasoning approach.

Sharma and Dhillon (2009) propose the use of chaos theory instead of the classical probability approach to risk management. They state that "the aim of utilizing chaos theory to understanding risks to computer based systems is not to predict the exact state but rather the overall behavior of the system" and it has been proven useful in information systems research when there is a high degree of uncertainty that limits classical approaches.

Alberts et al. (2003) present Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), a framework for managing security risks. It balances 3 aspects: risk, security practices and technology. The framework has 3 phases: build asset-based threat profiles, identify infrastructure vulnerabilities and develop security strategy and plans. The first phase deals with the organizational view and determines what is important to the business and what is being done to protect those assets. This involves asset categorization, prioritization along with threat evaluation to create an asset profile. The second phase focuses in a technical view to identify infrastructure vulnerabilities that affect the assets. The last phase consists in a strategical view, in which risks are identified and evaluated to be able to develop mitigation security plans. Each phase is composed by different processes with the total of 8 defined processes. The first phase has 4 processes: identify senior management knowledge, identify operational area knowledge, identify staff knowledge and create threat profiles. The first 3 processes are aimed at gathering the maximum asset information and their severity from key business areas and the last process selects the critical assets and establishes their threat profiles. Phase 2 has 2 processes, which consist in the identification of key components and their

evaluation, to refine the threat profiles defined previously. The last phase is also divided among 2 processes: conduct risk analysis and develop protection strategy. The OCTAVE criteria describes the principles and attributes that guide its implementation (Albert and Dorofee, 2001).

Alberts and Dorofee (2002) point out 4 main success factors to use the OCTAVE method efficiently: getting senior management sponsorship, selecting the analysis team with the desired interdisciplinary skills, setting the appropriate scope of evaluation and selecting participants based on their organizational knowledge and not solely their availability. OCTAVE is characterized by its implementation flexibility and different framework derivations exist, taking into account the target organization size and implementation effort required. The original framework is targeted at organizations with more than 300 employees and the variation known as OCTAVE-S is the best approach for small organizations. It is adequate to small organizations, because it simplifies the methodology with fewer processes that adapt to a flat hierarchical model. It acknowledges that the information technology service might be outsourced and it is possible to gather a small team that has broad understanding of the company under analysis (Alberts et al., 2005).

Caralli et al. (2007) developed OCTAVE-Alegro, a variation from OCTAVE that focuses more on the organizational information itself to assess risks. Its main advantages when comparing to the original OCTAVE are the simplification of the assessment process and reducing the commitment of affected resources. It is divided in 8 steps: establish risk measurement criteria, develop an information asset profile, identify information asset containers, identify areas of concern, identify threat scenarios, identify risks, analyze risks and select mitigation approach. The process begins by the definition of the risk measurement criteria by deciding how risks affect the organizational objectives and how they impact the business to establish a set of qualitative measures. The second step entails the creation of multiple information asset profiles with the description of its characteristics and business value. The third step details the information containers, that are ”the places where information assets are stored, transported, and processed”. The fourth step is performed with brainstorming sessions where the participants identify what are the critical threat areas. These sessions include the creation and discussion of threat scenarios that are part of step 6. Step 7 identifies the prevailing risks, step 7 quantifies those risks as accurate as possible and step 8 deals with risk mitigation tasks.

Shedden et al. (2011) argue that the methodologies for information security risk assessments do not take into account knowledge management risks and only focus on assets. They present an exploratory case study in a software company in which they use the OCTAVE-S methodology to

analyze the risks of the backup process. By strictly following the OCTAVE-S methodology they explain that the knowledge management risks of the 2 people involved in the process will not be discovered. They explain that explicit knowledge risk can be mitigated with documentation, but the tacit knowledge risk is difficult to address. They defend that within the people category of risks there should be also the knowledge risk. In this case they argue that having all the knowledge concentrated on 2 people should also be documented as a risk.

Wei et al. (2010) propose a hierarchy for e-government security risk assessment based on the OCTAVE framework. Based on that hierarchy they use fuzzy AHP and artificial neural networks to evaluate the risk. They test the model using twenty information security risk assessment's data from the China information security risk assessment forum and conclude that this approach can improve the efficiency and accuracy of the assessment process.

Multiple researches created risk models using different techniques. Sahinoglu (2005) applies a decision-tree model to provide quantifiable results to risk management. It takes into account the vulnerability and threat pair along with the existence of a countermeasure to calculate the residual risk. It also uses a criticality factor to differentiate the final risk. The final risk is then multiplied with the investment capital cost to determine the expected cost of loss, that helps to evaluate the cost-benefit of the risk mitigation investment. The model was tested with Monte Carlo simulation to verify the mathematical accuracy.

Pereira and Santos (2009) present a conceptual model for information security risk management in organizations with the following phases: identify the critical assets, identify the vulnerabilities in those assets, identify the threats that might be materialized in attacks, evaluate the risks and assess the policy and security controls involved. It supports business managers in security decision by focusing in 3 nuclear concepts: assets, threat and attack.

Samy et al. (2010) use a survival analysis approach with the Cox proportional hazards model to information security risk management. With this model they are able to identify which threat are most significant for the risk analysis. They advocate that cox proportional hazards model is robust and reliable even with an incomplete baseline.

Bojanc and Jerman-Blažič (2013) present a quantitative model for information security risk management. This model allows a comparison between different technical, people-focused or procedural security measures. The security investments can be compared using economic indicators such as: ROI, NPV and IRR. They also present a defined risk management process and apply this model in a case study to an IT company to safeguard their critical assets. They describe different types

of financial losses due to a security incident: cost of equipment replacement, cost of repairs paid to employers and contractors, corporate income loss, organization productivity loss, loss due to non-compliance and indirect losses such as loss of reputation and intellectual property breach.

Yeo et al. (2014) develop a flow risk reduction model to evaluate risk reduction, by calculating the damage of a risk before and after applying a control, and risk reduction return of investment (RROI) by adding the cost of the control solution. They tested the model with 162 unique random datasets and conclude that this method can demonstrate the trade-offs between risk reduction and investment in security controls.

Dioubate et al. (2015) defend that is difficult to apply a pure quantitative model to information security risk, due to the fact that is difficult "to comprehend numerical data alone without a subjective explanation". To address that limitation the authors propose the use of a risk assessment model that combines qualitative and quantitative approach. The C-RAM Model takes into account the CIA triad to evaluate asset impact, divides likelihood of threat and vulnerability in 5 levels and also evaluates existing risk mitigation controls. The resulting risk will be divided into a 3 priority scale and mapped into the each of the CIA domain individually.

Wang et al. (2013) analyzes how information security risk factors disclosed in periodical firm financial reports influence the occurrence of future security breaches. This study further explores how the textual contents of the written disclosure influences the market reactions. The data gathering process involved 101 firm events across 62 firms between 1997 and 2008 and for those events 43 security risk factors were collected. They develop a classification model that relates the textual risk factors with future breaches. They conclude that firms that disclose risk factors that lead to risk mitigation action are less likely to suffer a security breach in the future. They found no evidence of the relation in the type and the text content describing the disclosure with the market reaction.

Bayesian networks are commonly used in risk management research. Feng and Yu (2012) use a genetic algorithm to search the rules of risk management using historical data with a Bayesian network to predict the occurrence of a security risk. They use 200 historical risk cases and 34 risk factors from a Chinese financial firm to feed the algorithm. The results show that the communication and operation security risk exceeded 35% and the root cause was the lack of change management practices.

Poolsappasit et al. (2012) promote a dynamic security risk management approach using Bayesian attack graphs. They model network security attack graphs in a test network and they use the Common Vulnerability Scoring System (CVSS) to evaluate the existent vulnerabilities. They also

use a cost benefit approach with a genetic algorithm to evaluate 13 security controls that mitigate the risk in that test network.

Distributed systems increase the complexity of risk management practices. Feng and Zheng (2014) develop a cooperative model for calculating risk of information systems in distributed networks using Bayesian networks. They apply the model in a case study to 4 interconnected information systems and conclude that the model has great potential for future extensions and optimizations.

Chivers (2006) presents Security Design Analysis (SEDAN) with the aim of supporting the risk management and security design of large distributed systems. This information model simplifies the task of threat path analysis and the documentation and evaluation of the proposed protection profile that enables risk management decisions. Chivers et al. (2009) explain that the periodic risk assessment of distributed information systems is rapidly invalidated due to multiple changes. Due to these changes, the authors argue that risk assessment and the definition of risk profiles should be done at the information systems component level, which simplifies the ownership and the mitigation of the risk.

Lo and Chen (2012) present a hybrid risk assessment procedure that applies the DEMATEL approach to detect the relationships among control areas, it then uses ANP to rate the likelihood of risks and finally includes the subjective opinions of experts with FLQ-MEOWA. They present a case study of this approach in a health insurance institute in Taiwan by inquiring 5 senior experts with a questionnaire to rank the security control areas. The target of the risk assessment is 5 different information systems. The results of the case study show that controls within the management area should be the priority and they should focus on the information system of health insurance certification.

Amancei (2011) discusses some practical methods for information security risk management by providing examples of criteria for risk assessment, impact and risk acceptance. He uses questionnaires to assess the level of internal control and also evaluates existing controls with a vulnerability assessment. He concludes with the remark that the monitorization of identified risks after the assessment should not be forgotten as the risk exposure might change.

Saluja and Idris (2015) present a information risk management methodology based on statistical Partial Least Squares (PLS) under structural equation modelling (SEM). Their risk analysis methodology begins with the definition of risk indicators to serve as the bases for the statistical analysis. Then they define the statistical attributes of the collected data and use SEM to finalize the process.

The benefits of this approach are the clear definition of security metrics, different risk areas analyzed statistically, possibility of forming a prediction model and consequences of risk directly linked with the business.

Some research focuses on specific technologies or IT service models. Chen et al. (2011) argue that a strategy of information technology diversification minimizes the risk of loss of availability when vulnerabilities are exploited. They propose a model that measures the availability risk, taking into account the level of homogeneity of the technological environment, the correlated failures that the attack might trigger and the investment in the repair process. They explain that redundancy of IT equipment alone, is not sufficient to increase availability, as replicas might share the same vulnerability.

Paquette et al. (2010) enumerate and discuss the security risks associated with the governmental use of cloud computing. They advocate that prior to signing a contract or agreement with a cloud provider it is crucial to have a risk management program in place. They discuss risks such as access with the need to audit privileges and respect the laws of the country in which the information is housed, availability with a proper capacity management and business continuity safeguards, adequate infrastructure with the creation of standards that assure interoperability and avoid compatibility issues, integrity by clarifying responsibility and liability. They conclude by advising governments to adopt a wait and see approach to cloud computing and develop a proper cloud risk management program. Goettelmann et al. (2014) defend the integration of security risk management into business process management for the cloud. They defend the perspective of a cloud broker that helps the cloud client maximize the security while minimizing the risk when selecting a cloud provider. Albakri et al. (2014) explain that it is important to let the cloud client contribute to the risk assessment of the cloud provider by providing risk factors that do not increase the complexity of the cloud provider risk assessment. Cloud clients are the ones that own the data and know how the security violations affect their business. Limiting the interactions between cloud clients and cloud provider to a group of risk factors reduces the complexity of the risk assessment as cloud clients tend to increase. This approach creates the role of cloud service risk assessment manager to conduct the risk assessment and the role of the cloud service provider client communicator to manage the communication of the risk factors. The presented framework allows the constant alignment of the security objectives of the cloud client and the cloud service provider.

Zhang et al. (2010) propose a framework for information security risk management in cloud environments following the plan, do, check and act (PDCA) approach. The framework consists of 7

steps: selecting relevant critical area, strategy and planning, risk analysis, risk assessment, risk mitigation, assessing and monitoring program and risk management review. They test the use of this framework in software as a service logistic platform at the Yunnan University. Kaliski Jr and Pauley (2010) defend the use of risk assessments as a service for cloud environments to mimic the same service model used by cloud premises.

Risk frameworks for secure design and development of information systems also play a vital part in information systems security (Baskerville, 1993). These frameworks promote secure coding practices and evaluate information systems risk not only during the development, but also periodically as systems change and additional modules are added. Futcher and von Solms (2013) formalise the risk management process to establish security requirements from software development. These requirements are part of a secure software development model (Futcher and von Solms, 2007). They follow the common process of risk assessment, divided by risk analysis and risk evaluation and risk treatment, by identifying and implementing controls to mitigate risk. By following this approach it's possible to trace each security requirement to a specific risk. Chowdhury et al. (2012) use malactivity diagrams to model information security risk in the system requirements and software design phase.

As it can be seen by the researches presented in this subsection, most of them are focused on operational risk management and assessment, leaving the risk management decision process out of analysis. They do enhance the body of knowledge by enriching the risk assessment methodology and provide new meaningful phases or steps adapted to a current technology or business industry. The priorities for risk management decision making are left out as they focus mostly on the probabilistic economical models for risk assessment. They fail to address the intangible risks that concern business stakeholders in current enterprises and should be included in risk management decision making.

2.1.2 Maturity risk management

The research presented in this subsection has its theoretical basis in maturity theory and is directly connected with the creation or customization of standards and best practices with a continuous improvement approach for risk management. Some of these standards are adapted to current business sector or industry requirements. These researches have a strong emphasis on the risk process definition and design.

Aagedal et al. (2002) present the CORAS framework that has the main objective of providing methods and tools for the efficient risk assessment of security in information systems. The practical approach of CORAS using UML to model risks has 3 main benefits: precise descriptions of the target of evaluation, act as a visual vehicle to enhance communication among different groups of stakeholders and the modelling technology that facilitates the documentation of the risk assessment results. Beckers et al. (2014) enhanced the CORAS framework with the inclusion of risk management method for an Information Security Management System (ISMS) required by ISO 27001. They follow the general process approach of risk context, risk assessment and risk treatment, but they divide the risk context in 5 steps: develop target description, specify security objectives and assets, conduct high level security risk analysis, define the scales and risk evaluation criteria and finally identify legal aspects. They apply CORAS-ISMS method to a smart grid scenario and conclude that CORAS enhances the planning phase with a structured approach for security risk management.

Coles and Moulton (2003) present a new approach for operationalizing IT risk management called Business Process Information Risk management (BPIRM). The main advantages of BPIRM are the clear definition of ownership of the risks across the multiple business functions and the model ensures that the right people are engaged in the decision making process and also support the decisions' implementation. The authors discuss inhibitors that hinder a mature risk management process: the false sense of security that states that there were no major losses in the past, so the protection level is assumed right, even without assessing it. Moreover with this mindset, risk management, because of its preventive nature, is never a top business priority. Constant business and IT changes also hinder a mature risk management process, because management states that the results of a risk assessment process are true only during a small time period. The process is divided across 6 phases in a continuous improvement and feedback loop: initiate, define, assess, implement, manage and confirm. The initialization phase begins within the business process by identifying its purpose and goals. External factors and resource constraints are also considered in this phase. The definition phase identifies the requirements, that can be divided across information, business and IT requirements. These requirements have clear objectives that are impacted, if a risk occurs. The assessment phase matches each requirement with existing risk mitigation controls. The implementation phase consists of 2 main tasks: the establishment of new controls and testing the effectiveness of existing controls to evaluate if they are adequate. The management phase controls expectations by monitoring deviations according to the established service level

agreement (SLA) and reporting them to management. The last phase confirms the whole process in a brainstorming approach by assuring that risk are affectively managed within the established agreements and evaluates if new risks have arisen due to constant business and IT changes.

ISACA (2007) presents COBIT5 as a business framework, formed out of best practices for the governance and management of enterprise IT. It helps aligning business objectives with IT objectives in a simplified manner, while defining adequate responsibilities across business and IT departments. The main principles of COBIT5 are:

- Meeting stakeholders needs: COBIT5 creates value for stakeholders by ”maintaining a balance between the realisation of benefits and the optimisation of risk and use of resources”;
- Covering the enterprise end to end: It integrates IT business functions and goals into a enterprise wide strategy;
- Applying a single integrated framework: COBIT5 aligns with other relevant standards, because it serves as a best practices framework that can be customized to the enterprise needs;
- Enabling a holistic approach: COBIT5 leverages the accomplishment of business goals with the use of a set of enablers to support the implementation of a governance and management system of enterprise IT.
- Separating governance from management: COBIT5 divides the management from the governance level, as they require different tasks, organizational structures and purposes.

COBIT5 defines governance as: ”governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives” (p. 14). COBIT5 differentiates governance from management with the following definition: ”management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives” (p. 14). The goal of risk optimization is accomplished by addressing business risks related to the ownership, operation, involvement, influence and adoption of IT within the enterprise. Risk management seeks to preserve value by analyzing and mitigating risks that impact business. These risk management practices should be monitored to detect variations in the accepted risk levels.

COBIT5 has a total of 37 process, with 5 of them belonging to the governance domain of ”Evaluate, Direct and Monitor” (EDM). The remaining process are divided across 4 domains: ”Align, Plan and

Organise" (APO), "Build, Acquire and Implement" (BAI), "Deliver, Service and Support" (DSS) and "Monitor, Evaluate and Assess" (MEA). There are 2 processes that deal directly with risk: "ensure risk optimization" (EDM03) in the governance domain and "manage risk" (APO12) at the management layer. EDM03 is described as: "ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of IT is identified and managed". It has the main goals of preserving risk under the tolerated risk level, managing the impact of risks to enterprise value and reduce the potential for compliance failures. APO12 is described as: "continually identify, assess and reduce IT-related risk within levels of tolerance set by enterprise executive management" and should be integrated into an enterprise risk management (ERM) strategy. While EDM03 seeks to understand risk tolerance levels to safeguard business value, APO12 deals with the risk mitigation practices that affect directly IT.

NIST (2010) adopts a risk management process with 5 steps: categorize information system, select security controls, implement security controls, assess security controls, authorize information system and monitor security controls.

Divided by 3 tasks, the categorization step starts by matching the current information system with the business objectives taking into account the current security strategy. This categorization is performed by the information system owner with the consultation of the risk manager and it the result determines the business impact of that information system within the business strategy and influences the controls placed to protect the system. The next task is to describe the information system in the security plan and, as all systems are nowadays interconnected, it's important to document the boundaries of the system with input and output information flows. The last step is to register the information system in the organizational office, along with its key characteristics and the security implications of that system within the organization, namely the applicable security policies and procedures.

The step "select security controls" has 4 tasks. The first task is the identification of common controls for information systems and to document them in a security plan. The next task is to select the applicable controls from the common control list that are adequate to minimize the risk of the selected information system taking into account its categorization. Additional compensation controls not present on the list might be necessary. The selection of controls should be guided by a previous risk assessment. The purpose of each control and its effect on the selected system based on the organizational context should be documented. The next task is to define the strategy for the continuous monitoring of the selected controls, their effectiveness and frequency of monitoring.

The final task the approval of the security plan containing all the selected controls by independent reviewers which is normally composed by the chief security officer and risk manager for example. After the review the plan can be approved or sent back to the information system owner to revise the security categorization and controls.

The step ”implement security controls” has 2 tasks. The first task deals with the implementation of the controls specified in the security plan. These controls should be aligned with the enterprise security architecture. Establish a clear communication path with the information system engineers when necessary to accommodate implementation issues and integration with other information systems. Th next task is to document the functional description of the control implementation in the security plan, detailing planned inputs, expected behavior and expected outputs.

The step ”assess security controls” has 3 tasks. The first task is the documentation of the assessment plan with details regarding the objectives, the methodology used for the assessment and the employed procedures. The plan defines the expectations of the assessment along with the scope of the analysis. If the security controls under assessment are from a third-party then the assessment plan should be documented by that third party. The security assessors or auditors should have the technical expertise and independence to delivers an adequate and impartial report. The next task is to perform the control assessment taking into account the established procedures documented to assess if the controls are functioning as intended. The next task is to document the findings of the assessment in a report. Recommendations to correct the issues found during the assessment should be detailed in the report. The final task is to analyze the report and verify the criticality of the recommendations to evaluate if a remedial action is necessary and gather the resources necessary to initiate the task. It may be necessary to investigate further the detailed findings, to assess if it is possible to find a remedial action that is cost effective when compared to the benefits. These remedial actions require a follow-up to reassess if they are able to correct the inadequate situation. The status of the security plan contains all controls and their effectiveness, along with additional remedial actions to enforce the strength of the modified controls. These changes to the security plan may be added as an addendum to the original report.

The step ”authorize information system” has 5 tasks. The first task is to prepare a plan of action with milestones taking into account the recommendations advised with the exclusion of the immediate remedial action taken. This plan of action takes into account the following criteria: security categorization of the information system and the importance of the weaknesses detected in the security controls. The next task is to present the security authorization package to be adjudicated by the

organization authority. The security authorization package is composed by 3 documents: security plan, security assessment and the plan of action with milestones. These documents allow the decision maker to take risk informed based decisions. Based on the authorization package received the organization authority discusses with the risk manager and security officer the determination of the risk to organizational operations aligned with the enterprise risk management strategy. The last task of this step is to explicitly document the acceptance of the residual risk as a responsibility of the organization authority. This information is stored in the authorization decision document that should be attached to the authorization package.

The final step ”monitor security controls” has 7 tasks. The information systems are changing constantly, so the first task is to analyze the security impact of the proposed changes on the defined security controls. These changes have to documented and changes to the risk state should be updated in the security plan. The second task is the ongoing assessment of security controls after the initial system authorization. This assessment involves a subset of the full list of defined controls and it should be aligned with the risk monitoring strategy. The third task is to conduct the remediation actions based on the result of the continuous assessment. The forth task is to update all documentation taking into account the continuous monitoring process. The documentation includes the security plan, the security assessment report and the plan of action and milestones. The fifth task deals with the reporting process to authorized officials within the organization align with the risk and control monitoring process. The sixth task entails the review and acceptance of the revised risks and the information system risk status as an ongoing monitoring process by the authorizing official. The last task is the decommissioning strategy when an information system is removed from service. Removing an information system from current business requires that some security controls remain in use and all documentation is updated taking into account this new disposal status of the system.

NIST (2011) explains that risk management is ”critical to the success of organizations in achieving their strategic goals and objectives” and should not be viewed only from a technical perspective. It is critical that senior management recognizes the importance of risk management and establishes the governance structures. The establishment of a risk executive function and clear responsibilities are critical steps to manage risk. It should involve the organization, the business processes and information systems at 3 different tiers. Top management should be accountable for risk management decisions and the levels of risk tolerance should be defined. Risk management has the main objective ”to institutionalize risk management into the day-to-day operations of organizations as a priority and an integral part of how organizations conduct operations in cyberspace.” Risk framing

occurs at the organizational level (tier 1) with the definition of a risk management strategy, risk assessment, response and monitoring entail the business processes at tier 2 and the information systems at tier 3.

ISO (2011) in the standard 27005 details the information security risk management process. That process starts with the establishment of the information security risk management context. This context involves the definition of a risk management basic criteria. The basic criteria is divided by risk evaluation criteria, impact criteria and risk acceptance criteria. The evaluation criteria takes into account the strategic value of the information process, the criticality of the assets involved and if they are compliance requirement or contractual obligations. The impact criteria details the damage or costs to the organization with the a specific security event. The risk acceptance criteria is directly aligned with the organization's objectives and policies and takes into account the interests of stakeholders. Risk acceptance levels should have different thresholds and can require additional provisions to managers to be able to accept risks. The context should have a clear scope and defined boundaries. The organization for information security risk management should also be detailed when specifying the context, by detailing the main roles and responsibilities inside an information security risk management process that is adapted to the organization. The definition of decision escalations paths should also be identified inside the organization.

The next phase is the information security risk assessment which is divided among risk identification, risk analysis and risk evaluation. Risk identification is composed by 5 tasks. The first task is to proceed with the identification of assets with defined owners. The second task is to identify threats to those assets and that information can be gathered from previous incidents or external generic threat catalogues. The next task is to document existing controls and evaluate if they are any ongoing risk treatment implementation plans. The next task is to identify existing vulnerabilities that can be exploited by threats. The final task is to identify the consequences on the loss of confidentiality, integrity and availability of information residing on the affected assets.

The second part of risk assessment risk analysis. Risk analysis is composed by 4 tasks. The first task is the selection between 2 methodologies, namely qualitative risk analysis and quantitative risk analysis. Qualitative risk analysis uses a scale of qualitative attributes, for example low, medium and high risk of consequences. This is a subjective scale, but on the other hand is easy to understand. Quantitative risk analysis uses numerical values to describe risk, namely to quantify business losses taking into account historical incident data. This historical data is not always available, namely for new incidents, and this situation might give a false sense of accuracy of the risk

analysis. The second task deals with asset valuation and impact analysis of the consequence of multiple security incidents taking into account multiple loss scenarios. The next task is to determine the likelihood of the incident scenarios described earlier. The last task is to determine the level of risk taking into account the consequences of each scenario and the likelihood.

The last part of risk assessment risk evaluation. This part evaluates the detailed information about the risks gathered in the previous phases taking into account the risk criteria in the context phase and enables the decisions about future actions. The decision context also analyzes compliance and legal aspects related to the evaluated risks.

Risk treatment selects and implements controls to accept or retain, reduce or mitigate, share or transfer and avoid the risks. This also includes the documentation in a risk treatment plan. Some risk mitigation solutions might reduce multiple identified risks and a cost-benefits analysis should be performed to evaluate the viability of each solution. Residual risks should be analyzed with another iteration of the risk assessment phase to verify if additional controls need to be implemented or if the risk falls within the acceptable criteria. This decision with the consultation of the risk treatment plan should be performed by the organization's top management.

The information security communication and consultation is a phase that should always be present to achieve agreement of the risk management strategy among stakeholders with an effective communication. This communication and consultation contributes to an adequate decision making. The stakeholders may have a different point of view regarding the risk management strategy and for example different levels of risk acceptability and this agreement must be established among stakeholders with the identification of benefits.

The information security risk monitoring and review phase should always be present to supply the complete risk picture and to monitor changes in the identified risks and the context of the organization. This phase ensures the continuous alignment of the risk management strategy with the business objectives. This phase monitors, reviews and provides continuous improvement having as input all risk management activities and verifying the validity of the risk management criteria.

Comparison of practices against standards, for example ISO 17799, ISO 27001, ISO 31000 or ISO27005, are also a common practice for research. These researches adapt the standard to the current needs or propose a different approach for a section of the standard. Lalanne et al. (2013) propose a new annex to ISO 27005 standard to take into account service oriented architecture (SOA). They argue that the standard does not account for the type service and only classifies assets as software, hardware and network. They propose a new categorization of vulnerabilities: quality of

service, location of data and processing, loss of control of information, information ownership and the type of information. They also propose a new set of consequences for vulnerability in service exploitation: identity spoofing, tampering metadata, trust in service, quality of service, data stored in a foreign country, prohibited or copyrighted informations, provider with financial difficulties and data recovery.

Njenga and Brown (2010) promote the use of improvisation in information security risk management to be able to adapt to handling exceptional situations. They explain that improvisation can reduce the gap between formal security structures and the actual human security behavior. They analyze this theory within a exploratory case study using grounded theory. The data collected consisted of 11 in-depth interviews. They discuss collective and individual improvisation activities by mapping that behavior with the domains of the ISO 17799. They argue that by including improvisation in information security risk management the organization is able to remain flexible and adapt to detected changes. This enables the organization to take advantage of those changes.

Yang et al. (2013) present a Multi Criteria Decision Model to evaluate information security risk controls. They use DEMATEL to clarify the interrelations between the multiple components. AHP is used to obtain the weights and VIKOR is used to obtain the values of the gaps. They test the model in a empirical case of the government of Taiwan. The Taiwanese government organizations need to assess the risk controls to meet the required information security level. They use the control objectives of ISO 17799 as the basis for the model. They conclude that this method using VIKTOR is more suitable than the traditional ANP method for ranking the control objectives.

Karabacak and Sogukpinar (2005) propose ISRAM: a new method for information security risk analysis that is based on a quantitative approach that uses surveys as the data gathering technique. It employs simple mathematical and statistical instruments to be able to be adapted to different enterprises and minimize the time frame to assess risks. The authors argue that this method provides a good fit for the ISO 27001 organizational certification process as it involves the participation and communication of the staff and management (Karabacak and Ozkan, 2010). This collaborative method enhances the sharing of risk information to foment a risk based culture within the organization.

Ozkan and Karabacak (2010) discuss the information security management practices of eight cases in Turkey taking into account the ISO 27001 standard. They explain that the lack of support and commitment of top management in information security management programmes is seen as a major failure. They argue that a legal dimension that promotes accountability of information security to

top management is a critical step in the success path of information security programmes. This lack of commitment is most noticed when countermeasures to mitigate risk need additional spending. They propose a risk analysis method that promotes collaboration within departments and requires top management involvement from the start and across the programme.

Using the Plan, Do, Check, Act (PDCA) continuous improvement model approach is another approach researched in risk management. Meng (2013) presents an information security risk management approach based on AHP and the Plan, Do, Check, Act (PDCA) method. The approach is applied in a company in the tourism and hotel management area. The process starts by identifying the security risks and it establishes the hierarchy of security risks to be evaluated by AHP. Finally the risk control measures are evaluated across the Plan, Do, Check and Act (PDCA) phases.

Dai et al. (2012) analyse the current situation of information security practices the in IC manufacturing in China and explain that the earlier focus of information security was information confidentiality related to physical documents, but with the proliferation of technology and the Internet, the information security risk management practices have to improve to be able to decide timely the implementation of security controls. They propose a model based on the PDCA methodology with personal control, management control and technology control. They propose activities to be considered across the continuous process of audit and monitor within the model.

Silva et al. (2014) presents an approach to information security risk management using failure mode effects analysis (FMEA) and fuzzy theory. It considers 3 factors of risk: occurrence, severity and detection. It considers 5 security dimensions: access control of IS, security management, IS development security, infrastructure and communication security. They tested the method in an university lab and discover that the dimensions infrastructure and communication security need more investment, while for the other dimensions the focus will be to maintain current maturity levels.

Lai and Chin (2014) apply the failure mode and effects analysis (FMEA) used in the manufacturing industry to the information security domain. The infosec FMEA follows the PDCA cycle. In the plan phase, it starts by selecting and ranking the assets. It identifies the process flow, the potential failure mode and the effect or consequence of that component fails. In the do phase it determines the severity of each effect on the failure, it identifies the cause and estimates the probability of that potential failure. Next it identifies how controls put in place may detect the failure. Taking into account those factors it ranks the risk. In the check phase it evaluates if the risk is acceptable or not and in the act phase it treats risks that are not acceptable. The infosec FMEA was tested with success in a case study in the design and semiconductor intellectual property industry.

The researches in this subsection improve the current body of knowledge of maturity risk management by enhancing current generic standards and continuous improvement methodologies for risk management with additional steps, phases or needed deliverables. Most of them take as the baseline for research standards or best practices such as ISO 27001, ISO 27002, ISO 27005 or COBIT and adapt them to their current needs. They explore new paths to improve continuous improvement methodologies such as the plan, do, check, act cycle. While standards, best practices and continuous improvement methodologies play an important role in risk management, once again the decision process and benefits to stakeholders from the risk mitigation security investments are not addressed.

2.1.3 Behavioral focused risk management

This subsection presents research that is focused on the behavior of people to enhance the risk management process, it has its roots on theories coming from the psychological domain of research.

Lichtenstein (1996) presents 17 factors that influence the selection of a risk assessment method for an organization: cost, external influences such as government and authorities, agreement between management and security staff, organizational structure, complexity, completeness, level of risk, organizational size, organizational security philosophy, consistency, usability, feasibility, validity, credibility and automation. These factors are weighted in 2 different case studies to conclude that usability, in the sense of simplicity and understandability, and credibility play the vital part in the decision to employ a risk assessment method.

Suh and Han (2003) present a 4 stage approach for information systems risk analysis based on a business model. The first stage entails the organizational investigation in which they collect multiple organizational documentation to identify the organization's mission, objectives and business model. With this information they proceed to identify the objectives of each business function and the relative importance of each business function in the organization. They use Analytic Hierarchy Process (AHP) to weight business functions and objectives in a Delphi technique with the managers team. Stage 2 deals with asset identification and evaluation using the same weighting techniques and mapping each asset to the business functions. They take into account asset dependency in the final determination of asset importance, so the asset is classified with the highest weight taking into account its dependencies as input and output information flow. Stage 3 is the threat and

vulnerability assessment and stage 4 gathers all the previous information to calculate the annual loss expectancy (ALE), which takes into account the asset's income loss, asset's replacement cost and threat probability.

Bodin et al. (2008) introduce the concept of Perceived Composite Risk that is gathered from 3 risk metrics. The first metric is expected loss or annual loss expectancy (ALE), the second is expected severe loss that focuses on disasters that put the organization business continuity at risk and the third is the standard deviation of loss. The metrics are weighted by the decisionmaker using the Analytic Hierarchy Process (AHP).

Xinlan et al. (2010) use AHP and group decision making (GDM) to provide a method to gather the assets' value, the vulnerabilities and threats, as the first task of a security risk management process. They use this approach across a test case to conclude that they can easily prioritize the assets that pose increased risks and need the applicability of safeguards.

Spears and Barki (2010) examine the user participation in information systems risk security management to evaluate if it influences the performance of risk mitigation controls. They use three different theories of user participation in information systems development and apply their principles to information security risk management. The first theory is the buy-in theory in which the time invested with the user participation and influence in information systems development raises the system perception as relevant and important. The second is the system quality theory that explains that user involvement develops know-how about business needs, which in turn increases system quality. The last theory is the emergent interactions theory and it is based in the pillar that multiple user and IT professionals interactions contribute to the establishment of a good relationship that influences positively information systems development. They employ a multi method research design with a qualitative research to gather additional data from SOX experts to specify the research model hypotheses and then apply a quantitative research via a questionnaire to verify them. They conclude that user participation in security risk management raises organization awareness of security risks, provides better alignment with business objectives, improves the development and performance of security controls and provides detailed information to build a better security investment business case.

Jourdan et al. (2010) present the results of the practices of information security risk analysis within organizations. The methodology consisted of sending a questionnaire to 300 individuals who hold the "Certified Information Security Systems Professional" (CISSP). This certification assures that the respondents hold the same base of knowledge regarding the researched topic. The results

are based on the responses from 32 CISSPs. The authors argue that questions about information security to organizations are seen as intrusive, which might be the reason for the poor response ratio. The results show that organizations use multiple methodologies to conduct information security risk assessments on a frequent schedule. The information security risk analysis counts with the support of top management according with the collected results. Organizations find hard to calculate the ROI of security investments and most of them do not purchase insurance to cover the loss of information assets.

Ryan et al. (2012) use expert judgement analysis to quantity security risks. They develop a model to evaluate the following questions: ”How often does a computer or system come under attack?”, ”how many of those attacks are successful?”, ”it is worthwhile to make a large investment to protect a system from attacks?” and ”how probable is a successful attack under different protection scenarios?”. They interviewed a group of experts to quantify multiple parameters based on their experience by asking 31 questions. The authors conclude by stating that investments in information security should include a mix security management practices and technological solutions protection.

Stroie and Rusu (2011) discuss approaches to information security risk management. They divide between a proactive and reactive approach. The reactive approach is composed by 6 steps: protect human life, damage control, damage assessment, determining the root cause, repairing the damage and review the process and update policies. The proactive approach is centered in training activities, define and implement formal procedures and establish an internal control system. The risk management process is divided in four phases: design, implement, monitor and improve the risk management system.

Chatzipoulidis et al. (2010) expose multiple perspectives for enterprise risk management with the ultimate goal of information assurance. They explain that information security risk management should be included in an organizational enterprise risk management strategy that enhances compliance efforts. The risk management culture should foster adequate communication with formal security awareness training. This strategy of protecting the organization’s information records with risk management sustains security value as an intangible factor for long business competitive advantage. The risk mitigation measures should be aligned with business objectives and information protection security requirements, in order to carefully justify investments.

Fenz and Ekelhart (2010) test information security risk management methods across 3 phases: verification, validation and evaluation. In the verification phase to test the correctness of calculations

they use sensitivity analysis, results comparison and simulation. In the validation phase they use security experts to validate the results, test an alternate decision process and gather statistical evidence. In the evaluation phase they analyze the decision maker's behavior and review the quality assessment of implemented controls. They argue that the decision to choose a method for information security risk analysis is dependent on the trust on that method. That trust is dependent on the verification, validation and evaluation phases that are part of that method to be able to know if the security investments are going in the right path.

Fenz et al. (2011) present a security risk management methodology and its implementation in a tool called AURUM. They tested this tool in 2 case studies and conclude that the information security ontology that is the basis of the tool provides a common ground for the decision making process of risk managers. The tool allows the modelling of assets, vulnerabilities, threats in a consistent way, uses common best practices for control selection to minimize risk to an acceptable level and allows risk management decisions to personnel without deep knowledge of information security.

Beebe and Rao (2010) embrace situational crime prevention in the information security risk management process. Situational crime prevention is based on the premise that "criminals are rational and engage in crime to benefit themselves". They analyze the following 5 categories inside situational crime prevention: perceived effort, perceived risk, perceived benefit, perceived justification and perceived provocation to commit a crime. They categorize reducing techniques of situational crime prevention as increase effort, increase risks, reduce rewards, reduce provocation and remove excuses. They classify the four dimensions of the attacker: motivation, skills, insider or outsider victim relationship and involvement. They add 3 additional steps to the traditional risk management process. The first step is to classify and group human threats according to the attackers classification in the threat identification and classification phase. The other 2 steps are added in the controls and countermeasures identification phase in risk management namely verifying if the categorization of the techniques of situational crime prevention are applicable and identity countermeasures that influence the attacker's decision making based on that categories. They analyzed 3 case studies in 3 different sectors namely: higher education, finance and information technology industry to validate their security risk management change proposals.

Some of the research in the risk management domain focuses on specific business sectors or industries. Van Deursen et al. (2013) gathers the frequency of security risk scenarios in the healthcare industry, by conducting a Delphi study. The first phase consisted of gathering security incidents in the healthcare industry in a central database, they gathered 2108 from 117 organizations. These

2108 security incidents were grouped into 150 scenarios and subjected to a Delphi study with 3 rounds to evaluate their frequency by 12 security experts in the health sector from different geographical locations. These scenarios were focused in a socio-technical perspective and the results raise the awareness to the need to develop a risk monitoring strategy in the health sector. The results also demonstrate that the frequency of traditional risks is still higher than new risks that are brought by new technology adoption.

Zafar et al. (2014) analyzes the effectiveness of an information security risk management program in a healthcare institution. To assess the effectiveness of the risk management practices they define 9 success factors: executive management support, organizational maturity, open communication, risk management stakeholders, team member empowerment, holistic vies for an organization, security maintenance, corporate security strategy and human resource development. They use a mixed research methodological model with qualitative and quantitative techniques. They conducted a survey with 961 valid response within the institution and interviewed 8 people. They conclude that the employees consider the information security risk management program effective except for the critical factor team member empowerment where the perception is negative.

Mayer et al. (2013) focus on improving the security risk management process in the telecommunications sector in Luxembourg. The research method consisted of gathering specialists in workshops to fulfil 4 main steps: define the business processes involved with each telecom service, describe an information system architecture perspective focused on security risk management for the telecom services, define the baseline of risks for the established processes and architecture and integrate the results into a software tool.

Henrie (2013) analyzes cyber security risk management for SCADA environments. He interviewed 193 professionals within the oil and gas industry in a exploratory case study to understand the current practice. The results detail that organizations use multiple diverse risk management methods and that SCADA risks are growing. A consistent security program is not applied in the current status, as the big picture is often not analyzed. The merge of traditional security systems and their safeguards with SCADA systems is seen as a good approach. Top management support for the cyber security strategy of SCADA systems is lacking and a formal cybersecurity training program should occur to develop the cybersecurity culture.

Tsai et al. (2010) research the perceived risk of information security in online shopping. They administered a questionnaire to 387 online shoppers in Taiwan to clarify security risks such as ”how personal information is handled by online establishments and who has access to it”. They conclude

that users expect that online commerce site managers apply network security technologies in conjunction with security management practices to safeguard their information and secure their online transactions.

The increasing interdependency of risks is also a factor of research with the need to create trusted third parties and share sensitive information. Fang et al. (2014) defend the creation of a security compliance consortium, as a trusted third party, to minimize the risks of inter-organizational information systems. They explain that by using inter-organizational information systems the organizations are subjected to risks from their partners in addition to the internal risks. The accountability objective is also difficult to assure with the complexity of interdependencies. The creation of this community trusted third party will help to monitorize and separate organizations with inferior security profiles from organizations with higher risk assurance levels.

Khidzir et al. (2010) analyze information security risk management practices involving IT Outsourcing. A total of 110 questionnaires were analyzed to evaluate the importance of each of the risk management phases in IT Outsourcing. Risk identification is considered the most critical phase, followed by risk monitoring, risk treatment plan, risk analysis and risk control in the descending order of importance. The authors discuss that the importance given to risk management is found to be greater as the practices employed in reality in organizations.

López and Pastor (2013) argue that a comprehensive risk management process relies on adequate information sharing between organizations. They explain that risk management should be able to adapt to new threats that are known by having a situational awareness of the risk. This situational awareness is influenced by information sharing between similar organizations by common communication channels such as CERTS. They propose four aspects to improve information sharing: ”the creation of incentives for information sharing, information value perception and collaborative risk management, improving data exchange and automation of sharing mechanisms for technical data”.

Zhao et al. (2013) develop a model to manage interdependent information security risks across 3 domains: cyberinsurance, managed security services and risk pooling arrangements. They explain that information security risks are strongly interdependent, because they depend not only on the firm’s security practices, but also from the practices of other collaborating or partner firms. This interdependence can be positive or negative taking into account if the security practices of the main firm are higher or lower than the collaborating firms. This mindset explains that security investments do not only strengthen the main firm but also other firms. Cyberinsurance, managed

security services and risk pooling arrangements are methods of risk transference or sharing. They conclude that managed security services and cyberinsurance provide complete risk transfer, when compared with risk pooling arrangements. They discuss that managed security services promotes more efficient allocation of security resources when compared with cyberinsurance. They explain that the advantage of risk pooling arrangement is the ability to control interdependent risks by tailoring the mitigation of those risks across member firms.

Some of the researches focus on the reasons why risk management practices fail or their limitations. Webb et al. (2014) describe multiple limitations of information security risk management: multiple sources of risk are not included in the risk management process, the risk probability and the resulting losses are simplistic in nature without taking into account multiple important factors and finally the risk assessment process is performed as needed without a clearly defined cycle. They propose situation awareness model for information security risk management that is able to surpass those limitations. They adapted the US National Security Intelligence Enterprise (USNSIE) with the intelligence cycle in 12 phases and included situation awareness steps across the model. This result facilitates improved situation awareness in information security risk management.

Slayton (2015) explains that risk management is ”widely viewed as the way to achieve computer security at the lowest possible cost”. The need to have adequate security metrics that can be objectively used in quantitative risk management will often entail qualitative human judgement. These metrics are prized because they provide objectivity by gaining a knowledge of the current status quo, they can lead to an efficiency increase, enable feedback and control and finally they promote awareness and contribute to learning among employees. The author argues that the most important part of a risk assessment is not the final measure, but the learning that resulted from that process. Risk management is often overlooked due to the need of senior commitment, extra resources resulting in additional costs and time-consuming nature of the process.

Taylor (2015) argues that current risk assessment methods are flawed, because ”management decision regarding information security are often based on heuristics and optimistic perceptions”. The author explains that decision-makers are focused in satisfying, which means solving problems without worrying to maximize the outcome with the best solution. The common potential flaws for risk assessments are: seeking to find similarities with similar events in the same industry, increase the probability of an event that has been recently publicized and anchoring to a severity or probability starting point and adjusting that probability as further information is received.

The researches presented in this subsection explore to new paths for changing the behavior of indi-

viduals towards risk management, discovering new ways to improve the risk management process with active collaboration and information sharing among people from the same or different organizations. Decision making is only addressed at the operational level to improve the risk assessment phase, leaving risk management strategy out of the scope.

2.2 Security investments

Regarding the benefits of security investments, Gordon and Loeb (2002a) present a economic model to evaluate the optimum investment to protect a set of information from a security breach. They discuss 2 classes of security breach probability functions: in the first one the company is better off concentrating its security breach mitigation measures on high vulnerability information sets, while on the second class, the benefit of spending a given amount for increased information security is very small, when an information set is extremely vulnerable. This refutes the myth that information security investments is a function that increases with the level of vulnerability. Tatsumi and Goto (2009) improved the previous model by Gordon and Loeb (2002a) by adding a real options approach that adds the optimal timing of information security investment. It accomplishes that by delaying the activity and deciding when to abandon a security project investment. Daneva (2006) also applies the real options approach to the company's security strategy by participating in value networks to decide what types and how much of each security measure to include in the risk mitigation of information assets. Franqueira et al. (2010) is another research that includes real options thinking in decision making in security investments, that helps decision makers to reason about multiple alternatives not directly comparable and how to deal with the uncertainties in that information.

Matsuura (2008) extends the economic model from Gordon and Loeb (2002a) by adding the concept of productivity space and investigates the optimal security investment from that concept's point of view by analyzing the reduction effect on vulnerability and threat factors. He divides the productivity space in 3 areas: "the no-investment area where both the productivities are low, the mid-vulnerability intensive area where the vulnerability reduction productivity is high, but the threat reduction vulnerability is low and the high-vulnerability intensive area where the thread reduction productivity is high".

Gordon and Loeb (2002b) expose 4 myths about information security investments and the corresponding realities. In first myth: "the accounting concept of return on investment is an appropriate

concept for evaluating information security investments", the authors explain that "the accounting ROI concept is not equal to a true economic rate of return, so it shouldn't be used to evaluate investments", so a better approach is the use of internal rate of return (IRR). The second myth is:"maximizing the IRR on information security investments is an appropriate objective" and the authors explain that in reality the maximization of the net present value (NPV) is the right approach to maximize security benefits. The third myth is: "IRR and NPV are ex post metrics for evaluating the actual performance of information security investments" and the authors argue that in short time horizons the best approach is to anticipate IRR and NPV metrics and compare them with the actual or ex post metrics to evaluate the performance of security investments. In the forth myth, "it's appropriate to invest In security activities up to the level where the investments equal the expected loss from security breaches", the authors conclude that the firm's security investments should not exceed approximately one third of the potential expected loss.

Gordon and Loeb (2006) conducted an empirical study to evaluate the budgeting process for information security expenditures.They concluded that senior information security managers use economic analysis in budgeting security investments, although only a small part focuses on quantifying the benefits from the investments using a net present value (NPV) analysis. Some managers that participated in the study reported that they managed the security budget using historical information based on previous expending and best practices from the industry.

Bodin et al. (2005) use the AHP to decide on security initiatives with a limited budget and the justify to the CIO the increase in funds devoted to information security. They use the triad confidentiality, integrity and availability as the top hierarchy and the subcomponents of authentication, non-repudiation and accessibility for dividing the security budget according to these requirements.

Bistarelli et al. (2006) take the concept of attack trees commonly used in the qualitative risk assessment scenarios, which evaluate characterize different computer security compromises, and bring forward the concept of defence trees. Defence trees add the countermeasures to attack trees for evaluating the security investments from a graphical point of view by visualizing the attacks together with mitigation measures.

There are multiple studies that relate information security investments, with the company's market value loss after a security breach. In a study by Cavusoglu et al. (2004a) they concluded, that among the firms analyzed, the firms lost an average of 2.1% of their market value within two days surrounding a security breach. This severity increases for firms that depend directly from the Internet for their business, also known as Internet firms, and it contrasts with the rise of the market

value of information security firms during that period. During the dot com era Internet firms were penalized more for security breaches in comparison with Internet firms nowadays (Kannan et al., 2007). Cavusoglu et al. (2004a) argue that information security is a key issue for survivability in small firms, instead of the common management argument that a small firm cannot invest in security. Loss of information confidentiality and the sensitivity of the information exposed during a breach also influence the negative effect of the affected companies' market value (Campbell et al., 2003). Breaches that affect non-confidential information and denial of service attacks do not affect the companies' market value so severely. When comparing the long term performance of a firm with adequate security controls and a firm that has been breached, the result shows that the firm that has not been breached shows signs of increased performance (Ko and Dorantes, 2006). This market value loss phenomenon after a security breach behaves differently taking into account different markets as the study by Ishiguro et al. (2006) describes that in the Japanese market affected firms market value loss is noticed slower as in the American market. This market share loss phenomenon also applies to software vendors, when a software vulnerability affecting a product is brought to the public (Telang and Wattal, 2005). Acquisti et al. (2006) analyze a specific data breach that concerns privacy loss to conclude that privacy concerns affect negatively the affected companies' market value, but only for a small time period. Chai et al. (2011) take the opposite approach, they research how security investment announcements influence the firm's market positively using a sample of 101 firms across 10 years. They found out that investors react positively from announcements of security investments by a rate of 1,46% excess return. They differentiate 2 types of security investments: investments solely for improving the protection of business assets and security investments that can be commercially exploited to sell more product or increase market share. They conclude that security investments with commercial exploitation contribute more to an increase in the firm's market value than those for internal security improvement. Legal security requirements such as SOX also influence positively market's reactions to security investments, as investors become more aware of the need for information security. Security investments announced after the legislation are more rewarded with positive reactions, than before the legislation existed.

Cavusoglu et al. (2008) point out the benefits of adopting a game theoretical approach to IT security investments instead of the classical decision theoretical approach, by stating that "hackers alter their hacking strategies in response to a firm's investment strategies". They explain that hackers are rational beings, so they also take into account their effort and resources used in order to succeed, when defining a target to attack, in conjunction with the reward they will obtain with the hack and

the risk of being caught (Cavusoglu et al., 2004b). Game theory entails this cat and mouse duel between the attacker and the firm, instead of the classical decision theory that focuses on natural occurrences and assumes that the decision will have no impact on the attacker's mindset. They conclude that the use of the game theory approach obtains a higher payoff for the firm, when comparing with decision theory approach and this payoff is increased when the firm controls the sequence of actions by forcing the attacker to play a sequential game in which the firm invests first.

Cremonini and Martini (2005) take a similar approach and argue that the Return on Investment (ROI) should be coupled with a new index that they called Return on Attack (ROA). That index takes into account the convenience of the attacker to conduct an intrusion after the adoption of a security measure. The attacker also weights multiple factors before conducting an intrusion, so this new index measures the gain that the attacker expects from a successful attack over the losses that he faces when a new security measure is put into action. The authors conclude that the ROI alone does not take into account the attacker's behavior, so the extension to include also the ROA is able to provide better evaluations on security technology investments.

Bojanc et al. (2012) introduce a quantitative model to manage the investment in information security. This model takes into account the type of security measure when measuring the residual risk, namely preventive, corrective and detective measures. The model enumerates purchase, implementation, upgrade and maintenance costs separately and evaluates ROI, NPV and IRR variables (Bojanc and Jerman-Blažič, 2008a,b). It presents multiple scenarios of real-life situations: a spreading computer virus and a denial of service attack.

2.3 Current Research Gaps

As it can be seen by the literature review, past researches in risk management have a theoretical basis from three main groups: behavioral or human-focused theory coming from a psychology basis, economical, statistical or probabilistic theory and maturity process based theory, where most standards and best practices come from. From a more practical application point of view, the literature reviewed can be clustered into 3 main areas: creating or adapting a risk assessment model, risk management focused on a specific technology or IT service model, and risk management practices adapted to the requirements of a specific industry or business sector.

Most authors place their risk management studies at the operational level. Having a method for risk assessment is important, but what happens with the results? Is the risk assessment report left in a

pile of paper in a manager's desk? What is the organizational risk management strategy? How can the manager judge the multiple recommendations from that report and decide what is critical to the company?

Some authors focus on risk management for specific technologies or service models such as cloud, IT outsourcing, big data, mobile or e-commerce. These studies are important to clarify the risks with new technology adoption and raise awareness among IT managers. When looking at external IT service providers, these risks have an important role, as the clients trust that the service providers are having the adequate due care in risk management concerning their client's assets. Having frameworks, standards and best practices that help managing operational IT risk simplify some compliance tasks, but what happens when a decision should be taken to initiate, change or terminate such an IT service partnership? Is the decision maker able to decide based on risk management strategic objectives from stakeholders or does he simply decide on presented alternatives?

Some sectors, such as health, telecom and banking, have specific risk management requirements that should be taken into account when developing a risk management approach. These research domains are important contributions, but once again the existing studies, do not focus on these requirements at a strategic level, but opt to analyze them at an operational level, by adapting existing standards and best practices for risk management. Is there a risk management strategy for a specific industry? Should the risk management strategy be unique for an organization regardless of the operating business sector?

Maturity process based standards and best practices do offer some advances for risk management evolution, with for example, an organization being able to benchmark their position in comparison with the competition. The baby steps or small operational tasks that organizations should operationalize to advance from maturity step 1 to maturity step 2 provide an operational roadmap for initiatives. How good is a roadmap of initiatives, that may be turned into different projects, without a solid risk management strategy? These maturity standards are able to be audited by an independent auditor to assure compliance. The auditors use a pre-defined checklist, to evaluate the maturity of the organization regarding risk management. Checklists are verified at a point in time and do not assure that the strategical path is correct, they only assure that the requirements presented by the standard are met at that specific time. Multiple companies certified in standards in information security, with those standards having specific requirements for risk management, are later gone by being able not to recover from a security breach. Some of these standards and maturity frame-

works are not developed with the mindset to enhance risk management practices, but as a business generating sources of revenue with the continuous need to keep the certification active. Checklists and auditing guidelines are developed by the same source of the standard, being that source a company or association, which violate the separation of privileges principle. In some cases the creators of these standards and frameworks also assure the certification from their own auditor's pool of resources, violating independence.

Changing risky behavior is a clear requirement of risk management. People are the ultimate risk in information security. They are perceived as being the low hanging fruit by attackers and that explains the use of social engineering to simply bypass multiple procedural or technological controls. How does an organization raise awareness of risks to their employees? Do the employees' values match the current risk management strategy or are they presented with multiple policies that they do not agree?

A solid basis for risk assessment methods has been an economical probabilistic approach, where risks are weighted in money loss taking into account an impact and a calculated probability of that risk occurring. Such approaches are constrained by multiple factors. One of such factors is being able to calculate with precision the impact. What is the value of information? For example when taking into account the CIA triad, availability can be calculated more easily, the system is available or not available. How much money is lost if the system is unavailable? For information confidentiality those calculations can be based on an information classification process, being able to determine different levels of loss based on information criticality. How can we measure the risk for the loss of information integrity? Normally that risk is inherited in a wrong approach from the information availability or confidentiality risk metrics.

Another point is the calculation of the value of intangible assets such as client's trust or organizational culture for example. How much is it worth? Another factor that is important to calculate probabilistic risk models is the threat factor. What is the expertise of attackers? What is the surface of attack? Is the attacker an insider or outsider? In a world where information systems are interdependent and inter-connected to multiple sources and destinations, an analysis with that detail is not possible to achieve with the desired accuracy. Some of the current probabilistic risk analysis performed in organizations do not offer the desired results due to complexity, due to the time effort required to finish and due to constantly changing business reality. This constant change of business turns a today finished risk assessment report, tomorrow useless. These approaches should take into account a long term risk management strategy that allows management to decide according to

business stakeholders objectives.

Taking into account this segmentation of the literature review, it can be seen that researchers are not studying with adequate attention a critical step in risk management: the decision making process. The risk management decision making process should incorporate a defined risk management strategy with prioritization of stakeholders values mapped into clear long term objectives. This study addresses that research gap by focusing on the risk management decision process by integrating stakeholders' values. The value focused thinking approach by Keeney (1992) used in this study is a key step in the justification of the proposed investments to mitigate risk and it may lead to hidden alternatives that were not brought to the decision process initially.

The benefits of risk mitigation security investments can be quantified by traditional methods such as ROSI, NPV, IRR or ALE as it can be seen by reviewed literature. Most of these methods focus on costs and do not account for intangible business benefits and don't provide a solution to realize benefits. Disbenefits such as for example, fall of market shares or loss of reputation after a security breach are difficult to be taken into account (Smith, 2004). Security investments to mitigate cyber risks entail several variables that are guesswork to be accurate for use in those methods, which turn the results of those methods inaccurate (Böhme, 2010; Purser, 2004; Salmela, 2008; Stewart, 2004). For example, gathering information from past historical data taken from reports that detail security incidents worldwide does not mirror the real actual risks, as some organizations continue to not disclose their security incidents (Böhme and Nowey, 2008; Dowland et al., 1999). Some new security incidents do not have adequate historical data and threat analysis for that type of incident is not mature. The context or security level of the organization is not taken into account to maximize benefits by those methods. Hidden benefits will not be realized with those methods, as the focus will turn solely into cost savings, instead of identification and monitorization of additional benefits. The benefits management approach from Ward and Daniel (2006, 2012) not only evaluates cost saving benefits, by relying in financial measures, but also enables the identification and monitorization of intangible benefits, that are crucial in security investments to mitigate cyber risks.

The integration of the decision making process regarding cyber risks and the realization of benefits from those security investments have not been integrated into a single framework to the best of our knowledge. This integrated approach allows to close the cycle starting with the evaluation of risk mitigation alternatives based on a cyber risk strategy and assuring that those investments bring the forecasted business benefits to organizations.

2.4 Way forward

Mintzberg and Westley (2001) state that: ”Thinking may drive doing, but doing just as surely drives thinking”. To the best of our knowledge the decision process for cyber risks has not be carefully researched using an approach that drives thinking by doing, as it is currently an unexplored territory. The value focused approach by Keeney (1992) promotes ”doing” to generate an enumeration of objectives for cyber risk management as a wishlist and promotes ”thinking” with the discussion of those objectives in the decision making process. Mintzberg and Westley (2001) discuss that mindset by explaining: ”Thinking first workshops encourage linear, rational and rather categorical arguments. All too often, the result is a wishlist, with disagreements hidden in different points”. These disagreements are brought to the daylight with the discussion of objectives among participants across multiple scenarios. These objectives based on values will be the main components of the cyber risk decision model. This model will allow organizations to build a strategy for cyber security risk management. Cyber risk management principles will be taken into account to form that strategy.

After the risk management decision is taken and transformed into risk mitigation security investments, another important contribution is the definition and monitorization of business benefits realized with those investments. In this study we use the benefits management approach from Ward and Daniel (2006, 2012) that ensures the realization and monitorization of intangible benefits, that are crucial in security investments to mitigate cyber risks. The ownership and accountability for business changes to be able to realize benefits is also a crucial factor in this approach.

The definition of cyber risk objectives from stakeholders, the creation of a cyber risk management decision model, the definition of a cyber risk strategy oriented by risk principles and the evaluation business benefits from risk mitigation security investments allow to complete the continuous improvement cycle for cyber risk management. This way organizations will be able to enhance their cyber risk management practices, define their cyber risk strategy, justify the decision making process to stakeholders and realize business benefits from those decisions.

2.5 Conclusion

This chapter presents the literature review of the two main topics of this research: information security risk management and security investments. We present the risk management research

literature divided among three groups: economical or probabilistic risk management, behavioral or people focused risk management and maturity or standards risk management. This allows to identify the research gaps on both topics and notice the need for decision making research in cyber risk management and evaluation of benefits from security investments after the decision to implement risk mitigation measures occurs. Decision making research in cyber risk management entails the definition of cyber risk management objectives, creation of a cyber risk decision model and definition of principles to create a solid cyber risk management strategy. The integration of benefits management within this research allows the control and realization of the business benefits originated from the cyber risk management objectives that guided the decision to invest in security controls in the first place.

Chapter 3

Theory & Methodology

"All warfares are based on deception."

—Sun Tzu, the Art of War

3.1 Philosophical Perspectives

Scientific research is influenced by the beliefs in which the researcher generates and analyzes the knowledge that one perceives from reality. These beliefs take into account the ontology, epistemology and methodology. Ontology deals with the assumptions about the nature of the reality, epistemology concerns the ways in which the researcher acquires and justifies the discovered knowledge and methodology describes the process by which this knowledge is captured (Wynn Jr and Williams, 2012). Summarily, scientific research can be characterized by posing 3 main questions: What is the form and nature of reality (the ontological question)? What is the relationship between the researcher and what can be known (the epistemological question)? How can the researcher find out if whatever they believe can be known (the methodological question)?

There are three major philosophical perspectives: positivism, interpretivism and critical realism. Positivism positions itself ontologically as “an objective reality is assumed which can be systematically and rationally investigated through empirical investigation, and is driven by general causal laws” (Shanks, 2007). In the epistemological point of view the researcher stays independent and detached from the context to preserve an objective research. The methodology can be characterized

as generalizable theories that are subjected to empirical testing in the form of hypotheses, that were generated from propositions, to confirm or falsify them. The testing should be replicable. “Falsified hypotheses are then refined based on the reasons for falsification and subjected to further empirical testing” (Shanks, 2007). Orlikowski and Baroudi (1991) detail positivist studies as: ”the criteria we adopted in classifying studies as positivist were evidence of formal propositions, quantifiable measures of variables, hypotheses testing, and the drawing of inferences about a phenomenon from the sample to a stated population.“ They explain, that because this philosophical perspective does not consider the context of the research, it is rooted in the status quo and assumes the researcher does not play an active part in the social reality. The language used in positivist research cannot reflect the everyday language from the participants and must be redefined to eliminate the evaluative dimension, seeking to unify the measurement among researchers. Lee (1991) argues that the positivist approach, also known as logical empiricism, entails “procedures as those associated with inferential statistics, hypothesis testing, mathematical analysis, and experimental and quasiexperimental design.” He explains that the positivist propositions should fulfil “the four requirements of falsifiability, logical consistency, relative explanatory power, and survival.” Positivism characterizes knowledge as absolute and objective and that the reality exists external to human beings. Rooted in the scientific method, the results representing the reality are unbiased and value-free and findings are replicable by other researchers (De Villiers, 2005).

According to the interpretative ontology, the social world is produced and reinforced by humans through their action and interaction and not provided as is. It embraces ”multiple realities which are time and context dependent” (De Villiers, 2005). The epistemological belief is focused in understanding the social process and its context involves that the researcher is intrinsically part of it. The methodology deals mainly with field studies in which the researcher analyzes humans in their social settings. It assumes that “people create and associate their own subjective and intersubjective meanings as they interact with the world around them. Interpretive researchers thus attempt to understand phenomena through accessing the meanings that participants assign to them“ (Orlikowski and Baroudi, 1991). They diverse from factual explanations of the context in analysis without the social actors, but focus on the interpretation of the structures and roles inside that social setting to explain why people act the way they do. The language used by the researcher does not assume a position of neutrality, as the researcher integrates the situation that he studies, where he describes it as close as possible quoting the participants discourse. It is suited to understand the human behavior and its intentions in complex and dynamic situations that are context and time dependent.

Lee (1991) explains that in interpretivism “people create and attach their own meanings to the world around them and to the behavior that they manifest in that world”, so the researcher has the task to interpret the meaning that these people give to the researched phenomenon.

Hirschheim (1985) defends that ”information systems epistemology draws heavily from the social sciences because information systems are, fundamentally social rather than technical systems”, so ”they share all the difficulties associated with social sciences”.

Walsham (1993) explains that broadly interpretive methods of research are adequate to increase the understanding of organizational issues related to computer based systems. These methods are ”aimed at producing an understanding of the context of the information system, and the process whereby the information system influences and is influenced by its context”. The author explains that the interpretive epistemology ”considers knowledge as a social construction, and the use, design and study of information systems in organizations is thought of as an hermeneutic process of reading and interpretation”. An interpretative approach of information systems research is centered in the analysis of the context of an information systems implementation and learning what does the system influences and how does its success is influenced by its stakeholders. The interpretativism focused on the contextualization of the research situation, providing descriptive narratives of the events that characterize a given situation and understanding the meanings of the stakeholders (Smith, 2006).

Klein and Myers (1999) enunciate a set of principles for conducting and evaluating interpretive field studies in information systems:

- The first one is the principle of the hermeneutic circle in which “suggests that all human understanding is achieved by iterating between considering the interdependent meaning of part and the whole that they form.” To understand a complex situation or context, the researcher has to divide it in parts, to understand the meaning of the parts and analyze the relationships that form the whole. From the multiple iterations a whole with shared meaning emerges by connecting the complex web of multiple interpretations.

- The second principle is contextualization and it describes the need to reflect the historical and social background of the research setting in order to interpret the phenomenon. This happens for example in the interpretation of a text that has some historical distance. The moving target under interpretative analysis has to be seen by the researcher not as ”products of history” but as producers within an historical context.

- The third principle deals with the problematic on how the result data is socially constructed by the interaction between participants and researcher. This principle recognizes that the participants also can act as interpreters in the interaction with the researcher, being able to alter their actions and reflected points of view.

- The forth principle reveals the need to relate general concepts about social interaction with the data interpreted. This principle highlights the need for a strong theoretical basis for conducting interpretative research and the possibility of generalization within a predefined context.

- The fifth principle details the contradictions regarding the theoretical research design and the actual findings. When a researcher details his research design he already has preconceptions, on what he may find in the research, nonetheless it is important to acknowledge and confront these preconceptions when analyzing the gathered data.

- The sixth principle explains the multiple interpretations that the participants might give to the same event as they see it. The researcher must analyze the influences that move the social context and retain in his mindset the inherent conflicts of power, economics and values. These different interpretations should be confronted by the researcher in order to revise his understanding of the analyzed subject.

- The final principle warns about the sensitivity necessary to notice biases in the narratives collected from the participants. The principle of suspicion warns the researcher to look below the surface of the problem and refine the ability to spot distortions of the interpreted reality due to the social context. It is necessary to ”read the social world behind the words of the actors”.

Interpretative field studies have to convince the community that the findings or interpretations are credible and worth reading. The reader has to be convinced in 3 dimensions: authenticity, plausibility and criticality (Golden-Biddle and Locke, 1993). Authenticity transmits the reader the feeling of what the researcher experienced in the field by particularizing everyday life and gives vitality to the description of its genuine interpretation. Plausability defies the reader to question himself in the sense of positioning the written research within his previous beliefs. Criticality seeks to shake the reader’s previous beliefs, so he reconsiders his preconceived thoughts based on the presented research results. Interpretivism understands that it is difficult to gather value free data, since the researcher is also part of the reality that is constructed by human factors. It argues that the value of

interpretivism relies in the understanding of the social phenomenon and not in scientific predictions through quantitative statistical tests (Pather and Remenyi, 2004; Walsham, 1995a).

Walsham (1995b) explains that the philosophical basis of interpretative research is the ethnographic research in anthropology, in which researchers interpret the patterns of symbolic action that entail the creation and the business as usual context in organizations. The author evidences the need for a thick description of interpretative case studies to detail as close as possible the interpretation of the social context. The use of theory in interpretative research is characterized by the use of an initial theoretical framework with proven results in another previous context and this framework serves as the ground basis for the early empirical work. The author explains that this previous framework does not represent the final truth, but is a guide to approach the analyzed context. He discusses the two roles of the researcher in the conduction of the empirical work: outside observer and involved researcher. The outside researcher maintains distance from the analyzed personnel and is recognized as being external. This external position favorites honesty within interviews as the respondents do not see the researcher as a stakeholder within the organization that may put their position at stake. The outside researcher has a disadvantage of access to confidential information, which can be minimized with non-disclosure agreements. The involved researcher has access to the everyday life of the business in a insider, albeit temporary, view and can easily get access to more information. This direct involvement is perceived as non-neutral and can influence the frank conversations of the analyzed personnel, as the researcher is regarded not as a normal employee, even if he has a close temporary relation with the subject under analysis. The interpretive researcher's report contains his interpretations of the analyzed people's interpretations and not objective facts.

Walsham (2006) revisits his interpretive mindset and explains that even by adopting the posture of a neutral observer, it is not possible to do totally unbiased research. He says that everyone is biased, because of their background and previous knowledge that influence the ways they interpret information. He argues that a good point in maintaining access to an organization, is to deliver feedback of the results with a presentation or workshop, where the participants can discuss the context and organizational knowledge is generated. He explains that the main reason of the choice of a theory to conduct research in a particular context is direct identification. Direct identification in the sense that the theory fits into the context and also relates to the mindset of the researcher in an insightful manner. Data analysis is seen by the author as a looser approach in which he recognizes the advantages of using coding tools, but also argues that coding tools tend to lock the researcher

in the set of predetermined themes. He advocates that the best method for data analysis and category generation is to rethink periodically what the researcher has learned so far after each field work.

This research will be conducted using a critical realism philosophical approach adapted to information systems (Caldeira, 2000; Mingers, 2002; Wynn Jr and Williams, 2012). This philosophy was first discussed by Bhaskar (1978) in stating ontologically that "things exist and act independently of our descriptions, but we can only know them in particular descriptions". The events exist whether or not the researcher is trained to make the correct observations. It is necessary to theorize those events in laboratory and test if they happen outside the controlled environment in similar but broader situations characterized by an open system. He explains that the world is composed by entities that cannot be observed, although internally structured, and events that can be observable. He details three domains of the real: the empirical domain with events that are observed and experienced, the actual with events that are generated by mechanisms and the real, that entails the others described before, with mechanisms and structures with enduring properties. He argues that the main measure of a good theory is in its explanatory power. The epistemology of critical realism is open and interactive by default in the sense that it doesn't force a predefined method due to socially and historically conditioned knowledge and accepts the development of methods for each analyzed subject, as the focus is a explanatory and not predictive approach. Guba et al. (1994) argue in the same ontological direction by stating that: "the ontology is labelled as critical realism because of the posture of proponents that claims about reality must be subjected to the widest possible critical examination to facilitate apprehending reality as close as possible but never perfectly". It accepts multiple competing theories for describing a phenomenon and assumes that they can be changed and proved fallible. It is no simple task to prove or disprove a theory as critical realism assumes that there cannot be a collection and interpretation of data that is independent from the employed theory. It employs the concept of totality, which implies that there are no isolated elements as they are all connected somehow, even if not evident to the researcher (Orlikowski and Baroudi, 1991).

Critical realism is characterized methodologically as form of retroduction (Sayer, 1984), where we take a unexplained phenomenon and within a theoretical structure, we postulate mechanisms, that if the outcome tendency is verified, can cause the phenomenon to be explained by its pattern. Critical realism is not grounded in a mere description of events, but focuses why they occur by understanding their structures and mechanisms (Porter, 1993). It does not solely accept the self-understanding of the participants, but it criticizes it with a reflective mindset under a pre established

theoretical framework. Critical realism uses triangulation as the preferred test method, which is based on the use of multiple techniques like: interviews, observation and documents. It is based primarily on a qualitative research approach, although it can also use quantitative approach where applicable by specific objects of study. A critical researcher attempts to critique the true social reality and transform it, by shaking the status quo to reveal its static inconsistencies among the dynamic and emergent structures. The main objective does not consist only in understanding the phenomenon, but critically characterize it towards the pre-established framework theorized by the researcher (Orlikowski and Baroudi, 1991). It takes into account the social context and pays attention to social issues that affect participating actors such as power, domination, conflict and contradiction (Howcroft and Trauth, 2004). The critical realist acknowledges and defends its bias when researching a topic by confronting the status quo and challenging beliefs, social practices, routines and assumptions taking into account political, organizational power and stakeholder interests in the analyzed context. Critical realism should go beyond the organizational level if external influences, namely macro-economic, influence the analyzed context. Critical realism embraces theoretical diversity, if different theories complement each other to understand the social reality. Easton (2010) suggests that ”generalisation to theory via case research carried out under critical realist conventions occurs by virtue of clarifying the theoretical nature of the entities involved, the ways in which they act and the nature and variety of mechanisms through which they exert their powers or acted upon by other entities”.

Regarding the use of critical realism in information systems research, the approach deviates for the deterministic positivist and technical view and recognizes that the human influence plays the most critical factor in information systems research in an interpretive manner, but acknowledges why some interpretations dominate the reality in the research context with a focus on causality. Pather and Remenyi (2004) point out the following implications for critical realism in information systems:

- Critical realism bridges the gap between positivism and interpretivism and this is critical because of the strong representation of these two sides in information systems.
- Establish a clear distinction between transitive and intransitive dimensions of knowledge with the difference between the targeted information systems objects analyzed and the theories that are applied in that analysis.
- Critical realism embraces both quantitative and qualitative methods, its main concern is ”to offer deeper explanations as to why the objects of our study appear as they are”.

- Critical realism acts as a facilitator of the multiple disciplines and socio-technical dimensions of information systems, fitting within the awareness of a ”variety of objects of knowledge”.
- The observation of objects of study should be handled with the mindset of the differences between transitive and intransitive notions of knowledge or otherwise this unbiased observation might fail.

3.2 Theoretical foundation

This research uses two bodies of knowledge: value focused thinking and benefits management. Value focused thinking is focused on the decision making process by using objectives based on values and benefits management ensures that benefits are maximized from the investment after the decision takes place. Both these two theories are expected to complement each other due to this difference in focus across two distinct phases that enable continuous improvement. This is specially the match of cyber risk management and value focused thinking, risk management decision making is performed taking into account the risk management appetite of top management aligned with stakeholders objectives. Benefits management will ensure the next part of the cycle after the decision is taken to invest in security controls to mitigate cyber risk. Benefits management will ensure that the benefits from security investments to mitigate cyber risk are maximized. In this section both theoretical approaches will be explained and related research literature that uses those approaches in other context will be presented.

3.2.1 Value focused thinking foundation

The research is rooted in value theory (Catton, 1954, 1959) and the method employed is the value focused thinking approach by Keeney (1992). Catton (1959) explains that valuing is defined by the intensity of the desire to obtain an object and that the preference follows a motivational pattern. The author defines value as ”a conception of the desirable which is implied by a set of preferential responses to symbolic desiderata”. He states that value conceptions are “socially acquired”. He explains that some researchers advocate that values cannot be measured, but he argues that by following a judgement based on values it is possible to make predictions of decisions in a defined context. These values guide the decision makers in a decision analysis process. Keeney (2004)

defines decisions ”as situations where the decision maker recognizes that a conscious choice can be made” and enumerates the elements concerning the skill of decision making:

1. ”Problem: Define your decision problem so that you will solve the right problem”;
2. ”Objectives: Specify what you are really trying to achieve with your decision”;
3. ”Alternatives: Create better alternatives to choose from”;
4. ”Consequences: Describe how well each alternative meets your objectives”;
5. ”Trade-offs: Balance pros and cons of different alternatives for meeting your objectives”;
6. ”Uncertainty: Identify and quantify the major uncertainties affecting your decision”;
7. ”Risk Tolerance: Account for your willingness to accept risks”;
8. ”Linked Decisions: Plan ahead by effectively coordinating current and future decisions”.

The ultimate goal by following value focused thinking in decision analysis should be to select the best alternative, but that is not always possible due the existence of hidden alternatives. The enumeration of values and the creation of objectives serve the principle of eliminating the bad decisions that looked good before, but do not accomplish any of the proposed objectives. The unframing of the decision process should be performed as soon as possible by defining the problem at hand and removing the psychological traps that influence our clear judgement in creating new alternatives without the anchoring in the previous alternatives.

Keeney (1992) explains that values are principles for evaluation of the consequences of action or inaction towards a decision among different alternatives. He enumerates the uses of value focused thinking as it can be seen in Figure 3.1: ”uncovering hidden objectives, guiding information collection, improving communication, facilitating involvement in multiple stakeholder decisions, interconnecting decisions, evaluating alternatives, creating alternatives, identifying decision opportunities and guiding strategic thinking”.

He describes the desirable properties of objectives as:

- “Essential, to indicate consequences in terms of fundamental reasons for interest in the decision situation”;
- “Controllable, to address consequences that are influenced only by the choice of alternatives in the decision context”

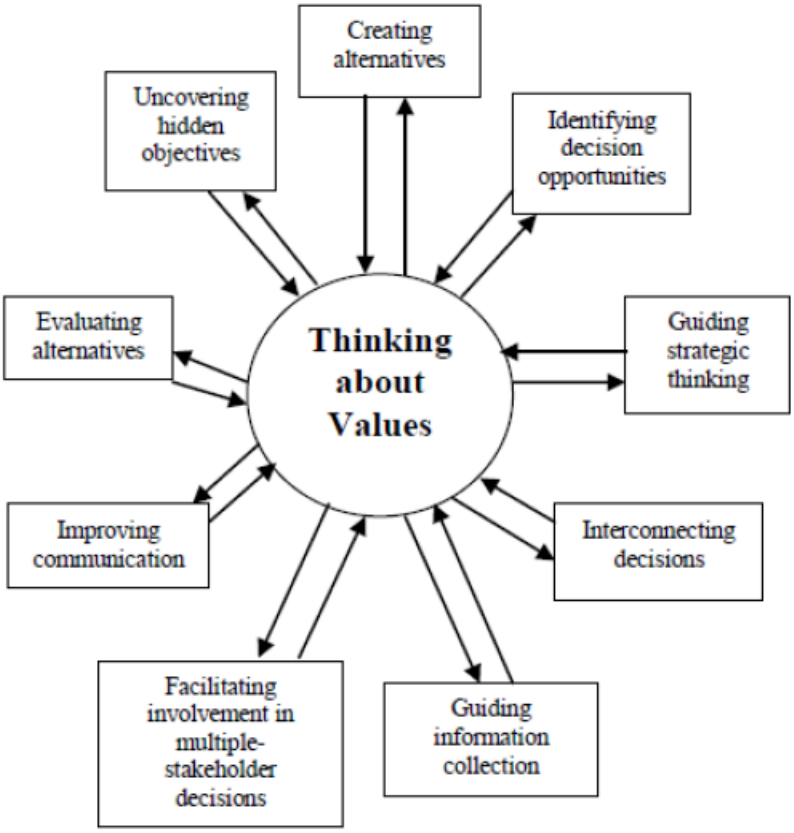

Figure 3.1: Thinking about values (Keeney, 1992)

- “Complete, to include all fundamental aspects of the consequences of the decision alternatives”;
- “Measurable, to define objectives precisely and to specify the degrees to which objectives may be achieved”;
- “Operational, to render the collection of information required for an analysis reasonable considering the time and effort available”;
- “Decomposable, to allow the separate treatment of different objectives in the analysis”;
- “Nonredundant, to avoid double-counting of possible consequences”;
- “Concise, to reduce the number of objectives needed for the analysis of a decision”;
- “Understandable, to facilitate generation and communication of insights for guiding the decisionmaking process”.

The process can be summarized into a 3 step methodology: collect the detailed list of values for the decision context, rewrite those values in a common form and transform them into subobjectives and finally classify the objectives using the WITI test into fundamental objectives and means objectives.

Keeney (1994a) says that this value focused approach is proactive instead of the reactive basis of alternative focused thinking. He describes values as being "principles for evaluating the desirability of any possible alternatives or consequences." Alternatives are not fundamental, they should be viewed as means to accomplish defined values. Decision makers will align their decision structure by expliciting values, thus discovering hidden objectives which lead to adequate information gathering to support the decision process. He describes 10 techniques for identifying objectives of value focused thinking through questions:

- Strategic objectives: What are your ultimate or long range objectives? What are your values that are fundamental? What is your strategy to achieve these objectives?
- A wish list: What do you want? What do you value? What should you want? What are you trying to achieve? If money was not an obstacle, what would you do?
- Alternatives: What is a perfect alternative, a terrible alternative, a reasonable alternative? What is good or bad about each?
- Problems and shortcomings: What is wrong or right with your organization or enterprise? What needs fixing? What are the capability, product, or service gaps that exist?
- Consequences: What has occurred that was good or bad? What might occur that you care about? What are the potential risks you face? What are the best or worst consequences that could occur? What could cause these?
- Goals, constraints, and guidelines: What are your goals or aspirations? What limitations are placed upon you? Are there any legal, organizational, technological, social, or political constraints?
- Different perspectives: What would your competitor or your constituency be concerned about? At some time in the future, what would concern you? What do your stakeholders want? What do your customers want? What do your adversaries want?
- Generic fundamental objectives: What objectives do you have for your customers, your employees, your shareholders, yourself? What environmental, social, economic, or health and safety objectives are important?

- Structuring objectives: Follow means–ends relationships: why is that objective important, how can you achieve it? Use specification: what do you mean by this objective?

- Quantifying objectives: How do you measure achievement of this objective? If not, would you measure achievement of this objective? Which objective is the most important? Why is objective A three times as important as objective B?

Keeney (1988) describes that the structuring of objectives into a hierarchy improves communication among stakeholders thus creating a basis for a common understanding of values leading to compromise to achieve a consensus. The communication barrier with a specific language that separates multiple specialities, such as IT as an example, and the business is minimized by the common understanding of values. The involvement of stakeholders as soon as possible in the decision process increases their willingness to cooperate to reach a common goal. Thinking of values before looking at alternatives will allow a out of the box design of alternatives, that were not discovered beforehand. The creation of scenarios used to detail objectives will also help as a guide to evaluate the effectiveness of existing alternatives. The author states that “one of the most important uses of objectives is to generate ideas to create alternatives”. With this idea in mind, another important step is the creation of a matrix to match the objectives discovered with the alternatives discussed in order to weight alternatives and to conclude if the alternatives take multiple objectives into account.

Strategy and strategical decisions affect the core of an organization, but most organizations have not taken the time to write down the strategic objectives that will guide the management vision. Not only should these objectives be written down and known by top management, but also be shared with the common employee. This foments an internal organizational culture that is the trait of a successful organization. Keeney (1994b) warns that these strategic objectives should not be confused with mission statements that are too vague to bring added value to decision makers and should be clear and understandable by anyone inside the organization.

Leon (1999) defends that value focused theory achieves multiple benefits when compared with alternative focused theory. These benefits are: the alternatives show innovative signs, the range of alternatives has a wider reach, the decision consequences are analyzed with more due care, new alternatives appear and consequences tend to be more desirable. He describes that the greatest difference between alternative based theory and value focused theory is that the in the first approach the alternatives are balanced first without taking into account the objectives of the decision

and in the second approach the objectives, gathered from values, are specified first without focusing beforehand on the alternatives to decide. The decision should be regarded as an opportunity to improve business capabilities instead of a problem that management will be anxious of which path to take. A decision not based on values will be questioned by others and a similar decision presented at a later time could be decided in the opposite way, thus creating business instability. Employees should be able to expect grounded decisions from their managers, instead of unstable mood decision curves without strategic vision.

Gregory and Keeney (1994) argue that value focused thinking is a facilitator in a negotiation situation to reach consensus among stakeholders, as the unique list of objectives is part of the values and contributions from all the people involved in the decision process. This list of objectives forms the context to evaluate alternatives that assure the commitment from stakeholders, even if each stakeholder wants to push a alternative, he will have to justify the inclusion of the alternative as a consequence of multiple previous agreed objectives. The design of alternatives will have also to take into account the accomplishment of the type of objective, namely the division between fundamental and means objective.

Keeney and Gregory (2005) research the process of the creation and selection of attributes that measure the achievement of the defined objectives of value focused thinking. They describe 3 types of attributes: natural, constructed and proxy attributes. The natural attributes are intuitive in nature, in which for example the number of fatalities per time frame is a attribute to the objective of setting automotive speed limits. The proxy attribute is characterized by not measuring the objective directly, but count in conjunction with other attribute to define the objective's achievement. Using the same example of setting the speed limit, the proxy attribute for example can be the number of accidents. The constructed attributes, are like the name explains, the construction of a scale when the natural attribute doesn't exist. Once the scale is known and continuously used, the constructed attribute becomes intuitive and resembles a natural attribute. Proxy attributes are most used when intuitive natural attribute lack information, so they apply to means objectives that influence achievement of the fundamental objective. They explain the desirable properties of an attribute:

- Unambiguous: "A clear relationship exists between consequences and descriptions of consequences using the attribute";
- Comprehensive: "The attribute levels cover the range of possible consequences for the corresponding objective and value judgements implicit in the attribute are reasonable";

- Direct: ”The attribute levels directly describe to the consequences of interest;
- Operational: ”Information to describe consequences can be obtained and value tradeoffs can reasonably be made”;
- Understandable: ”Consequences and value tradeoffs made using the attribute can readily be understood and clearly communicated”.

The process for selecting attributes starts by identifying a natural attribute. The use of a natural attribute to measure an objective facilitates the ordering and understanding of the scale for common people. When that is not possible, we should develop a scale for a constructed attribute. A definition of a good scale for a constructed attribute by specialists will in due time seen as simple as a natural attribute. When it is not possible to construct an attribute, then use a proxy attribute.

The combination of the different attributes into a value model follow 3 main independence concepts Keeney (2001): additive, preferential and utility independence. Additive independence means that the attributes do not escalate taking into account the consequences of the objective, for example saving money on product 1 and saving money on product 2 can be added to fulfil the objective saving money on products. Preferential independence deal with pairs of attributes that are independent from the other attributes. Utility independence normally involve risk situations where the risk taking strategy from one attribute is independent from the fixed levels of other attributes. These independence concepts lead to 2 value model alternatives. The additive value model functions when all attributes are additive independent and the multiplicative value model functions when each pair of attributes is preferential independent and one attribute is utility independent. The common uses of value models are the creation of alternatives, evaluating existing alternatives, product design, guiding information collection, identifying and resolving conflicts ,facilitating decision making, and identifying decision opportunities.

Keeney (2012) ties the common brainstorming techniques with the VFT practice and provides guidelines for the gathering objectives and their alternatives in workshops. This differs from the traditional brainstorming approach by stating the problem and making its objectives and alternatives explicit before engaging in the group discussion of alternatives. This limits anchoring on the alternatives provided by others. To summarize the approach the 4 steps of VFT brainstorming and their specific order are: ”state problem to be solved, identify objectives of a problem solution, individually generate alternative solutions and collectively generate alternative solutions”. He explains that the main goal of a research can be only the identification of objectives, so the step 3 and 4 will

have to be adapted to individually identify objectives and then collectively discuss those objectives to discover additional ones. As managers tend to overlook important objectives, this group discussion and collectively revising the listed objectives, enhances the final objectives' list (Bond et al., 2008). Numerous objectives critical in a decision context tend to slip the mind of the manager with the urge of deciding as soon as possible. Even if this decision period is widened, still important objectives remain unnoticed. This external aid provided by group discussion and brainstorming provides additional objectives to take into account to the decision context that are on average as important as those generated individually.

Keeney et al. (1990) defend the need to "illuminate and clarify public values in complex policy problems". Risk management is an example of such complex policy problems where there's no clear path and different objectives should be weighted to value tradeoffs. Direct value elicitation consists of the interaction with individual to assess their opinions across different policy options. These policy options are composed by activating preference over a group of objectives, while decreasing the weight of others. Focus groups promote the discussion of those values across different example situations. This combination of direct elicitation and focus groups is called value forum. This forum supports a reasonable set of preferences across objectives of a complex theme to guide the creation of a policy. The weighting of objectives is performed with swing weights. Multiple scenarios that explain the different impact of changes in each objective is presented in the forum. Feeling the impact of each of the objectives in real society allows to frame and clearly decide the adequate weight for each objective. There are 2 choices in this value forum model: weighting each of the scenarios to choose the best possible alternative and weighting the changes of each of the objective in each scenario.

3.2.2 Value focused thinking research

The literature review process started by looking at research that employed the value focused thinking in multiple areas namely energy, information systems, information security and operations (Parnell et al., 2013). The problem always resides in the ability to justify a difficult decision by weighting the multiple objectives (Keeney et al., 1986).

Dhillon and Torkzadeh (2006) present an assessment of information systems security in organizations, in which they use a value focused approach with the major objective of maximizing information systems security in organizations. They interviewed 103 managers from multiple organizations and

initially identified general values for managing information systems security and recorded them in a wishlist. In a second phase values are clustered, labelled and converted into security objectives. The third phase consists of the classification of the objectives in the fundamental and means objective group by elaborating the "why is it important?" (WITI) test. The final phase deals with the validation of the objectives list in a panel of experts. The research resulted in 86 objectives that were organized into 25 clusters with 9 fundamental and 16 means objectives. According to the authors a need to amplify the principles beyond confidentiality, integrity and availability arises for designing security, as other objectives were valued by the individuals.

Mishra and Dhillon (2008) develop control objectives based on the values of IT managers using a value focused approach. They classify controls according to scope of control and target of control. In scope of control, controls can be classified as technical, formal and informal. Technical controls target electronic information and can be for example the use of encryption algorithms or authorization mechanisms. Formal controls target organizational structure and management and an example is the enforcement of policies, standards and procedures. Informal controls deal with the importance of values and examples are the expectations of responsibility and accountability. The target of control can be input, behavioral and output. Input controls deal with the alignment of employees with business interest by applying training programs. Behavioral controls determine how work is accomplished in the organization through the following of defined business processes. Output controls manage results by measuring the transformation process. With this classification process in mind they interviewed 54 individuals and gathered 7 fundamental objectives and 18 means objectives related to internal controls. By analyzing the outputs they conclude that technical controls by themselves cannot provide the necessary information security governance that an organization needs. They state that a formal control structure should be present in an organization by enforcing documented policies and procedures via top-down approach with top management awareness and involvement. Informal values should not be underestimated by the business, as they enhance the impact of security governance and motivate employees, if the business and individual values are aligned to achieve a sense of ownership, ethical behavior and trust.

In the article by Drevin et al. (2006), they use value focused thinking when identifying user security awareness aspects. Training is a vital initiative to prevent users from accidentally acting against security without knowing it. Following security controls is simpler for the user if he is aware of the risks involved and the need for security. The information was gathered by conducting 7 interviews using a discussion document instead of a questionnaire. After the fourth interview no new values

were identified. The fundamental objectives identified were based on the confidentially, integrity and availability pillars and others were related to effective use of information systems, responsibility for executed actions and the maximization of resources.

Keeney (1999) uses value focused thinking to develop a comprehensive list of costumer values related to Internet commerce, as the value proposition of a product can be higher or lower if bought online. These values are transformed into objectives composed by: a decision context, an object and a direction of preference. By using costumer values a company can adapt their products to fit the needs of the buyer, but as costumers may have different values, a value proposition in one product for a costumer, may be different for another. Values can also be prioritized by asking the costumers to decide the importance between fundamental objectives, therefore achieving knowledge to create and redesign products. This knowledge allows the creation of a framework for addressing companies decisions that do business over the Internet. The values of prospective customers that were identified in this research will allow the forecast of Internet commerce for a new company.

In Torkzadeh and Dhillon (2002), the authors describe the development of two multidimensional scales to measure the factors that influence Internet commerce success. One of the instruments measures the fundamental objectives gathered by Keeney (1999) and the other instrument measures the means objectives. They identify the multidimensional nature of the factors involved and demonstrate the reliability and validity of the constructs. The research methodology involved 2 phases. In phase 1, they generated and categorized 125 questions, grouped into fundamental and means objectives, that were administered to university students. In phase 2, a sample was extracted from the 421 respondents. The data analysis in phase 1 regarding the means objectives resulted in a 4 factor model after performing factor analysis with 21 objectives. For the fundamental objectives in phase 1 resulted a 4 factor model with 17 objectives. Data analysis in phase 2 suggested a 5 factor model with the addition of the "Internet shipping errors" factor for the means objectives and confirmed the 4 factor model for the fundamental objectives.

Chang et al. (2004) reevaluate the 2 measurement models presented before by Torkzadeh and Dhillon (2002). They used the data from 331 respondents to develop a confirmatory factor analysis following the same data gathering methods. The results are a 5 factor model with 15 items for the means objectives and a 4 factor model with 8 items for the fundamental objectives. In addition to refining the 2 models, they presented a second order model for the fundamental objectives with a very strong goodness of fit.

Dhillon et al. (2002) analyze using a value focused thinking approach the main concerns regarding the privacy of Internet commerce. They interviewed a total of 92 individuals in UK and USA with previous Internet commerce experience to record an initial list of 413 wishes or concerns. After shaping those concerns into means and fundamental objectives they concluded that the main 8 objectives are: maximize discreetness of transactions, increase prevention of fraud, maximize reputation of firm, decrease spam, maximize security of personal information, maximize shoppers ability to control personal data, maximize expectation of shopping privately and maximize privacy relative to ease of online shopping.

Gregory et al. (2001) apply a value focused approach to enhance the decision of public and expert stakeholders regarding environmental risk consultations. The analysis uses a five step process: stating values in the form of objectives, creating a set of alternatives, provide technical information to characterize the impacts of the alternatives, identify tradeoffs and summarize the information into areas of agreement and disagreement. These values can be used to guide time limited discussions in order to achieve agreement more quickly. The authors argue that the elicitation process of describing values will lead to a more informed decision not only subjected to intrinsic emotional bounding or taking into account market analogies. They explain that environmental risk decisions are difficult to take due to their lack of external benchmarks of correctness by balancing company's costs and environmental risk. These decisions are characterized by the diversity of elements that should be considered in the process. The tradeoffs should be subjected to a deep analysis because these decisions involve giving up something valued in order to opt for another element that is also valued for different reasons.This problem leads to a dilemma where deep moral values are put at stake. This experiment was applied to the potential ecological benefits that the salmon habitat could get from changing the way hydroelectric plants work in British Colombia. They prepared a 15 page workbook for alternative focused thinking and a 18 page workbook for value focused thinking. The workbook is a structure to question the audience about risk management and record their answers. The hypothesis presented states that the participation in a value focused thinking approach will lead management to feel more comfortable and satisfied about their decisions. The research concludes by validating the hypothesis demonstrating that participants were able to make higher quality decisions using value focused thinking.

Sheng et al. (2005) help to reveal how the deployment of mobile technology is aligned and strategically impacts an organization using a value focused thinking approach. The set is a case study research of a company in the segment of textbook publishing, where the authors interviewed 12

employees to evaluate how mobile technology supports their job. They identified 6 fundamental objectives: maximize customer service, maximize company image, maximize employee satisfaction, maximize efficiency, maximize effectiveness and minimize cost. Taking into account the objectives identified, the authors concluded that the 3 main strategic implications of mobile technology are: improve working process,increase internal communication and knowledge sharing and enhance sales and marketing effectiveness. Sheng et al. (2010) continue the study of the values of mobile technology and examine how those values adapt to education delivery via a mobile network anytime and anywhere. They interviewed 33 individuals in a University among students and professors to enumerate the following main values: convenience, usability, security, individual privacy, cost and ensure academic honesty.

Keeney and Von Winterfeldt (2010) use the value focused thinking approach in the security defence context by trying to understand the terrorists' objectives when selecting certain modes and targets to attack. Their sources of data to analyze the objectives are Internet terrorists' speeches and propaganda in order to enumerate their values. Using VFT in this context allows to learn the modus operandi of an organized terrorist organization. By defining the objectives for terrorists and also defining the objectives of anti-terrorism actions, this type of research allows the creation and continuous monitoring of a value model to guide national defence decisions (Keeney, 2007b; Keeney and von Winterfeldt, 2011).

Keeney (2001) discusses some of the values for telecommunications management and some of the difficult decisions that managers face such as: product development, Internet commerce,locating new facilities, profit vs. market share, investment to avoid outages, customer quality and guiding all corporate efforts. He explains that values for telecommunication management are complex, because not only the values of the employees are at stake, but also values from stakeholders that are difficult to enumerate. He clarifies the differences between qualitative value models, sustained in a fundamental-means network, and quantitative value models, where measures or attributes for the objectives are specified. He explains that attributes that measure the accomplishment of an objective might be difficult to determine and in that case the attribute can be constructed from simpler attributes.

Daher et al. (2013) use the VFT approach to align business values with information technology objectives. They present a case study of a Brazilian retail company in which the CIO has problems in showing the return of investment from recent IT projects to business objectives. They report that the initial listing of values as a wish list allowed the CIO to discover additional hidden objectives. The

result is the listing of 3 fundamental objectives for maximizing IT aspects for supporting business strategy: ensure agility in business processes, ensure efficiency in IT service and ensure good corporate image with customers.

Merrick et al. (2005a) understand the organizational safety values of a major domestic oil tanker operator deviating from the commonly used probabilistic risk models to evaluate safety procedures. They interviewed 13 organizational staff from 4 domains: vessel crew, health and safety personnel, senior management and vetting personnel. With the safety objectives listed, they evaluated the existent safety performance measures and aligned them with the objectives. This analysis assists the safety decisions to minimize accidents, due to human or mechanical failures and the containment of consequences when an accident occurs.

Morais et al. (2013) use 3 case studies to analyze the decision context with a value focused thinking lens. The decision context of the case studies occurs in: water management, information technology strategic planning and plaster work. In the water management case study they listed 4 fundamental objectives to achieve the strategic objective of maximizing operational efficiency to improve customers' satisfaction: improve operational management, improve the maintenance system, improve staff qualifications and reduce the annual percentage increase of water tariffs. The information technology strategic planning case study was conducted in a Public Hydro-Electric Energy Company and discovered the following fundamental objectives to influence the IT value for the organization: promote competitive advantage for the business, reduce costs and have a good credibility. The third case study deals with plaster work within construction companies and how to deal with their environmental waste in comparison with economic development. The fundamental objectives in this case study are: maximize protecting the environmental and health aspects, maximize the use of plaster, improve the company image, minimize the non-purposeful exploration of gypsum and maximize quality of service. The authors also developed attributes to monitor the achievement of each of the objectives in the different case studies.

Duarte and Reis (2006) uses the VFT approach and the multiple attribute value theory to gather the objectives to help the Portuguese Public Administration to choose among projects implementation. The objectives considered are: "maximize the innovation, maximize the geographical impact (economics of scale), maximize the connection between partners and skills (networking effect), maximize the number of direct beneficiaries (enterprises, citizens and other organizations), maximize the number of agents indirectly benefited (enterprises, citizens and other organizations), maximize the technical skills of employment (jobs created and maintained), maximize the economic efficiency

(economic sustainability) and maximize the synergies between actions (project integration)". The second step consisted of developing multiple attributes from the objectives to be able to weight projects and support decision making. They tested the evaluation framework against 5 project proposals, where 2 projects were terminated after evaluation, and developed a computer interface to be able to apply the same principle to other future project proposals in a simplified approach.

Averill et al. (2009) discusses egress technology, efficient communication and safe evacuation during emergencies from large buildings using a VFT approach during a 3 day workshop. They gathered 7 main objectives: save lives and prevent injuries to occupants, save lives and prevent injuries to firefighters/responders, minimize property damage, minimize impact on property operations, minimize economic costs, reduce stress and reduce grief. The discovery of alternatives to respond to the multiple objectives is also a goal of the workshop, so it was divided into 2 stages. The first stage entails the individual definition of values and their objectives along with the alternatives to achieve those objectives. The second phase includes the group discussion of the proposed objectives and alternatives and the creation of multiple subgroups to reevaluate and discover new alternatives. The alternatives were classified on 3 criteria: quality, feasibility and creativity. Quality deals with effectiveness of the alternative, feasibility concerns the implementation within a 10 year period and creativity awards out of the box ideas.

Dhillon and Chowdhuri (2013) collect individual values for protecting identity in social networks using a value focuses thinking mindset. They interviewed 147 individuals and summarized social media objectives across 19 clusters divided by 5 fundamental and 14 means objectives. The 5 fundamental objectives are: maximize end user trust, ensure development of social networking ethics, ensure authenticity of user identity, maximize identity management to make social networks useful and maximize social networking infrastructure protection. These results deliver a roadmap for individuals and organizations to be able to set up a identity protection strategy for social networks.

May et al. (2013) define value-based objectives for Enterprise Resource Planning (ERP) systems planning. They defend there is commonly a misalignment between organizational business processes and ERP packages. To narrow this gap they use value focused thinking to develop a list of objectives collected with 16 interviews across 3 ERP implementation case studies on Southern Europe. They argue that without determining stakeholders values prior to the ERP implementation, the project will only consider the technical implementation as the main critical success factor, disregarding other social, organizational and contextual factors. The results consists of 13 means objectives and 4 fundamental objectives: minimize cost, ensure ERP benefits realization, enhance

product and service improvement and maximize costumer relationship effectiveness. These objectives, grounded in stakeholders values, aid organizations to understand the complex technical and social issues related to ERP projects and provide the basis to develop an ERP strategic plan.

Barclay and Osei-Bryson (2008) present Project Objectives Measurement Model (POMM) using value-focused thinking and Goal Question Metric (GQM) techniques. They explain that ”POMM involves the elicitation of objectives and measures that reflect the strategic and tactical vision of the project from the perspectives of its multiple stakeholders”. They verify the applicability of POMM with two rounds of interviews among subject matter specialists. The first round involved the gathering of perspectives regarding the model and the second focused on discussing specific points of improvement. They present a practical illustration of POMM within a graduate programme in an university which concerns programme design, thesis development and thesis outcome evaluation. They develop a means and fundamental objectives network and develop metrics to monitor and evaluate the completion of the fundamental objectives. In Barclay and Osei-Bryson (2009), the authors apply POMM to a different project in a large financial services company and evaluate the average priority of objectives collected using value focused thinking. The project consisted of automating a decision support information system to suppress multiple reports that were performed manually.

Barclay and Logan (2013) integrate stakeholders values to enhance the implementation, adoption and delivery of massive online open courses (MOOC) using a value-focused approach. The study takes place in an university in the Caribbean with the collaboration of instructors, students, administrators, online learning specialists, and education executives. The results include multiple means objectives that lead to 5 fundamental objectives: maximize preparedness for the work world, maximize satisfaction with the learning experience, maximize viability of MOOC offering, maximize access to learning and maintain reputation for quality.

Coss et al. (2015) apply a value focused thinking perspective to help venture capitalists align information technology opportunities with investment objectives. This alignment is divided across 4 categories of research: emotional-fit focusing on individual personality and traits, behavioral-fit that is centered in the behaviour characteristics such as motivation and dedication, organizational-fit dealing with processes and resources and financial-fit. They gathered the qualitative values in 52 hours of interview data by interviewing venture capitalists (VC) with a minimum of 10 years of experience. These 130 values were converted into 76 objectives and after forming 22 clusters the final result was 7 fundamental and 15 means objectives. The fundamental objectives are: maxim-

ize VC-Entrepreneur trust relationships, maximize understanding of market-making mechanisms, maximize understanding of the emerging technology market, maximize entrepreneurs financial commitment, maximize confidence of entrepreneur's individual abilities, maximize understanding of marketing strategy and maximize understanding of entrepreneur's competence.

3.2.3 Benefits management foundation

In this research, we will adopt the Cranfield benefits management methodology (Ward and Daniel, 2006, 2012; Ward et al., 1996). Ward and Daniel (2006) define the 5 stages process model for benefits management seen in Figure 3.2: "identify and structure benefits, plan benefits realization, execute benefits plan, review and evaluate results and establish potential for further benefits". The first stage discusses the rationale behind the investment and lists what are the initially expected benefits to the business. The investment should be classified across a strategic, high potential, key operational or support quadrant, taking into account the axis importance to future business and current business. With high importance to current and future business is the strategic investment, with low importance to future business but high importance to current business is the key operational investment, with high importance to future business and low important to current business is the high potential quadrant and finally with low importance to current and future business lies the support investment.

Summarily the main purposes of this first stage are: drivers for change have to map into agreed investment objectives, identify the potential benefits that derive from the achievement of the investment's objectives, combine the IT enablers with the business changes to maximize the realization of the benefits, define owners and measures for the benefits, identify organizational issues that may drive stakeholders to hinder the project and develop a business case that details if the investment shall advance or stop.

There's a clear dependency between realizing the benefits from the investments and assuring the changes necessary for those benefits to occur. To answer that dependency the authors detailed a network map that is called "benefits dependency network" that interrelates the benefits with the necessary changes. Some of the changes can be quickwins but other changes will question if the benefit can really be realized due to the complexity of assigned changes. The creation of the benefits dependency network should involve the contribution from the multiple shareholders to enhance organizational knowledge and establish accountability with identification of a owner to drive each

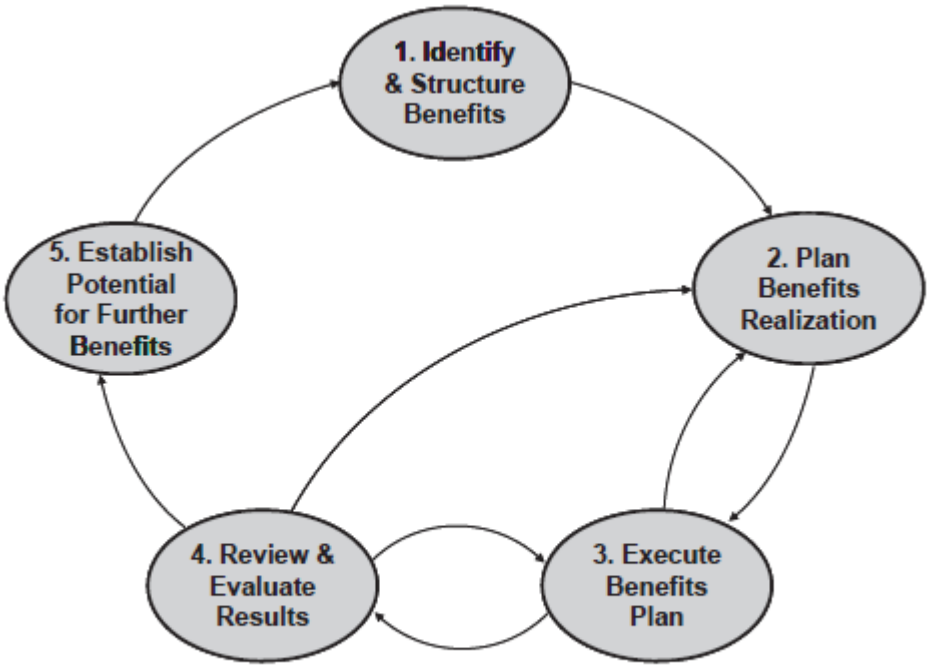

Figure 3.2: Benefits management process (Ward and Daniel, 2006)

necessary change. This ownership of changes will trigger the commitment and the necessary planning to allocate resources to drive the change. The change owner should be someone responsible in the area that the change affects and influential or senior enough, so that the change can be produced. The benefit owner can be different than the change owner and sometimes benefit owners are viewed as a group that must also have an active part in the benefit monitorization and have a close communication with the change owner. The drawing of the benefits dependency network can uncover new benefits from changes that were not thought before. There are 2 types of changes: business changes defined as “new ways of working that are required to ensure that the desired benefits are realized” and enabling changes defined as ”prerequisites for achieving business changes” (Ward and Daniel, 2006) (p. 72 & 73). Examples of enabling changes can be training and education or process redesign. There’s no point in engaging in a benefits management approach for a project, if the strategy is not defined or it is build marginally apart from the core business. The key part of a department like IT or security is to bring added value to the business, so the strategy should be clearly aligned with business objectives.

The second phase is centered in the benefits plan and if necessary a business case to achieve

the top management approval for the investment. It details the following tasks: define responsibility and describe with detail each benefit and necessary change, define measures for benefits and expected results at the end of the project, establish a baseline for benefits measures and introduce new measures as needed throughout the project to ensure benefits realization, establish ownership for running organizational changes and monitor stakeholder involvement that may affect the results of the necessary changes, establish the criteria for evaluating the success of changes and design the benefits dependency network with maximum detail.

A fundamental step in this second phase is the analysis of stakeholders. Normally a step in project management risk analysis, it is known that some individuals will act positively as they are seen as natural beneficiaries, while others will have the burden of accomplishing the changes. Other stakeholders will indirectly lose organizational influence and will resist the changes and try to sabotage the investment. This stakeholder analysis will initially expose those concerns that often result in lack of cooperation and project failure during execution. This analysis details the identification of stakeholders and their positions so that a action plan can be made to encourage the necessary involvement and understand how the resistance can be surpassed and the necessary changes executed efficiently. It is possible to divide stakeholders into 4 groups taking into account the benefits receiver and the changes required: collaborators, compromisors, resistors and accomodators. The collaborators realize high benefits with less changes and should champion the project with high involvement and be prepared to influence others. Compromisors also obtain high benefits but require also high changes to obtain them, so it is important to realize quickwins quickly so that they see the advantages as soon as possible. This group may change its view if the changes are too difficult to execute and no return is gained progressively. Accommodators realize few benefits but also don't have many changes to execute, they should be informed of the project pace and continue their business as usual. The last group is the resistors with few benefits and high changes, they will resist the changes, so it is necessary to take special precautions from the beginning to try to address some of their concerns.

The third stage is the execution of the benefits plan with the adjustment of the necessary changes, as issues and events affecting the plan occur. It entails the necessary monitorization of milestones and the use of key performance indicators as measurable as they can be, optimally linked to financial values. The use of the visually effective benefits dependency network will serve as an additional project guideline to ensure that the benefits and necessary changes occur as similar as possible to the plan and the benefits that enable the business objectives will really be realized. A custodian of

the benefits plan should be designated to interact as the main facilitator among the shareholders that have an active part in the project execution.

The forth stage deals with the post implementation benefit review and the need to evaluate the results after project completion. Some benefits will have been achieved, others have not been fully achieved but may be realized with remedial actions and some of them, hopefully few or none, will not be achieved due to misalignment of initial planning or due to unexpected events. A good surprise from this review will be that additional benefits will turn up as realized and they were not initially planned. The lessons learned from this benefits management case will improve the overall benefits management approach for future investments.

The fifth and final phase details the potential for realizing further benefits, as the uncover of hidden benefits becomes evident after the project implementation. There's always space for continual improvement in processes and this phase ensures it, as business performance may demand further benefits.

Ward and Daniel (2006) explain the need to conduct a business driver analysis periodically, being business drivers the views of top management strategy for the company that need organizational change. They characterize 3 origins of strategic drivers: the content driver focuses solely on IT and its infrastructure, the context driver relates to business reorganization and the outcome driver entails a specific business goal. Having these strategic business drivers defined, now it is necessary to develop investment objectives that address these business drivers. Objectives are detailed in terms of targets to achieve, while the benefits are performance improvements that a organization will achieve if it accomplishes the desired objectives. Taking this mindset into account, a business objective, if correctly achieved, will most of the times realize multiple benefits across a particular or group of stakeholders. As an example objective, the increasing costumer loyalty will derive multiple benefits such as the reduction of costumer account management, improved costumer satisfaction and less marketing spend on costumer acquisition. Most of the benefits are derived from 3 consequences: do new things, do things better or stop doing things The first one deals with doing something absolutely new, namely an innovational work, or redesigning the way things are done. The second one deals with work performance improvement and the last one results from stopping some processes that are no longer needed, normally associated with manual tasks that are planned to be automated. The benefits should also be classified according to its degree of explicitness namely financial, quantifiable, measurable and observable. The observable benefits entails subjective matters and a person should be identified to assess its realization with a objective judge-

ment. This type of benefit should be handled carefully when justifying the investment, because it deals normally with behavioral change, but it may play a vital part for example in the adoption of a new system. Measurable benefits enable improvement in performance, albeit it can not be measured initially how much will it improve after the implementation. Normally this type of benefits is related with process improvement and the adoption of a balanced scorecard or KPIs. A quantifiable benefit exists, when it is clear how much improvement results from the changes. Measurable benefits can be further enhanced into quantifiable benefits by doing a pilot implementation, using modelling, simulation techniques or conducting external benchmarking. Financial benefits quantification happen when they can be measured in the investment currency or monetary terms. This result provides how much will it save taking into account multiple factors like efficiency, accuracy and speed.

3.2.4 Benefits management research

There are multiple benefits management approaches that serve as basis for researches in benefits management of information systems (Nogeste, 2008; Sapountzis et al., 2008, 2009). The benefits management concept is flexible and can act as a complement to multiple methodologies in project management and IT management maturity models (Gomes et al., 2014; Karamitsos et al., 2010).

Ward et al. (1996), as authors of the Cranfield University benefits management approach, define benefits management as: ”the process of organizing and managing such that potential benefits arising from the use of IT are actually realised”. They explain that IT delivers no benefits on its own, but it serves as an enabler to realize business benefits. These business benefits require organizational changes to be able to take the most of the information that IT provides. The necessary changes to maximize benefits should be detailed, with adequate responsibility definition, before the IT project starts, evaluated during its execution and after the project is completed. They present the results of a postal survey of benefits management practices in the UK industry in 1994 to evaluate the status of the current practice, if a methodological process for benefits management is followed and to discover the relevance of a benefits management process model. The target of the questionnaire were senior IT and business managers that worked in large organizations across the public and the private sector. The results show that managers believe there’s space for improvement of the current benefits management practices within their organizations, as post project implementation reviews do not include benefits evaluation and responsibility for benefits management is not defined. The results give proof of evidence that few organizations have a comprehensive benefits

management process and around 50% have formal methodologies for systems development and project and investment appraisal. The results also show that respondents believe it is impossible to identify all benefits for a project before it is completed. Project management practices in surveyed organizations do not account for specific benefits management practices, so benefits are over stated initially to drive forward the investment and not discussed and evaluated in the end.

Remenyi and Sherwood-Smith (1998) present an active benefits realization (ABR) methodology to manage IT projects more effectively. They advocate the identification and continuous involvement of stakeholders in IT projects. The active benefits realization is an iterative process that positions itself as an additional task in the continuous IT project evaluation milestones to ensure that benefits are being monitored and still are being able to be realized at project completion. The main objective of these ABR sessions "is to ensure that the information systems which are ultimately delivered meets the organisation's current business requirements and in so doing provides the best possible collection of specific processes and tools which may be used to maximize the potential business benefits within the information systems terms of reference." These sessions evaluate if further organizational changes are necessary to maximize the benefits.

OGC (2005) explains that benefits management "aims to make sure that desired business change or policy outcomes have been clearly defined, are measurable, and provide a compelling case for investment - and ultimately to ensure that the change or policy outcomes are actually achieved". Change programs require a constant evaluation of benefits to sustain the alignment of IT and business goals. Value delivery starts with the planning of a change programme and "continues through the identification, profiling, tracking and embedding of benefits". This benefits tracking process allows managers to steer the change programme accordingly in order to maximize benefit realization. Managers responsible for project delivery should have an initial task to ensure benefits are monitored and optimized. They present the following benefits management methodology divided by 6 phases: benefits management strategy, benefits realisation plan, benefits identification, optimising the mix of benefits, realising and tracking benefits and reviewing and maximising benefits.

Ashurst and Doherty (2003) present a framework for benefits realization with 3 phases: benefits planning, benefits delivery and benefits review. Benefits planning deals with the definition of the benefits that an IT project will deliver after the implementation finishes and what changes necessary to deliver those benefits are. These benefits are recorded in a benefits plan. After the planning is concluded there's the phase of benefits delivery, in which the actions planned to maximize benefits are executed and monitored. This phase focuses in organizational change rather than the delivery

of the technical solution. The benefits review phase deals with the assessment of the previously recorded benefits and their maximization during project execution. This is the phase for organizational learning, by conducting lessons learned meeting across stakeholders and realizing further hidden benefits that were not recorded in the benefits plan. They conducted a exploratory study using this framework in a large software company with the selection of 16 projects from the knowledge base system. The method used was document review of the 16 projects. The results show than in the benefits planning phase all projects were focused solely in the technology being developed with no linkage between benefits, organizational changes and the project delivery plan. The review of the benefits delivery phase shows that the projects were focused on achieving project deadlines within planned budget with specified functionalities. Once again the focus was on the technological side and, although there was project sponsor identification, the project sponsor did not have clear responsibilities to perform the necessary organizational changes. The benefits review phase was non-existent for all the analyzed projects. The authors conclude that there's a wide gap between benefits management theory and its applicability by project managers in practice.

Ashurst et al. (2008) enhance the benefits realization framework with the creation of benefits realization competences to develop an organizational benefits realization capability. They add an additional phase to the framework for benefits realization (Ashurst and Doherty, 2003): benefits exploitation. This final phase ensures that the benefits realization process does not stop after the IT project is finished and continues to deliver benefits. They developed a exploratory case study that consisted of benefits practices reviewing in 25 IT development projects. They found no evidence of a defined portfolio of benefits management across all 25 projects. Some benefits practices were adopted ad-hoc. Most of them relied on the identification of benefits for initial investment justification to the business, but during implementation those benefits were forgotten giving priority only to the technical features of the project. Although a benefits practice capability is termed in literature as a critical component in bringing value from IT projects to the business, the study gathered no evidence that this capability is being actively exploited by organizations.

Ashurst and Doherty (2014) evaluate the 4 phases of the benefits realization framework across 5 projects from 2010 to 2013. The results show that this research supports the view of the creation of a benefits realization capability to bring added value from IT to business and it contributes also to the inclusion of a benefits realization practice in the day-to-day working routines by changing mindsets.

Peppard et al. (2007) summarize the Cranfield University benefits management approach, that maximizes the benefits obtained from an investment. They state that “most organizations focus on implementing the technology rather than on realizing the expected business benefits”. They explain the organizations are focused in reducing the return of investment through calculations that they forget how an investment can generate benefits. They posed seven questions to IT professionals to discover the current investment goals, characterized by performance improvement, ways that redefine the business processes to work differently and means to regain full IT capabilities exploration. They enumerate 5 principles for realizing IT benefits. The first principle states that IT has no value per se, but the benefit results from effective use of IT resources. The main focus of IT is to create value for the business. The second principle concerns how does IT enable people to change the normal ways of doing the everyday work to a more effective and efficient way. The third benefit explains that realizing IT benefits requires organizational changes so only business managers and users can be beneficiaries. The IT department should not be accountable for the realization of the benefits and this point of view enables the integration of the business in IT projects. The forth principle explains that IT projects can bring negative outcomes to an organization, some of them can even put the business at stake, so the better approach is to avoid the negative outcomes by maximizing the benefits from the positive results. The fifth principle describes that benefits do not happen by a miracle and they must be actively managed to be obtained. The benefits management approach is a continual effort that does not stop while the investment is being implemented and when it is finished. During implementation careful project management has to be established to minimize threats to the benefits and a post implementation review has to take place when the project is finished to discover hidden benefits that can also be realized. In this paper the authors describe 2 types of investments: problem-based and innovation-based interventions. Problem-based interventions deal with problems that the business recognized and can quantify, such as overcoming a disadvantage against the competition. This approach is based on achieving a defined end, the question is how to apply the necessary ways and means to achieve that objective. In innovation-based interventions the business has not a clear view on what to expect and is exploring new terrain. This uncertainty may result in business objectives not correctly described and the burden falls in IT to find out a new and better way of conducting the business. This approach is more focused in technology and does not take into account the necessary changes that the organization must conduct to fully exploit the technology implemented. This innovation-based intervention is subdivided in 2 groups. In the first group, the ways-driven innovation is targeted at taking advantage of an identified opportunity and the approach in this case is to analyze if the

business together with IT can make the business changes necessary to exploit the opportunity by using a new IT solution. The second group is means-based innovation and it appears when a new technology is discovered that shows signs of providing competitive advantage. In this second approach the capabilities of the new technology must be studied first by the IT department to conclude how can the business conduct the changes necessary to exploit the technology and if the benefits realized by the use of this new technological trend are in fact true and can be obtained by this type of organization. They describe a case study of benefits management for a customer relationship management (CRM) application in a large European paper manufacturer where the results were the clear understanding of the changes necessary for the business benefits to be realized. The company realized that their marketing campaigns were ineffective and opted for a single unified process and IT system for the whole group. Another example describes how five hospitals concluded that they must first unify their practices before implementing the new IT system. They conclude that the benefits management approach has been used by more that on hundred companies in the world with the following results: clearer planning of the investments implementation, improved relationships between the business and IT, wiser investments reducing unnecessary spending and the main objective of maximizing the realization of IT benefits.

Ward et al. (2007) extended the Cranfield benefits management approach by adding a section to project portfolio management and conducted a web survey to 106 organizations to evaluate their benefits management practices. They found out that organizations use a business case to justify investments and try to use a benefits management framework, but most of the times this benefit evaluation is performed ad hoc. The organizations that show signs of mature benefits management process differentiate from the others by carefully planning their investments with detailed benefits and have also performed a post implementation review to enhance the knowledge on the progress of benefits realization. Regarding project portfolio management this study concluded that the majority of the organizations performs some sort of unstructured portfolio management of IT projects.

Lin et al. (2000) set the initial guidelines to conduct research of IT investment evaluation and benefits realization in Australia and Taiwan using surveys and case study research. Lin and Pervan (2003) performed a survey that focuses in 3 main topics: "How benefits from IS/IT investments are identified, evaluated, structured, delivered and realized by organizations. What criteria and methodologies are used to evaluate as well as to realize appropriate and adequate benefits. How organizations in Australia attempt to review and improve their current evaluation and benefits realization processes and practices." The survey was directed to the CIOs of the 500 largest organiza-

tions. Although the survey response rate was very low, they concluded that the main perceived IT benefits were: cost savings, process efficiency, competitive advantage and satisfying information needs, as one major point of reference was the alignment of IT benefits to business requirements. They also state that most organizations felt that benefits were overstated at the project approval phase and that the intangible ones were not revisited in a later phase. The IT benefits realization also lacked a formal process, as only one third of the responses reported its formalization. Tsao et al. (2004) follow the same approach to evaluate the benefits of IS/IT investments in Taiwanese Business-to-Business Electronic Commerce companies. They conducted a survey and analyzed 106 responses to reach the conclusions that those companies already use investment evaluation and benefits management techniques, but their use is not effective as most companies show signs of immaturity in their IT benefits management practices.

Lin et al. (2005b) conducted a survey to Taiwanese SMEs to evaluate their IT investments and benefits realisation practices. They issued 400 surveys and received 104 responses. They concluded that IT investments and benefits realisation practices were not effective and the successful adoption of these practices does take into account the company's size, as larger companies tend to adopt these practices more effectively and widely than smaller companies.

Lin et al. (2005a) performed a study to evaluate the benefits of IT investments and its practice in large organizations in Australia. The study used triangulation techniques to gather data, first by conducting a survey with 69 valid responses and then having the problems identified in the benefits management practice, they proceeded to 2 case studies in the public sector to clarify some inconsistencies in the survey results. They discovered that the top 3 reasons for IT investments were: process efficiency, saving costs and competitive advantage. They state that "organizations employing a benefits realization methodology were more likely to: use formal processes for their investment evaluation, be more confident about what they do in their IS/IT activities, have better integration of their IS/IT functions and manage their projects or contracts to achieve better results and with less problems". They concluded that the benefits management practice showed signs of informality and, in some of the organizations analyzed, it evidenced little knowledge about benefits management to guide IT investments.

Irani and Love (2001) discuss the case study of the failure of an organization to adopt a vendor supplied manufacturing resource planning information system. The manufacturing resource planning information system was later implemented with the additional efforts of employees. They analyzed the information systems benefits management approach and discovered the key factors that im-

pacted the result of the information system implementation. They divide the benefits in 3 types: financial, non-financial and intangible. They argue that operational benefits are more tangible in nature and strategic benefits are usually intangible. They state that the strategy ”when evaluating the investment was an act of faith, and thus ad hoc in nature” in the vendor supplied information system and in the bespoke information system the ”significance of human and organizational factors” were not neglected.

Love and Irani (2004) evaluate IT benefits management in the construction industry by examining 126 construction organizations in Australia and their IT investments. They discover that IT investment is not directly influenced by firm size and a major barrier to IT benefits management is the lack of a clear strategic vision. Other findings show that the types of organizations influence significantly the IT investments and indirect costs play a vital part in IT investments decision making.

Irani and Love (2013) analyze not only the expected benefits, but also focus their attention in disbenefits and define them as: ”a disbenefit can be defined as an impact, direct or indirect of ICT, which has an unwanted and negative effect on the performance of an individual or organisation”. Not only should a benefits management plan exist to maximize the benefits, but also to minimize the disbenefits. The authors introduce another problem that they define as benefits leakage, where a benefit that was a business driver for the implementation of an information system is lost to a competitor or another third party during project execution, due to bad timing or external context changing. The authors distinguish between anticipated disbenefits, in the sense that this sort of disbenefits can be managed in a proactive manager and unanticipated disbenefits, which can only be handled in a reactive manner. Examples of anticipated disbenefits can be business disruption due to projects implementation or new information systems learning curves. They warn the unanticipated disbenefits often travel unnoticed, until they turn into a crisis that can put business at stake. These disbenefits are directly viewed as business risks. They classify unanticipated benefits in 3 classes:

- Law of unintended consequences, where the disbenefit arises as a side effect from the implementation of a new information system; Example: Information system performance problems;
- Unforeseen use, that is characterized with the human misuse of technology; Examples: Loss of productivity due to diversion, Email Spam, Hoaxes;
- Creation of new risks, being the impact of those risks legal, personnel or business; Examples: Fraud, Cybercrime.

Irani and Love (2013) enumerate 6 steps for disbenefits management. The first is benefits identification, which can be performed using organized workshops to brainstorm the expected disbenefits. The second step involved the establishment of metrics that can quantify the impact of disbenefits. These metrics are commonly measured in units of money loss, time, risk and health. The third step is setting a target for disbenefit reduction. The fourth step is the creation of an action plan that focuses the human behavior: training, awareness and detailed procedures are common mitigation measures. The fifth and sixth step are common with the traditional benefits management methodology. The fifth deals with the need to measure progress and the sixth entails the periodical review.

Yates et al. (2009) present BeReal: a benefits management framework developed by the Health and Care Infrastructure Research and Innovation Centre to evaluate benefits realization from projects in the healthcare sector. This framework is to be integrated with a collaborative tool that assists the management of the healthcare programme and its projects. They use a multiple case study strategy that applies to different development phases of the healthcare programme. The authors explain that by using a different case study in each phase it aligns with the continuous improvement cycle known as Plan-Do-Check-Act (PDCA). They describe the 4 phases: phase 1 deals with benefits management strategy & benefits realization, phase 2 entails benefits profile & benefits mapping, phase 3 details the benefits realization plan and phase 4 considers benefits evaluation and review. Tillmann et al. (2012) apply the BeReal framework for a programme in a large healthcare organization. The programme consists of the development of the Regional Centre for Teaching, Trauma and Tertiary Care and the analysis is focused on the planning stage. The following contributions of the BeReal framework are detailed in this case study: the adoption of a inclusive process that engages all stakeholders, increasing awareness to the expected outcomes, promoting rational decision making based on expected benefits and providing clear accountability with defined methods.

Caldeira et al. (2012) describe the benefits management approach regarding a case study of the adoption of a paperless information system by a Portuguese hospital. The data gathering was conducted between 2006 and 2011 taking into account the planning and implementation of the information system. The data gathering techniques were semi structured interviews, observation, quantitative analysis of the emergency services and documentation review. 54 benefits were identified and grouped into 8 macro benefits. The benefits were realised with financial saving impact and the increase in the quality of service.

Greenwell et al. (2014) analyze the benefits of cloud investments. They evaluate the benefits across 4 case studies that adopted cloud computing: a micro start-up company, an actuarial services consultancy, a public sector division of large software company and a public sector managed services. They state that in all the case studies a major benefit is cost reduction when evaluating the Infrastructure as a service (IaaS) cloud model. Platform as a service (PaaS) augments the benefits of new product development to achieve competitive advantage. Software as a service (PaaS) creates the ability to innovate in pricing and ownership by redesigning existing software such as CRM and ERP. Cloud storage delivers the benefit of being able to recover from an IT disaster. The cloud ownership of the 4 case studies is divided between public, private and hybrid clouds and all models are able to provide competitive advantage in the short term and support the requirements to enable business strategy in the long term.

Pina et al. (2013) advocate that benefits management can identify the benefits for knowledge management in organizations and, as a consequence, contribute to the achievement of business goals. This point of view is analyzed in a case study of an organization that provides technology services in Portugal and data collection was conducted with document analysis and semi-structured interviews in top and middle management. Document analysis provides the basis for the script used in the interviews. Project management practices and methods are reviewed and knowledge management in those settings is analyzed. During the exploratory case study they discover additional critical success factors to achieve the outcomes of knowledge management: good project management practices, measuring models to monitor KPIs and the creation of mechanisms and systems to facilitate sharing knowledge across the organization. Top management and stakeholders commitment, along with clear responsibility definition, are also factors to be taken into account to ensure knowledge management success. As results, there are 3 main aspects that were critical project success factors: the benefits dependency network, the benefits-oriented use case diagram and the benefits-oriented prototyping. The benefits dependency network aided the project in the sense of visually informing the dependencies and the changes necessary to maximize the benefits, while also considering the stakeholder's interests. The benefits-oriented case diagram served as the basis to maintain the focus on value delivery, before diving into the technical system specifications. Benefits oriented prototyping caused stakeholders to give periodical feedback to the system's evolutionary state, as multiple prototypes were reviewed to evaluate, if the benefits still could be maximized.

Caldeira and Dhillon (2010) detail 23 organizational competencies for gaining IT benefits within organizations using semi-structured interviews in 16 case studies across Europe, Asia and North

America. These competencies are divided in 6 fundamental competencies and 17 facilitating competencies. The 6 fundamental competencies are: ”conduct IT strategic thinking and planning, align IT with business processes and objectives, deploy cost-effective applications and systems, conceptualize the maintenance of data integrity and confidentiality, facilitate behavior enrichment for technology adoption; and ensure compliance with standard IT methods and procedures”. The facilitating competencies function as supporters to achieve the fundamental competencies. The authors conclude that this enumeration of competencies, that involve individual skills and organizational processes, helps firms to evaluate how they are positioned to exploit the benefits of information technology.

Almeida and Romão (2010) describe the benefits management process with a case study of the implementation of an e-invoice system in an airport management organization with the main goals of reducing resources and operational cost with process dematerialization. They explain that the topic of investment in information systems is always related with the evaluation of the return of investment (ROI), but this is a shortsighted vision as some business benefits cannot be quantitatively measured. Data collection started by sending surveys to ten billing departments and to the one corporate accounting department. This data collection procedure served no statistical purposes and the main goal was to evaluate the invoicing process and to establish the initial basis for benefits enunciation. The disbenefits of some stakeholders were managed by integrating them in other areas and developing a career changing plan, as the support for physical invoices was not necessary anymore with the new system. This benefits management approach allows ”strategic alignment of the resources (human, financial or material) with the priorities and objectives of the company and provide a more rational support for decisions involving IS/IT investments”.

Doherty et al. (2008) present the benefits realization process of a Clinical Trial Support System. This system is divided among 4 main areas: trial registration, patient randomization, electronical data capture and adverse events reporting. Although the technical functionalities of the system are easy to evaluate, there’s a major concern on the organizational changes that should be undertaken to realize the benefits from the implementation of the new system. Taking this context into account, this single case study has 2 main research questions: how can the benefits management strategy be adapted and applied to information systems development and during the implementation how does benefits management functions in practice to conduct an assessment of business benefits. The results show that benefits management help to maintain the team focused on benefits and organizational change and stimulates focused communication amongst all the stakeholders.

Doherty et al. (2012) discuss some factors affecting the successful realization of benefits from systems development projects across 3 case studies in the public sector. The first organization is an UK Strategic Health Authority, the second an university and the third a Council transformation programme. They enumerate 6 factors that affect successful realization of benefits from systems development projects: benefits orientation, organizational change, tailor to context, factors are interdependent constructs, life-long application and portfolio focus. Benefits orientation deals with the clear focus on benefits realization that goes beyond the development and delivery of a piece of software. Organizational change ensures that business leadership supports and implements the necessary changes to accommodate the new IT system. Tailor to context clarifies that there is no one size fits all solution in IT development projects and each approach should be tailored taking into account the context of the IT development and the surrounding organization. The authors explain that success factors are interdependent constructs, that should not by analyzed independently. Success factors should be conceived by taking into account the long system lifecycle and not only the initial IT development and deployment stages. Success factors should be applied to a systems portfolio rather, than a specific IT system.

Paivarinta et al. (2007) research the adoption of benefits management of IT investments in Norwegian municipalities. They conducted a Delphi study to define the issues that influence the creation of a benefits management process among 28 expert professionals. The first stage consists in an enumeration of benefits management issues and in the second phase a validation of those issues with the selection of the most important ones is proposed. To perform this selection a division of the experts across 3 different panels is conducted. The third phase deals with the consensual ranking of the benefits management issues. The first and second phase reached its goals with the enumeration of 59 benefits management issues, but in the third phase it was not possible to reach consensus (Paivarinta and Dertz, 2008). The issues were then divided across 4 broad categories:government-level policy for enhancing benefits management, municipality-level policy for enhancing benefits management, organizing the benefits management process and requirements for methods and techniques.

Schwabe and Banninger (2008) analyze the benefits management practices in the Swiss financial sector. They collected data with interviews from top managers across 31 large companies in the Swiss financial sector. They conclude that there is a focus on the initial phases of benefits management with the adoption of benefits in project proposals, but the benefits management practices seem to be forgotten during project execution and rarely evaluated at project closure and during

operation. They asked about the maturity of the process using the COBIT framework and the respondents classified their process as repeatable or defined. The authors conclude that there's a contradiction based on this process maturity, because companies sense that they are mature in terms of benefits management, but they only use benefits management initially to justify the project and forget to reap the benefits during the entire project's lifecycle by doing benefits reviews.

Breese (2012) applies benefits realisation management to government-funded regeneration programmes in the UK. The author discusses that the use of benefits management in regeneration programmes is more complex because it is not centered in a project in a defined industrial sector, but there are diverse programmes that manage funds that deliver external benefits to local communities. The author states that benefits management "will be played out in an ambiguous and contested manner, reflecting the roles and actions of the different stakeholders, who will vary in the degree of power and influence they wield". The author advocates that benefits management should be more tied with an analysis practice and be able to accommodate the ambiguity and uncertainty that arises during projects.

Ahlemann et al. (2013) seek to understand the core principles of benefits management using design theory research. They interviewed 36 top managers from 29 organizations operating in the insurance, banking, logistics, IT provision, energy and retail market industries to discover their benefits management practices. They derive multiple benefits management principles from the requirements and recommendations collected during the interviews: establish accountability for benefits analysis, planning and realization, define goals and incentives for realizing benefits, strategic planning process should incorporate the benefits management approach, define specific processes for benefits planning and realization, establish the change management process for realizing benefits, continuously improve benefits analysis with improved metrics, nurture the benefits management mindset across all departments to improve collaboration and foster the mindset for "spanning cause-effect chains" across the organization.

ISACA (2007) with the COBIT5 framework integrate benefits management as a governance objective to create business value. It has a specific process inside the Evaluate, Direct and Monitor (EDM) domain to ensure benefits delivery (EDM02). This process is described as: "Optimise the value contribution to the business from the business processes, IT services and IT assets resulting from investments made by IT at acceptable costs." It has the main purpose: "Secure optimal value from IT-enabled initiatives, services and assets; cost-efficient delivery of solutions and services; and a reliable and accurate picture of costs and likely benefits so that business needs are supported

effectively and efficiently". A critical part of benefits management is driving organizational changes during a new implementation to be able to maximize benefits. COBIT5 define change enablement as: "A systematic process of ensuring that all stakeholders are prepared and committed to the changes involved in moving from a current state to a desired future state." A change enablement cycle is also presented to maximize benefits following the approach by Kotter (1995). The cycle consists of 7 phases:

- Phase 1 Establish the Desire to Change: This phase seeks to understand the scope of the envisioned change, which stakeholders are to be involved and at which depth, and the ability or readiness of the organization to adopt the planned change.
- Phase 2 Form an Effective Implementation Team: This phase consists of gathering the necessary resources to drive the change. This resources should include people from IT and from business and if necessary external expertise with previous experience such as external consultants.
- Phase 3 Communicate Desired Vision: This phase details the communication strategy with a clear roadmap to achieve the vision with consequences for not adopting the required changes along the path. It should be diffused across stakeholders and expect feedback and suggestions for improvements.
- Phase 4 Empower Role Players and Identify Quick Wins: This phase empowers role functions that should drive the core improvements, functioning as agents of change, and also identifies quick critical tasks that deliver instants benefits and give immediate credibility to change enablement within the organization.
- Phase 5 Enable Operation and Use: During change implementations, the change requirements and objectives should be revisited in order to maximize benefits. Coaching and training should be established to support changes at the operational level. Success factors should capture employee's feelings and behaviours when dealing with change management.
- Phase 6 Embed New Approaches: As changes become mature, it is necessary to document them in written policies and procedures and monitor them for compliance.
- Phase 7 Sustain: The sustainability of a change is achieved with continuing communication and discussing lessons learned during implementation in order to share knowledge and enable corrective measures to drive the continuous improvement process.

The business changes required to maximize IT benefits are also discussed in Ward and Elvin (1999) where the authors distinguish 3 sources of intents for business changes:context driven, outcome driven and content driven. Context driven intent arises from the feeling that something within the organization is not right and has to change. The primary focus is to remove the problem and the business and IT context are vague. The context driven intent requires a clear understanding on why the change is needed with the definition of IT and business content along with the desired outcome. In an outcome driven intent there is a clear vision of the main objective and the focus is to adapt the content to the current context in order to achieve the desired goal. This requires the enumeration of stakeholders perspectives and definition of expected benefits in relation to the necessary business changes. In content driven changes there's the need to change the normal way of doing things, because there's new legislation or the current way of doing that task or process has become obsolete. There's a need to move to a new technology and the focus is on the content of the change, where the benefits are unclear and the outcome undefined. To drive content driven changes it is necessary to characterize the objectives in terms of benefits to establish the outcome clearly. The context in which the content changes occur should be taken into account in relation to the desired outcome.

Gomes and Romão (2013) discuss the contributions of benefits management to a balanced scorecard approach. They explain that the balanced scorecard model is limited in the following categories (Gomes and Romão, 2014): rigidity with the focus centered in the four dimensions, immobility by not being able to adapt to constant business changes, inadequacy to external innovative connectivity by considering the firm in isolation, dealing with knowledge creation, learning and growth only internally within the firm and linear thinking without the consideration of cross-perspective key success factors. These limitations can be mitigated with the use of a benefits management approach by using a benefits dependency network that involves all stakeholders and clarifies business drivers. The benefits dependency network clearly sets responsibilities, details objectives and enables performance measures. The authors corroborate their opinion with the description of a practical case study of the VIAPAV investment by taking a specific objective detailed benefits dependency network and linking it with the strategic objectives using the balanced scorecard strategy map. This linkage between the benefits dependency network and the balanced scorecard strategy map will "enlighten the description how the company will achieve its desired outcomes to satisfying customers, shareholders and employees, including the value proposition (customer perspective), the innovation (internal process perspective), the employee skills and information technology cap-

abilities (learning and growth perspective), and all combined to ensure that the identified benefits will be realized according to the expectations" (Gomes et al., 2013).

3.3 Research Strategy

This section presents the research strategy, detailing the multiple options that will be continuously evaluated during the research. The foundation for case study research is explained along with the case study selection criteria and unit of analysis. The method for data collection and analysis is also discussed.

3.3.1 Overview

The research strategy started by reviewing the literature that concern the main themes of the research: risk management and information security investment benefits. This literature review allows to refine the research questions and establishes the mindset for the research procedures. Maxwell (2008) points out the importance of choosing a good theory for organizing information. He states that: "A useful theory also illuminates what you are seeing is your research. It draws your attention to particular events or phenomena and sheds light on relationships that might otherwise go unnoticed or misunderstood". The two theoretical frameworks used in this research are: value focused thinking and benefits management. Both these theoretical frameworks allow to understand the meaning of events to the people involved, but also the role of the context as an influencer in these events. Another step is to identify studies that used each of the theoretical frameworks. This helps to develop the question guideline that will be used during the interviews. It is important to distinguish between the goals of the research questions and the goals of the interview questions: "research questions identify the things that you want to understand; interview questions generate the data that you need to understand these things" (Maxwell, 2008).

The initial list of values for the underlying problem will be gathered by conducting semi structured interviews with several security and IT professionals. The choice of interviews when compared with surveys relies in understanding the basis and context behind the responses. The researcher understands that he will have to manage more data and will take more time with interviews than with surveys, but the granularity of the gathered data helps to understand the problem at hand with rigour. The problem of surveys is that some targets of the survey, most of the times in top

management, will not answer the survey or will not answer some specific questions. The chosen theme of the research also does not help the survey method, do to confidentiality constrains. Risk management, investments and information security are subjects that are normally not to be responded remotely (Jourdan et al., 2010; Kotulic and Clark, 2004). The problem with interviews is the availability of the interviewees, but once the surface of the face to face access is scratched, the data gathered will be collected with more granularity.

The interview data gathering approach is adequate because values should not be constrained and should be intrinsic from the individual and from the group behavior fomented within the organization. Interviews will be conducted within borders by using general targeted topics, broad categories and examples, but posing open questions that allow the respondent to reflect on his past decisions and review his judgemental values. These values gathered from the interviews will be formulated in objectives by applying an active verb that turns an objective into an effective action. These objectives will be correlated and consolidated by removing duplicates and a WITI test will be performed to separate between fundamental and means objectives in a defined framework. The fundamental objective is characterized by executing the WITI test and come up with the answer: it just is important, based on human nature. The means objective is an dependent objective that is the source to achieve a fundamental objective. When performing the WITI test to a means objective the fundamental objective will be the answer.

These collected objectives will be used as input to generate a decision model for cyber risk management policy decision. These objectives will be weighted using the swing method to be able to help decision makers in the justification of security investments. The weights given and their justification will be discussed in multiple workshops to develop a common understanding of the arguments behind the chosen weight. Scenarios with practical consequences of the application of the risk management objectives will also be subjected to weighting among participants. If possible, different workshops containing only specialists in the field and other workshops containing common IT professionals will be conducted to compare the results afterwards. Conducting workshops in different time frames can also be useful to compare results.

These objectives, and their relative weight in the decision model, will also be taken into account in the planning of a cyber risk management strategy for organizations and develop grounded principles that should be used as a baseline for cyber risk management in organizations. These cyber security strategy based on captured objectives will be subjected to research using a case study approach in organizations with ongoing security programs that impact technology, people and pro-

cesses in the form of policies. Using as a case study an organization that has only technical security controls, which is the most common practice, will amper the results.

A benefits management analysis from security investments will be performed using the same risk management objectives. A benefits management approach will be used that details the necessary changes to be performed to realize the risk management objectives. These benefits will be mapped in a enhanced version of the benefits dependency network that also includes the means and fundamental objectives retrieved from the value focused thinking approach. This benefits management approach will be conducted within a case study involving a security program.

This dual theoretical approach delivers a consistent basis that analyzes the security investment lifecycle, using value focused thinking to enhance the decision making process by detailing objectives based on values and using benefits management to plan and continually monitor the realization of the benefits, that trigger the achievement of the proposed objectives during the investment execution. The post implementation review and the continual improvement phase to discover additional hidden benefits are also part of the benefits management process.

The described research design is illustrated in Figure 3.3.

3.3.2 Case study research foundation

This subsection presents the foundations to perform case study research. Yin (2003) explains that ”doing case study research remains one of the most challenging of all social science endeavors” (p. 1), as it is adequate to explain complex social phenomena. He divides case studies among 3 purposes: exploratory, descriptive and explanatory. Each of the case study purposes can be chosen based on the type of research question, the control over the analyzed behavioral events and the focus on present or past subjects. Research questions beginning with the word ”what” are commonly used in exploratory case studies, questions starting with ”who” and ”where” are characterized by descriptive case studies and the words ”how” and ”why” are mostly found in explanatory case studies research questions. He explains that case study research should not be classified as a research with lack of rigor and states that the generalization is performed to theoretical propositions and not for the entire population. He describes a case study as ”an empirical enquiry that investigates a contemporary phenomenon within its realtime context especially when the boundaries between phenomenon and context are not clearly evident” (p. 13). Case study is a comprehensive research strategy, because is has a specific method for covering the logical research design, data collection

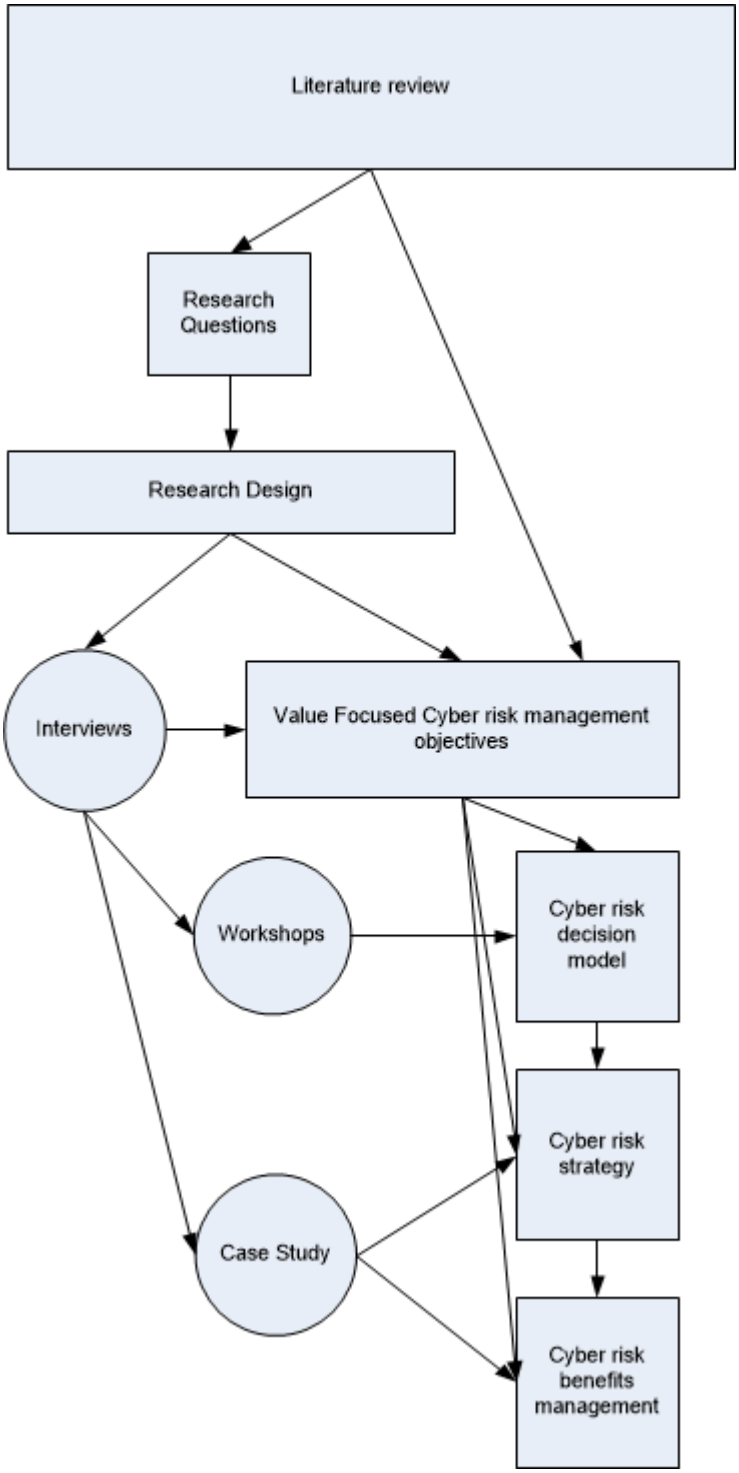

Figure 3.3: Research design

and data analysis.

When designing case studies 4 conditions have to verified to ensure research quality:

- Construct validity: This condition deals with establishing the correct measures for the concepts under study. It entails tasks such as establishing multiple sources of evidence for data collection, maintaining the chain of custody of evidences and present the draft case study report to key individuals to align the content;
- Internal validity (applicable to explanatory case studies only): Explain a causal relationship between 2 or more factors. The tasks are centered in data analysis with pattern matching techniques and logical modeling;
- External validity deals with the problematic in discovering if the conclusions can be generalized or replicated outside of the case study specific context;
- Reliability concerns the ability to verify the research steps by another investigator and reach the same conclusions. It deals with the methodological research protocol with the main goal of minimizing research bias or errors.

Yin (2003) reveals the criteria for choosing between a single and multiple case studies. The single case study occurs when it is supposed to test a refined theory, it details a rare event or context, it is representative or it serves a longitudinal or revelatory purpose. A multiple case study approach is often characterized as being more robust, because of the comparative nature between the multiple cases. The logical mindmap for multiple case studies has to be the verification of the literal replication that deals with achieving the same results based on the proposed theory or the theoretical replication that concerns with concluding different scenarios but understanding why they happen. This contributes to a refined and richer theoretical framework that can later be successfully applied to new case studies. He argues that choosing multiple case studies over a single case study strengths the external validity condition. He enumerates the skills of a good case study investigator: being able to ask the right questions and interpret the answers with the traits of a good listener, be flexible enough to adapt to new situations, but without losing the methodological research focus or being influenced by preconceived behaviour.

Eisenhardt (1989) defines case study as: ”a research strategy which focuses on understanding the dynamics present within single settings”. The author explains that case studies are used in multiple purposes: to provide description, to build theory or to test a pre established theory. When the aim

is to build theory, a situation can happen in which the researcher adapts the focus of the research when he starts to collect data from case studies, because the goal becomes clearer. The selection of case-studies should take into account the need to replicate or to extend the theory and multiple forms of data collection or triangulation should be used to provide stronger substantiation of the propositions. Collection approaches that limit bias include interviewing multiple and high knowledge individuals that have the capability of viewing the phenomena from diverse perspectives due to their diverse geographical, hierarchical or outsider position. During notes taking during an interview the researcher should ask himself the following questions:" What am I learning?" and "How does this case differ from the last?". Data collection ends when theoretical saturation is reached. It means that the effort necessary to increment learning is maximized, because the analyzed phenomena is repeated and only minimal knowledge is added with additional data gathering. There is no ideal number of cases for multiple case study research, but the author points out that "a number between 4 and 10 cases usually works well". The reconciliation of evidence across cases and corroborated with literature review helps the researcher to reframe the proposed theory into a new theoretical vision and due to the clash of possible conflicting realities evidenced by the case studies, it defies the pre established mindset. The theory building process with case studies is directly linked with gathered evidences "and this intimate interaction with actual evidence often produces theory which closely mirrors reality". There are also less positive aspects in theory building from case studies, namely the high volume of gathered data in a case study, that might increase the complexity of developing a theory that entails every perspective. Even if such complex theory is build, it may lack simplicity to be understandable and applied in other cases. The author enumerates some questions that can be used to evaluate case studies to other readers be able to make their conclusions about the fit of the theory in the context: "Have the investigators followed a careful analytical procedure? Does the evidence support the theory? Have the investigators ruled out rival explanations?"

Eisenhardt and Graebner (2007) argue that: "while laboratory experiments isolate the phenomena from their context, case studies emphasize the rich, real-world context in which the phenomena occur". This requires a constant and recursive analysis of gathered data and multiple interactions with different case study individuals. Theory building case study research typically focuses in answering "how" and "why" question in a terrain that remains unexplored with no existing theory providing a feasible answer. The multiple case study approach is advocated in the sense the case comparisons provide an analogy to multiple laboratory experiments, where the theory can be verified among different contexts. The initial theory can increase its robustness with every additional case by being

better grounded by gathered evidence. The authors state that ”multiple cases also enable broader exploration of research questions and theoretical elaboration”.

Benbasat et al. (1987) explains that the use of case studies is adequate in 2 situations: when research and theory are at their early, stage and when the experiences of the participating individuals are important to be analyzed inside their active context. The authors state that ”the case research strategy is well-suited to capturing knowledge from practitioners and developing theories from it” and present the definition that” a case study examines a phenomenon in its natural setting, employing multiple methods of data collection to gather information from one or a few entities”. They enumerate key characteristics of case studies: examine the phenomenon in a natural setting, collect data by multiple means, examine one or few entities, being that entities, a person, a group or organization, study the complexity of the unit intensively, develop a receptive attitude to explore, deny manipulation and experimental controls, there’s no need to specify the analyzed variables apriori, results depend heavily on the ability of the investigator, the investigator may change data collection methods and analyzed sites, as new hypotheses are developed and focus on actual unexplained situations. They explain that ”case studies are more suitable for the exploration, classification and hypothesis development stages of the knowledge building process”. They state that: ”case research is useful in the study of "why" and "how" questions because these deal with operational links to be traced over time rather than with frequency or incidence”.

Woodside (2010) proposes that ”deep understanding of the actors, interactions, sentiments, and behaviors occurring for a specific process through time should be seen as the principal objective by the case study researcher”. This deep understanding also involves the learning of the participants mental models, in which a mental model is: ”the set of propositions a participant in a case understands to be reality”. Maxwell (2008) follows that line of thought by stating that: ”you are not interested not only in the physical events and behavior taking place, but as in how the participants in your study make sense of these and how their understandings influence their behaviour”. He underlines the importance of the context to be able to ”understand how events, actions and meanings are shaped by the unique circumstances in which these occur”.

Stake (1998) divides case studies into 3 groups: intrinsic, instrumental and collective case study. Intrinsic case study deals with the analysis of a particular case of interest that requires further understanding. The purpose is not theory building as this case study is characterized by an unique trait or problem. The instrumental case study provides further insight into theory refinement as it plays the supportive role in the researcher’s pre-established theory. The researcher analyses the

case study in depth detailing its ordinary activities and underlying context to support his theory. When a researcher opts to analyze a group of related case studies to understand a phenomena then we are in the presence of collective case study. The differences and similarities between cases influence the advancement of the understanding of the phenomena under analysis as a whole, where the individual case fails to fulfil that task.

Lee (1989) warns about 4 problems when conducting MIS single case studies: making controlled observations, making controlled deductions, allowing for replicability and allowing for generalizability. Making controlled observations is difficult in case studies due to the lack of laboratory experiments and statistical methods, but it can be surpassed by using natural methodological controls. Making controlled deductions deals with the problematic that in a qualitative case study the validity of the deductions are not mathematical in nature and can not be verified by algebra rules. Despite that constrain it follows the same logical reasoning although not formal so it is also possible to use deductions in a qualitative case study. Allowing for replicability to other MIS case studies raises the discussion that the other case studies do not have the same structure and the same set of organizational events. Replicability can be achieved by using the same theories and methodological steps, adapt them to a different set of initial conditions taking into account the case study settings and even so be able to verify the same theory by using different propositions. The possibility of generalizability follows the same principle of natural sciences in the sense that it cannot be verified with only a single experiment, but it requires the same experiment to be conducted in the case of qualitative MIS research by another case study to verify similar findings.

Case studies are specially suited to analyze information systems within organizations, because they are nowadays the vehicle to restructure the entire organization, while in the past information systems were only a subfunction of the organization. MIS case studies analyze a phenomenon that should be researched within an organizational context, with an in-depth investigation to capture the complex environment where it resides (Paré, 2004). The use of a case study protocol increases the reliability of the research. A typical case study protocol consists of 4 components: the overview of the case study detailing the objectives, issues and topics under investigation, enumeration of field procedures, namely sources of information and access to sites, explaining interview guides or survey instruments and finally a guide for the report that entails the format for the narrative.

Darke et al. (1998) enumerates 5 questions that must be asked when contemplating the use of case study research:

1. ”What kinds of research can be addressed using the case study research approach?”

2. ”How can a case study research project be designed, shaped and scoped tin order to adequately answer a research question?”

3. ”How can the participation of organizations in case study research be obtained?”

4. ” How can case study data be collected from case participants in efficient and effective ways?”

5. ”How can rigour be established in writing up case study research so that is publishable in academic journals?”

To answer the first question Darke et al. (1998) explain that in information systems research the main areas for case study research are the ones where there's few knowledge why some phenomenon occurs, that involves a specific set of experiences from individuals within a context and their behaviour to understand their actions. Emergent areas where theory is lacking to explain a phenomenon that is dynamic and not mature should be also researched with case studies. The second question answers itself with an extensive literature review that helps to position the research question and to refine the scope in the sense that the unit of analysis and number of cases can be determined. The authors argue that the number of cases depends from the focus of the research question, although they ”allow literal of theoretical replication and cross-case comparison”. The case study design depends not only from purpose of the research question, but also from the resources available to the researcher and the deliverables to be documented. The third question relies on the ability that the researcher has to position the research topic in a win-win situation, so that he gathers the participation from targeted organizations. Organizations must explicitly know what to expect from the research and how their internal knowledge can increase with the results. Confidentiality agreements should also be considered between the organization and the researcher, if it entails critical information. The fourth question requires extensive case-study pre-planning by learning the targeted organizations and selecting the positions to interview based on existing documentation. Interview time should be minimized and is only applicable if the information cannot be obtained from another source. Forming a case study research database is also a step that should be prepared before going into the case study field. The last question can be handled with supporting evidence. Case study evidence should be the focus of the researcher's interpretation and alternative interpretations should be considered and their rejection explained. The strategy for data collection and analysis must be explicit and clear to the researcher. The researcher's mindset should always take into account his influences on the researched events and how the case study participants react and adapt to being studied. This bias should be minimized with gathering data

from multiple sources of evidence to corroborate the gathered information.

Caldeira and Romão (2002) argue that information systems research should be evaluated from a diverse perspective that entails social sciences in contrast with a purely technological research. They explain that case study research should be carefully planned and executed in order to capture all the diverse aspects of the social reality in which organizations use information systems. The researcher will mainly use collected evidence and observation to propose explanation models of that analyzed reality that are not an absolute truth but explain the analyzed real context approximately.

Interviews are seen as a fundamental part in case study research, as Fontana and Frey (1994) state that ”interviewing is one of the most common and most powerful ways we use to try to understand our fellow human beings”. Types of interview can be divided in structured, unstructured, group and semi-structured. Structured interviewing entails a group of predetermined questions where the respondent has a limited options of answer types. It is characterized by giving the respondent little room for variation and the interviewer follows the question script in straightforward manner without any flexibility. Group interviews consist of questioning several individuals at once and in this type the respondents also turn into listeners which might influence their answers in a follow the leader mindset, but in the other hand there's the benefit of discussing deeply a problem and the reconnaissance of hidden options which helps exploratory research. One of the two types of group interviews is focus group, which is characterized by a directive role of the interviewer and a structured question format and the other type is brainstorming, in which the interviewer plays a non directive role and the questions are unstructured to promote discussion. Unstructured interviewing, also known as ethnographic or in-depth interviewing, is characterized by an unnoticed informal interview where the interviewer participates without a pre-established mindset of categories and is influenced by the respondent. The interviewer puts himself in the role of the respondent by establishing rapport to understand the situation from the respondent's point of view. Semi-structured interviews present a set of open questions to the respondent without constraining him in the variation of the answer, letting him divagate and explain the reality context, justified most of the times, with real life examples. It allows the interviewer to clarify some aspects of the answer to see if he understands it correctly, by posing questions that were not previously considered. ”The focus of interview research is (mostly) the individual experience of the participant, which is seen as relevant for understanding the experience of people in a similar situation” (Flick, 2008).

The interviewer must discover a style of interested listening where he rewards the respondent with attention, but fails judge orally their responses or direct their conclusions to a pre-established

mindset. If the interviewer adopts an interviewing style that directs the interview too closely without leaving space for the respondent to explain the context, he loses the material evidence. In the other hand if the interviewer is too passive without directing the respondent, the respondent might think that the interviewer is not interested or has no own opinion about the subject researched (Walsham, 1995b). The most used interview data gathering techniques are tape recording and notes. Tape recording has the downside that may constrain the respondent in some answers about sensitive matters or the respondent may not allow it, but allows the researcher to collect more data than using note taking. Interview schedule and its duration should be maintained with the consequence of losing additional information, but it is better to lose information and reschedule if necessary, than to irritate the respondent if he is pressured with other business matters (Walsham, 2006).

Dubé and Paré (2003) explain that case study research has the versatility to use any philosophical perspective: positivism, interpretivism or critical. It can combine qualitative and quantitative data collection methods. They explain the importance of carefully describing the research design, data collection and data analysis methods in case study research. They advise on best practices to achieve rigor in case study research, namely in the research design phase: clearly identify research questions, describe the rationale behind the case selection, use pilot cases if necessary, consider the use of longitudinal case studies and consider rival theories to increase the validity of case studies. In the data collection phase they advise on providing detailed information on the data collection methods and use triangulation to increase validity. In the data analysis phase they advise to provide detailed description of the analytic methods and procedures, increase the use of preliminary data analysis techniques to provide means to reflect early on the data, provide quotes to increase the judgmental view of the reader and compare the findings with existing literature. They argue that although data analysis is a critical step in case study research, it is normally the least documented part. In Dubé and Paré (2001), the authors consider additional areas of improvement for case study research such as: ”strategies for enhancing case study rigor and limits and relevance of the case study”.

3.3.3 Case study selection criteria

Case study selection starts by looking at organizations that have direct responsibility in safeguarding the protection of sensitive information and critical infrastructures. The target is not small or medium enterprises, because of their lack of risk management practices. An important point to take into account is the selection of enterprises with differences in IT team size, to evaluate if the

practices differ significantly. Selection of case studies in different industries is also a factor to take into account.

Each organization's structure is analyzed to see find sponsors of the research within that organization. A first formal contact is issued via email detailing the context and objectives of the research, along with its confidentiality and anonymity principles and asking for the opportunity to detail further the research in a face to face meeting. When the researcher knows someone at the target organization, he talks first with that person, to try that the email is replied. Unfortunately in Portugal some organizations opt by security through obscurity and do not see the opportunity to promote internal know-how with the research and are only concerned with the possibility of their security and risk management practices being put at stake. Other organizations responded to the formal email by saying that they were waiting for approval from the legal or human resources department or even from the CEO of the company to conduct the research. Unfortunately that sort of formal approval is never given due to the reasons explained before.

3.3.4 Unit of analysis

The unit of analysis reflects the core of the research and relates directly with the research questions (Yin, 2003). In this case the unit of analysis spreads across multiple parts. This research focuses in three units of analysis within the main themes of cyber risk management and information security investment benefits:

- The individual is one unit of analysis, as in this research value focused thinking is centered in the decision context of security investments to respond to a risk mitigation strategy. This decision is taken normally by an individual within an organizational context. This follows the suggestion from Langley et al. (1995), not to focus on the decision as a unit of analysis, but on the individual making the decision using a predefined process. This research details the values and objectives towards risk management of multiple information security specialists and IT professionals.

- Planning a strategy for cyber risk management will take as unit of analysis an organization within a case study to evaluate priorities among risk management objectives.

- Benefits management takes as unit of analysis an organization within a case study to evaluate, if they maximize the benefits after an security investment decision takes place. It aims to

discover if the initial drivers that were the basis of the investment are realized as benefits for the organization in the project implementation.

The literature review was not focused specifically in one type of approach, but it gathered all relevant literature on value focused thinking and benefits management from a starting theoretical framework. The interrelated themes of risk management and security investments were the main part of the literature review.

A industry focused unit of analysis will not take place, although the selected case study takes part in a public organization, detailing the context of the public administration in Portugal.

3.3.5 Data collection method

The risk management values are documented by the researcher in a datasheet after qualitative analysis of interviews. The initial approach is exploratory and risk management values are gathered in interviews. Multiple interviews take place in different organizational contexts to professionals in the IT, risk management and information security fields, where the interviewees discuss and justify their chosen risk management values. The basis for the development of a cyber risk management strategy based on the collected objectives and the analysis of business benefits from security investments is also gathered with interviews from key members from the chosen organization under case study.

Guides were developed to direct the interviews, but the researcher believes that the most important information is gathered when the respondent divagates about its organizational examples and daily tasks, so the guide is not to be strictly followed. If a new topic of interest is found that is not present in the guide, it will be used in subsequent interviews. Each interview starts with the researcher explaining the topic and the main objectives of the research and informing the interviewee about the anonymity and confidentiality principles. The interview continues by giving the respondent the chance to explain his main responsibilities and daily tasks, along with his main past projects and lessons learned, this allows the interviewee to relax. Interviews are recorded in a digital media, but when the researcher notices some constraint in the response about a subject the recording will be turned off. The interviewing strategy focuses first in interviewing positions that have management responsibilities. The researcher also asks to the respondent within each interview, which are the key roles that he thinks that will bring added value to the research, in order to see further targets to be interviewed beyond the organizational hierarchical position diagram. Interview duration is

initially scheduled for one hour for each respondent, but the duration is very volatile taking into account, if the researcher notices that the respondent brings added value to the research or not. The researcher adopts a flexible and available attitude towards the respondents in the sense that is better to postpone an interview if the respondent has limited availability that to have the interviewee respond to questions quickly and under pressure due to other tasks. The researcher adopts the posture of the outside researcher (Walsham, 1995b), in order to let the interviewee reveal his internal values and opinions about each discussed subject, which is most of the times exemplified with organizational situations, without having to be constrained with hierarchical pressure or disapproval. Taking into account that this posture might give the sense to the interviewee that the researcher has no own opinion or is not interested in organizational examples, the researcher adopts a proactive attitude that asks the respondent to corroborate his opinion with daily examples and supports the conversation by referring existing best practices and frameworks.

Workshops are conducted to foment the discussion of previously gathered values in the form of objectives. An initial presentation of the study is performed by the researcher and definitions of main concepts for alignment of the group will be provided. In the workshops participants weigh cyber risk management objectives across real world scenarios and discuss the results with the researcher and among themselves.

Documents are reviewed in full by the researcher if possible in digital format, but when it is not possible to retain the document, the researcher takes notes about the documentation. Public documents and information available on the Internet are also reviewed. Documents are descriptive or informative in nature and are best analyzed taking into account the context in which they were created.

Note taking takes place in every situation: during workshops, during individual interviews, during the researcher's internal review and also during field observation. These notes corroborate recorded data and retrieved documentation. Note taking also records the overall mood and physical reactions or body language observed to questions that the respondent is excited about, is angry about or is extremely careful in the response.

Field direct observation not only registers the daily business of the case study, but also notices emergencies and the person's attitude towards problems that deviate from the daily tasks, that might indicate change resistance. Direct observation also is a source of easily noticing conflicts in the daily organizational context and identifying the skills of the employee when he deals with a problem.

Triangulation is achieved by interviewing people in different sectors and different hierarchical positions which give the research multiple views about the same topic, some influenced by the real context that the organization faces and taking into account the objectives of each respondent in the organizational hierarchy. Triangulation is also achieved by corroborating the interviews with collected documentation. An interview database to manage the high volume of data is created by the researcher and the chain of evidence is maintained with rigor, detailing every aspect and schedule of each iteration.

3.3.6 Data analysis method

The data analysis method of the risk management values takes as a basis the value focused thinking (VFT) by Keeney (1992). Risk management values will be compiled using a spreadsheet in the raw value form as gathered by the researcher. Raw values will be transformed into objectives and they will be clustered based on their similarity. A WITI test will be performed and objectives will be divided into fundamental and means objectives.

Interviews will be transcribed into a qualitative data analysis software. The transcription of the recorded interviews allows the researcher to enhance the deep knowledge about the message transmitted in each interview and with that understanding it becomes easier to find and analyze the data. Miles and Huberman (1994) iterative model for qualitative data analysis will be followed as the basis for this research. The first stage known as data reduction entails the simplification of collected data. In this research data will be collected from different sources and using different methods, so some of the data is redundant and other is not important to the research problem at hand. Focusing in specific data is critical in this stage, although not always directly this stage reoccurs during the whole research process, as the researcher decides what is important to the research. Writing summaries, memos and dividing into clusters or partitions are tasks related to this phase. Data display is the next phase which is characterized by adequately displaying the organized and compressed data that permits conclusions to be drawn. Types of data displays are charts, graphs and matrices. The last phase is conclusion drawing and verification and this phase deals with making sense of the collected data and verify if the conclusions remain stable as further data is collected and analyzed.

3.4 Discussion

The expected results of this research will be the uncover of hidden cyber risk management objectives that are not thought on a day to day basis. These objectives will simplify the decision process of security managers turning a problematic decision based on existing alternatives into an opportunity that resembles a multiple win-win situation. With new objectives and their clear prioritization, new alternatives will be enunciated and these alternatives will be better supported by stakeholders than the existing ones (Barrese and Scordis, 2003).

The creation of a decision model based on those objectives, with the input from subject matter experts, will help organizations in the evaluation of alternatives during the decision making process. By using this model, the decision maker is able to choose and justify the investment with the values gathered from stakeholders in a adequate time frame to be able to respond to time to market pressures. This constant competitiveness urges decision makers to decide as soon as possible and decision makers may decide with incomplete basis for justification to agilize the process. It is expected that the results from different workshops, even with participants with different knowledge, will show a common path to develop the decision model. When that path is not common, the discussion will bring forward the differences in opinion.

The creation of cyber risk management principles will help organizations in the development of their cyber security strategy in a complex world where threats continue to rise. These principles establish a guideline for starting the creation of the strategy with common reference domains that organizations case about in the cyber risk management field. These principles will be formed taking into account the development of a cyber risk management strategy within an analyzed case study.

Benefits management closes the security investment lifecycle gap by enabling the close management of the risk mitigation investment and by assuring the necessary organizational changes, after the decision is made to maximize the realization of the benefits for the organization and its stakeholders. It is expected that the analyzed organization, with the adequate cyber risk management strategy, is able to use the cyber risk management objectives to guide their security investments and realize the identified benefits that were the basis for the approved decision. It is also expected that other hidden business benefits, that were not identified initially, will be discovered throughout the process, as the changes become internalized by employees.

The integration of the value focused thinking and benefits management theory is expected to complement each other, being the value focused thinking centered in the decision making process

based on objectives from stakeholders, and the benefits management focused on the realization of business benefits resulting from the security investments to mitigate risk. As risk management drives security investments, these two theories provide a direct match to integrate the full cycle from the decision to the realization of benefits during implementation.

Yin (2003) discusses 4 key criteria factors to evaluate the quality of a research design: construct validity, internal validity, external validity and reliability. Construct validity is ensured by collecting evidence from different sources and in different formats, while preserving the chain of evidence. Internal validity is achieved in a specific context by recognizing patterns. These patterns emerge from the collection of risk values to form objectives, through the discussion of scenarios based on risk objectives in the workshops, by evaluating those objectives to form a strategy and evaluate the benefits from security investments in a case study. External validity in this research does not apply to statistical generalisation, but to analytical generalization with the contribution to a theory. The findings are discussed in relation to existing theory to strengthen the research validity. Reliability is achieved by following the methodology from both theories, value focused thinking and benefits management, with rigour, while minimizing the researcher's biases and possible errors. If another researcher follows the same methodology with rigour, he will achieve similar results.

Discussing the research design using Klein and Myers (1999) principles, the principle of the hermeneutic circle is achieved by dividing complex situations into parts and their relationship analyzed later, after being confident with the analysis of each part. The principle of contextualization is taken into account in this research, as all data collection is performed within a described context and analyzed with a critical perspective using that context. The principle of interaction is difficult to ensure, as the research also interprets the gathered data, but the researcher adopts the outside researcher point of view by posing open questions that allow respondents to clarify their opinions based on past experiences and using triangulation mechanisms. The principle of abstraction and generalization is ensured with rigor in the research by capturing and analyzing information with as much granularity as possible within the theoretical framework, so that the conclusions may be able to be as much abstractable as possible to be generalizable to a similar context. The principle of dialogical reasoning is ensured in this research with an open mind limiting prior conceptions in the research design and accepting the differences in the actual findings. Multiple and different interpretations will be given by respondents to the same event and this helps the researcher in understanding the event from multiple perspectives and different behaviors. These different interpretations are also captured by interviewing respondents with more or less knowledge about the chosen theme,

namely risk management specialists, IT professionals or managers. The principle of suspicion is minimized with the researcher adopting a critical posture of all the information transmitted and by validating the information collected among multiple sources.

3.5 Conclusion

This chapter contextualizes the multiple generic philosophical perspectives available. The chapter describes the theoretical foundations of value focused thinking and benefits management, along with researches that use that approach in different contexts. It explains and discusses the research strategy. It details the foundation for case study research, how to select the case study, how to collect and analyze data.

Chapter 4

Risk management objectives

"Know your enemy and know yourself and you can fight a hundred battles without disaster."

—Sun Tzu, the Art of War

4.1 Introduction

Why are risk management objectives important nowadays in organizations? Risk management allows optimization and prioritization of safeguards to minimize information security risk to organizational critical assets. Risk can be mitigated until it reaches an acceptable level from top management based on their risk appetite. This perception of risk is what guides security investments, according to a defined security strategy that allows to protect business information (McFadzean et al., 2006). Is this perception of risk dependent from a single authority or part of a decision board with multiple stakeholders? Companies should embrace the objectives from multiple stakeholders in a risk management decision, as this step simplifies the acceptance of the decision in the first place (Barrese and Scordis, 2003). These risks should be monitored at the board level, as they can affect the current business dramatically and cannot be longer be treated with the delegation to operational risk control. Risk is the common language between business and the technical jargon of information security and the problem of lack of engagement of the board in such discussions will tend to be minimized in the future with the cyber risk based approach (Johnson et al., 2009; McFadzean et al., 2007).

This chapter uses the value-focused thinking approach from Keeney (1992) to develop objectives for risk management in organizations using values from multiple stakeholders. These objectives contribute to the achievement of the ultimate strategic objective: Minimize information security risk. This is a sensitive decision problem that all organizations face in their daily business.

4.2 Developing objectives

The initial list of values for cyber risk management were gathered by conducting semi structured interviews in Portugal with several security and IT professionals who represented a wide variety of job descriptions, such as the CIO, CISO or IT Manager, for example. The interviewees were representative of multiple business sectors, but were predominantly from consultancy, banking and the telecommunications industry. Should the information gathered require further explanation that was relevant for the research, we interviewed other employees from the same organization in order to clearly identify the context of the information collected. The interview was planned for 1 hour, the smallest was 28 minutes and the longest passed beyond 2 hours of productive discussion. The interview data gathering approach is adequate according to the value focused thinking methodology, as values should not be constrained and should be intrinsic from the individual. The interview process allows to discuss and define the problem under analysis and clarify the objectives of the interview. This allows to establish a common understanding of the concepts involved. It is also important to discuss face to face why the interviewee chose those values to gather and understand the context. The interview started with a general introduction to the value focused thinking methodology, focusing specifically on the guidelines for understanding and identifying values. Interviews were conducted within borders by using general targeted topics, broad categories and examples, but open questions were posed which allowed the respondents to reflect on their past decisions and enabled a review of their judgmental values. The values were collected as part of a wishlist in an ideal situation. The values were then analyzed to see their advantages and disadvantages in the interviewee's context to collect real professional examples and generating decision scenarios. These scenarios reflect the consequences of good and bad decisions and what was the impact of those decisions on the organization and on its employees. The examples allow to understand more clearly the values expressed by the interviewee. A total of 71 interviews were performed in the early part of 2014. Some interviews had more than one interviewee and were conducted as an iterative discussion. At a given point no more interviews were carried out because the total of

values that were collected from the last interviews were repetitions of previous values, so we thus opted for theoretical saturation.

The process started by enumerating all collected raw values into an unique document. These raw values are transformed into a common form, specially if they can be transformed into multiple objectives, to capture each objective individually. Some participants detailed the value as a wish, others as minimization of a problem and others already described the value in the form of an objective. There are many ways of wording the same raw value and that's why this common form is important. Duplicate values are merged and the number of times that each value is stated is preserved to capture the strength of that value across multiple respondents. Values are transformed into objectives and then the categorization phase takes place, by grouping similar objectives into clusters. These clusters with similar objectives are analyzed and an objective that represents the cluster's idea is discovered. This part of the process involves discussion with multiple specialists, most of them professors or experienced professionals in the field, to capture the essence of the data collected. Discussions were supported with qualitative analysis software and, if necessary to simplify the visualization of the objectives, these were printed into cards and arranged into groups. These final objectives are divided into fundamental and means objectives by taking the WITI test. This classification is critical for making informed decisions, although it is a subjective and interpretive process. Fundamental objectives are ultimately important and means objectives contribute to the achievement of another objective.

4.2.1 Respondent profile

The interviews were targeted at IT professionals or information security specialists. No interviews were performed outside of that scope, because we believe that the risk management values that influence information security are directly entailed within that two areas. Positions such as IT manager, chief information security officer, chief information officer, IT director, IT system administrator, IT network administrator, security consultant and risk manager are part of the interview data. This broad choice of professionals that were interviewed contribute to the study by stating risk management objectives in multiple areas: business, project management, IT technical operation, IT governance, information security operations, processes and governance. The respondent profile is divided among multiple sectors such as: IT consultancy, banking, insurance, service delivery, public sector, utilities and health. There are 71 respondents who have enumerated risk management values. All respondents are Portuguese citizens and are over age 18 and the oldest respondent

has 59 years. All the respondents have a minimum of 1 year of IT experience and the highest IT experience of a respondent is 30 years. The percentage of males in IT is high when compared with female respondents, weighting only 5% of the respondents.

4.2.2 Interview script

The interview script includes open questions that allow for the respondent to speak freely and express his opinion, providing also the context in the organization.

1. Are you familiar with the term Risk Management?
2. What does the concept of cyber risk management mean to you?
3. What do you value in cyber risk management? Develop a Wishlist. Give examples? Reliability and integrity of financial and operational information, Effectiveness and efficiency of operations, Safeguarding of assets, Compliance with laws, regulations, and contracts.
4. What is important in terms of risk to protect critical IT infrastructures? CIA?
5. Who is responsible for risk management in your organization?
6. What is wrong or right with cyber risk management in your organization? What needs fixing? What has occurred that was good or bad? Examples
7. How does risk management contribute to protect critical IT infrastructures?
8. 8. How do you manage risks in your organization?
9. How do you prioritize risks? How are risks treated?
10. Why are these values important to you?
11. What are the limitations regarding cyber risk management?
12. What risks can be accepted by management?

Raw Objective	Cluster
Encourage criminal records review Encourage non disclosure agreements Promote security clearance measures	Maximize vetting of employees for cyber risks
Maximize compliance with risk standards Ensure compliance with security policies Maximize legal compliance Ensure copyright management	Maximize compliance

Table 4.1: Clustering of objectives

4.3 Data analysis

The data analysis was performed using computer spreadsheets and qualitative analysis software. The researcher reviewed the recordings and collected documents to corroborate the enunciated values. A total of 612 cyber risk management values were collected, and after the removal of duplicates, a total of 414 values were identified. These values were enlisted in a common form and followed the methodology of obtaining a wishlist from the interviewees. Some examples of this wishlist are: ”I wish we maximize top management involvement” or ”I wish there is task delegation and clear responsibility”.

The values in a common form were then transformed into 114 distinct sub-objectives, and any duplicates were removed, which resulted in the same goal in different words, following a correlation and consolidation procedure. This transformation into sub-objectives is accomplished by applying an active verb which turns an objective into an effective action. Examples of duplicated sub-objectives were: ”Maximize information confidentiality”, ”Maximize information integrity” and ”Maximize information availability”. The CIA Triad is present in every information security content, so it’s normal that multiple respondents pointed out these objectives in cyber risk management discussions. The objectives were then sorted into 23 clusters, taking into account a shared common theme or idea.

As an example objectives of a cluster were: ”Encourage criminal records review”, ”Encourage non disclosure agreements” and ”Promote security clearance measures” were grouped together to form the objective: ”Maximize vetting of employees for cyber risks”. Another example of objective clustering was: ”Maximize compliance with risk standards”, ”Ensure compliance with security policies”, ”Maximize legal compliance”, ”Ensure copyright management”. These objectives were clustered into the single objective of ”maximize compliance”. These examples are detailed in Table 4.1. These clusters were highlighted and filtered with colors to facilitate data treatment inside the spreadsheet and ease the visualization for discussion among experts.

These 23 clustered objectives were further classified into means and fundamental objectives, by using the "why is this important" (WITI) test. This structured procedure is important for enabling reflection as to what individuals care about in a cyber risk context, and for seeing how these objectives relate in terms of importance. The fundamental objectives are the core values for the decision context and the means objectives enable those core values. For example the means objective ”Reduce human negligence” will influence the fundamental objective ”Maximize the protection of human life”. Means objectives can also have dependent relationships, for example: ”Develop a training program for cyber risk management” will contribute to ”Develop cyber risk management competencies” which will influence the fundamental objective ”Maximize cyber risk knowledge”. The WITI test resulted in a total of 6 fundamental objectives and 17 means objectives. This analysis was done visually in a blackboard by placing the objectives and drawing their dependencies to form the fundamental-means objective network. The initial network was then drawn in a computer software and multiple changes were performed to the initial version following discussions with professors and experienced professionals in the field for validation.

4.4 Results

To accomplish the main objective of minimizing cyber risks, 6 fundamental objectives and 17 means objectives resulted from the analysis. The relation of those objectives is detailed in a fundamental-means network as it can be observed in Figure 4.1. The following 2 subsections discuss the fundamental and means objectives by relating them to the literature and presenting real world examples from the interviewees.

4.4.1 Fundamental objectives

This section discusses each of the 6 cyber risk management fundamental objectives, taking into account existing best practices and by detailing the context in which they were structured.

Ensure risk management governance includes the adoption of IT and security best practices. Adequate risk management governance entails the nomination of a risk committee, which has the role of discussing risk at top management level and which consults all relevant stakeholders (Westby and Allen, 2007). It ensures the alignment of the risk management function within the organization to match the business objectives. This alignment of business objectives and risk management

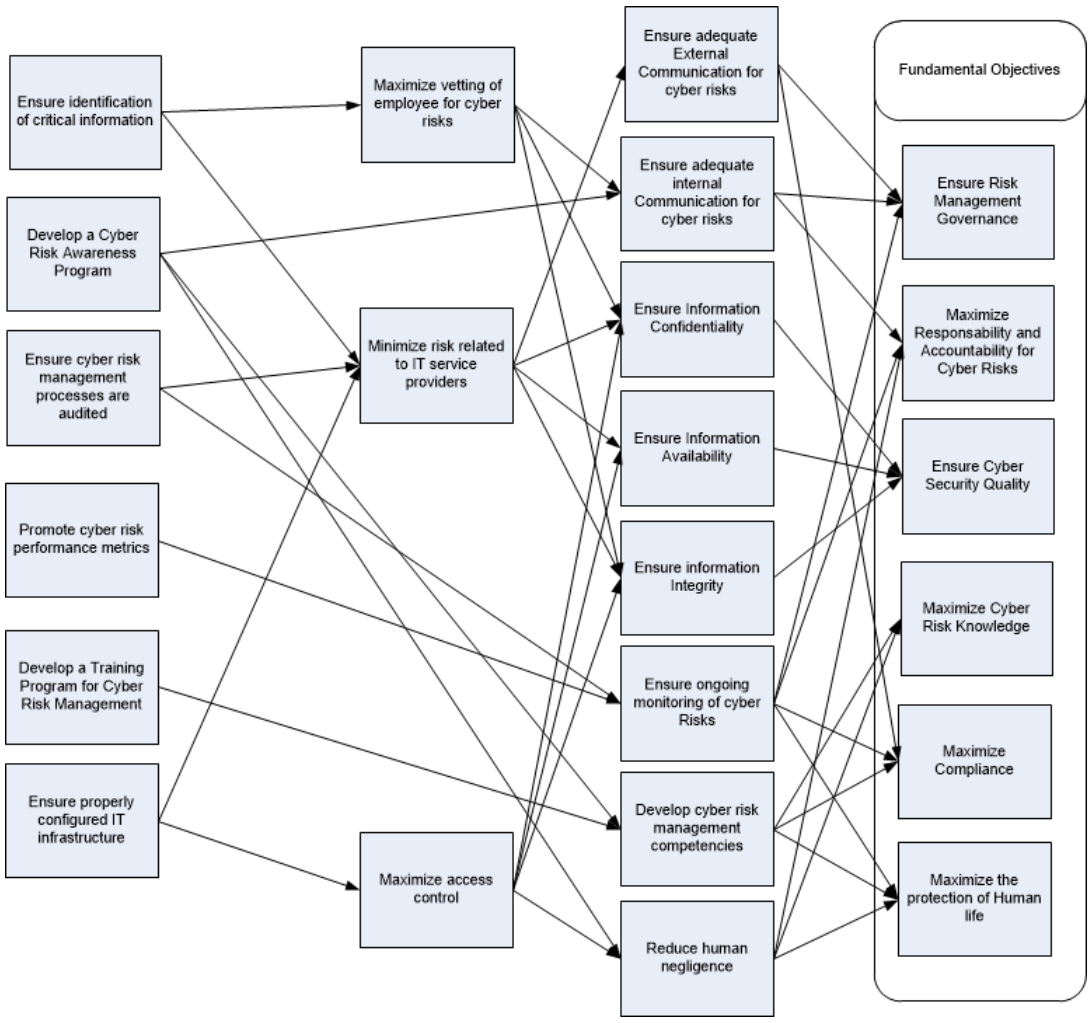

Figure 4.1: Fundamental-means objectives network

practices is seen as a critical step in risk management (ISACA, 2007), following the consolidated approach of strategic alignment between business and IT (Henderson and Venkatraman, 1993). It establishes the virtual structural basis that guides everyday's activity with responsibility boundaries and adequate path of action. It allows to integrate cyber risk management into corporate governance responsibility and place that topic into the top management's agenda(Posthumus and Von Solms, 2004). Consolidated risk management practices cannot be restrained to be controlled only inside the IT department or within a department dedicated to information security, these practices have to be raised to top management level, integrated within enterprise risk management (ERM) (Chatzipoulidis et al., 2010; Fakhri et al., 2015; Fitzgerald, 1995; Tiganoaia, 2012). The governance framework allows for cyber risks to be included as a major slice inside operational risk management or in an autonomous category and have the adequate attention by top management.

A CISO explained: *"After forming the committee, cyber risks started to reach the management board."*

Maximize responsibility and accountability for cyber risks deals with who does what, and who is ultimately responsible for risk mitigation measures (Lichtenstein, 1996). Most of the time, the person who is responsible for executing tasks is responsible for a specific delegated task, and the data owner is the person who is accountable for either accepting the risk, or deciding whether to implement additional safeguards (Purdy, 2010). These data owners should be clearly identified in cyber risk management and, together with their responsibilities in the risk management process, their role should be clear and objective. This identification and definition process prevents finger-pointing across the organization when a risk turns into a real situation. The responsibility and accountability is also enforced legally by binding security and risk management policies to the employee's contract. Otherwise it may be difficult to take action against employee's that violate defined mandatory policies. If employees perceive they are likely to get caught when violating policies, they tend to follow defined policies with more due care (Herath and Rao, 2009). The policies should delineate responsibility and accountability clearly, define to whom they are applicable and consider how specific enumerated exceptions are viable (Palmer et al., 2001). The policies detail what is expected of each employee when dealing with organizational information resources and a user declaration of acknowledge should be signed before having access to information and that signature renewed on an annual basis to reinforce the accountability (Höne and Eloff, 2002). An IT manager noted: *"I wish that accountability in security becomes a reality".*

Maximize cyber risk knowledge entails the creation of an intangible capability as a risk management organizational culture, in which each stakeholder is aware of existing cyber risks and the controlling management practices. This organizational culture based on shared values of risk management will automatically direct and unify accepted activities, while limiting the success of individual deviating behaviour by some employees who prefer to follow their non-acceptable ideas and preferences (Furnell and Thomson, 2009; McFadzean et al., 2006). Knowledge sharing is an effective way of promoting employee involvement in cyber risk management (Furnell et al., 2007; Safa et al., 2016). Focusing on empowering employees rather that seeing risk management as a tool augments the flow of risk information within the organization (Thapa and Harnesk, 2014; Veiga and Eloff, 2007). The empowered employee puts his personal knowledge or intimate understanding into the nurturing organizational culture (Mintzberg, 1988). Adequate testing of procedures and know-how should be performed in order to ensure that every employee is informed about the cyber

risk culture and knows what their role is in the risk management framework (Veiga and Eloff, 2010). People are considered always the weakest link in information security, being presented as the low hanging fruit waiting for the attacker to collect (Furnell and Clarke, 2012; Reid and Niekerk, 2014). Promoting the cyber risk knowledge within the information society by governments and extending that knowledge to specific requirements of organizations helps to strengthen that weakest link (Furnell, 2008). The active participation of employees, in a collaborative approach, to form that risk management culture is critical to achieve adequate results (Karabacak and Ozkan, 2010; Spears and Barki, 2010). An IT director explained: *"Building a risk management culture takes time and results are not always visible".*

Maximize compliance deals with ensuring that requirements from supervisory entities are met and the current regulations are followed. This objective impacts on an organization's business directly, as sanctions are applied for lack of compliance and, in extreme cases, this may lead to the legal prosecution of management. An organization has to adopt those proven methodologies, frameworks and best practices that guarantee the maximization of compliance. Risk management has defined standards and best practices which should be adapted for cyber risk management in the context of every organization. The documentation of clear cyber risk policies and procedures, together with the definition of internal sanctions for their non-compliance, should be an initial step in establishing the risk management framework. These policies should be written with adequate care, taking into account multiple principles adapted to the current context and requirements of the business and not follow the common copy and paste from templates from other organizations or consultancy services (Höne and Eloff, 2002). Legal compliance issues should also be accounted for, such as, for example, data retention time frames, which differ for each country. Copyright management is also a compliance requirement which affects not only the software acquired by an organization, but also, for example, a cyber attack with the intention of implanting illegal software. Several mandatory standards that impact organizations, like for example SOX, Basel or Solvency, have specific requirements for ensuring information security risk management as part of minimizing the operational risk (ISACA, 2014; ITGI, 2007). PCI-DSS is another mandatory standard that affects payments with credit cards, having specific security requirements to protect cardholder information (DSS, 2016). A CISO explained: *"Compliance in the banking sector is critical to the business and we must assure that internet payments security is compliant with the requirements from the European Bank Authority".*

Maximize the protection of human life may seem an outside objective at first glance when deal-

ing with cyber risks. However this objective makes complete sense, after careful examination, and when considered for example within the mindset of those cyber risks which affect critical infrastructures that may harm human life. Critical infrastructures are being attacked daily with advanced persistent threats (APT), with the goal of compromising their infrastructures, examples being energy companies and water management, for example. A real example was when a computer worm named stuxnet was created to attack nuclear power plants (Farwell and Rohozinski, 2011). These cyber risks should be carefully managed as most critical infrastructures, although not directly connected to the Internet, are indirectly exposed to attacks and loss of human life may occur. When reflecting about cyber warfare, wars happen first in the cybersphere before a physical attack occurs (Baskerville and Portougal, 2003). It is easier to attack a country that is rendered blind, through the lack of communications or power, for example. Recently, efforts are being secretly pursued by countries to enhance their cyber competitive intelligence. At the individual level with the Internet of Things phenomenon, those risks will affect the common citizen in their houses, in their jobs and directly in their life with the adoption of e-health devices for example. Cyberstalking and cyberbullying are also phenomenons that migrated from the physical into the cyber domain with the rise of the social networks and the digital footprint of every individual (Dhillon et al., 2016a; Von Solms and Van Niekerk, 2013). A security consultant divagated on that topic: *"We security professionals live in constant fear that technology will bring harm to someone sooner or later"*.

Maintaining data privacy is also a critical factor for maximizing the protection of human life, by contributing to maintain freedom as an individual has the right to choose what private information is communicated to to which entity (Son and Kim, 2008). As our day to day life increases in the digital world with different means of access beyond the traditional computer, the emergence of information contribution to social networks, wiki or other web 2.0 platforms, so grows the risk to privacy. It is known that when information reaches the web, it never leaves it again. Trying to delete information that reaches the web by accident is a quest of endless loops, as that information may be copied easily before removal from a specific service. The rise of big data, with the capacity of computers to process enormous quantities of data, also increased privacy concerns, with previously impossible relations about entities and their online behavior being profiled in seconds. Geo location tracking is also simplified with the use of devices with GPS or other geolocation mechanisms. RFID and NFC mechanisms also contribute for location tracking (Madlmayr et al., 2008; Pramatari and Theotokis, 2009). The emergence of smart toys also raise questions about the risks posed to small children, not only from the security point of view, but also targeting privacy rights (Dobbins, 2015). An IT

administrator noted: *"Privacy requirements in the EU are different from the US".*

Ensure cyber security quality objective aggregates security concepts, including explicitly the information confidentiality, integrity and availability triad. Examples of some of the fundamental concepts for assuring security quality are: information authenticity, reliability and non-repudiation (Alcalde et al., 2009). The ability to counteract aggressive actions can be ensured by robust authentication, complemented with strong auditing mechanisms and an adequate identity management of multiple stakeholders across multiple platforms, and also by using applications with strong access controls. A CISO noted: *"My job is to ensure the security of our critical assets".*

4.4.2 Means objectives

This section presents the 17 means objectives and details the context for the formation of each distinct theme among the sub-objectives.

Ensure properly configured IT infrastructure to protect against attacks which exploit vulnerabilities in unpatched systems. A lack of system hardening procedures that do not remove unnecessary services and remove default credentials is another risk that has to be accounted for. The security of legacy systems with discontinued support from the vendor should not be disregarded. A fundamental principle for the safeguarding of information availability is the adoption of solutions that ensure high availability in the case of failure. Contributions towards ensuring an adequate infrastructure architecture plan include developing a strategy for promoting interoperability across platforms and choosing a solution which minimizes technological dispersion in the technological environment. The rise of the shadow IT concept, where organizational applications bypass local IT department administration, and are contracted as a service directly by non IT departments is a growing risk in organizations (Fürstenau and Rothe, 2014; Silic and Back, 2014). Is the IT infrastructure where that application runs properly configured? Most of the times the IT department has no information that some departments use shadow applications and does not reserve the right to audit that infrastructure (Paquette et al., 2010). An IT administrator explained: *"We have a configuration database of our infrastructure, but the information stored there is most of the times outdated".*

Ensure ongoing monitoring of cyber risks to comply with best practices for continuous improvement. Risk frameworks and standards such as, for example, ISO 31000 (ISO, 2009), follow continuous improvement methods within the classic cycle of 'Plan, Do, Check, Act', (Johnson, 2002) and contribute to an ongoing monitoring of cyber risks, as they evaluate the current risk level, deploy

risk mitigation measures or accept the resilient risks and also reevaluate whether the risk exposure remains the same after organizational changes. A CISO explained:*"We do follow-up of security measures to evaluate if the risk was minimized or not."*

Promote cyber risk performance metrics is the best way to carry out quantitative evaluation if the cyber risk mitigation objectives are being met, depending on how much is completed during execution. This obliges the implementation of an adequate systems' logging level, as a means of extracting meaningful information. This measurement allows for the planning of changes when they are needed, according to the plan, as part of the ongoing process of enabling the delivery of benefits (Bodin et al., 2005; Gordon and Loeb, 2002a; Slayton, 2015). Key performance indicators (KPIs) allow management to follow the initiatives that have been implemented to improve the current risk level. Dashboards are also used which periodically analyze current metrics and identify deviations, which permits timely decisions to be made, which put an organization's risk management back on track. A good metric is clear and objective and the data collection occurs automatically to minimize errors. The creation of metrics follow a defined process starting with scope definition and ending with the testing of the designed metric following the pragmatic principle for example (Brotby, 2009; Brotby and Hinson, 2013). An IT administrator noted:*"I'm tired of collecting metrics that are never used."*

Ensure cyber risk management processes are audited to have an independent vision to check whether risk management is being applied with adequate due care (Straub and Welke, 1998). It is always important to have another opinion regarding a critical business process and risk management is no exception, as an internal or external audit will inevitably point out recommendations for improvement (ISACA, 2007; ISO, 2011). In the case of an internal audit department they may propose controls to strengthen the risk management processes, ensuring for example separation of duties (Saltzer and Schroeder, 1975). They discover and alert management to common anomalies within defined processes. In the case of an external audit, a specialist auditor will be able to benchmark current cyber risk management practices against those that are being practiced by similar organizations, and thus guarantee the adoption of the current risk management benchmark. This objective leads to the implementation of an adequate process testing framework which is able to produce tangible evidence for the auditors.

Software code auditing review tests and penetration tests should also be performed to discover hidden risks. One IT Director who was interviewed noted:*"Recently we started to audit web applications before they go online and noticed a decrease in existing common vulnerabilities, as the*

development department started to employ secure coding practices".

Minimize cyber risks related to IT service providers is an important objective, as organizations tend to outsource some of their IT processes and information is now moving on to the cloud (Pereira et al., 2012). The alignment of objectives between providers and clients is critical to the success of these partnerships, as security objectives tend to be positioned in different priorities by the client and the IT service provider (Dhillon et al., 2016b). A simple mistake caused by the IT provider can trigger multiple business losses across multiple clients (Salmela, 2008). Conflicts of interest, for example by selling and then managing security solutions or implementing and then auditing solutions should be minimized. Information and IT knowledge lock-in risks should be safeguarded in service level agreements. This lock-in technically occurs when the vendor does not adopt appropriate technological standards for migrating information to a different provider, or when the vendor goes bankrupt and shuts down their services. This lock-in can also happen when an organization loses core technological competencies and becomes hostage to the provider, who knows everything on that specific subject about the organization and refuses to document or pass on that knowledge to the organizations' internal resources. Legal requirements also need to be safeguarded, taking into account where the information is physically stored when using cloud services, and what the applicable law is of that country. The maintenance of intellectual property rights have to be ensured in contracts and with adequate monitoring. The security chain is as strong as the weakest link, so it's necessary that IT service providers maintain at least the same security level as required by their clients (Johnson et al., 2009). The access to critical information should be limited in the case of outsourcers, and non-disclosure agreements should be signed to prevent disclosure. Temporary credentials should be issued and these have to be renewed if the outsourcer still needs access after their contractual period ends.

As an interviewed IT manager pointed out: *"We found out recently after a system migration several active credentials belonging to outsourcers that had several years without login attempts"*.

Maximize access control protects information from unauthorized access. Access control plays a critical role in the validation of authentication, authorization and accounting. The principle of segregation of duties should be enforced to prevent a single entity from having full access to a critical process. Critical processes should include an authorization phase, which is carried out by another entity, rather than the one that is responsible for its execution (Saltzer and Schroeder, 1975). Access control allows for the maximization of access segmentation, following the network defense in depth security principle (Lippmann et al., 2006). Password management policies should be en-

forced to maximize access control, using multi factor authentication when available, and obliging the use of complex passwords that must be periodically renewed. Multi factor authentication is used when 2 or more factors are used for accessing a resource. Examples of such factors are: some that you know for example a password or a PIN, something that you have for example a smartcard or one time token and something that you are focusing in biometry (Jonvik et al., 2008). Other factor are something that you do with examples keystroke dynamics or form of writing and something that identifies where you are accessing from: GPS or type of device. Minimum privilege should be the default option for access control, giving users only the allowed access to fulfill their daily tasks (Saltzer and Schroeder, 1975). An IT administrator noted: *"We use 2 factor authentication in all external accesses to our infrastructure."*

Reduce human negligence attempts to minimize human errors that occur due to a lack of awareness, or simply because human nature is negligent. Negligence applies to the failure of establishing the adequate due care of a prudent person to protect information from risks that may harm others (Von Solms and von Solms, 2006). Human error is often underestimated as a business risk (Im and Baskerville, 2005). A business impact analysis should be carried out to evaluate the impact of negligence or malicious conduct regarding information (Whitman et al., 2013). Only after this analysis has been completed, is it possible to evaluate and quantify what is critical to the business and to then implement adequate written procedures that explain the critical task step by step, thus minimizing human negligence. The use of applicational controls that immediately detect human errors along with the monitoring of anomalies to detect errors afterward (ISACA, 2014).

Maximize vetting of employees for cyber risks can be ensured by adopting best practices for hiring human resources. Employees should be subjected to criminal records checks. Security clearance practices that take into account the criticality of information should be mandatory implemented. Non disclosure agreements for internal employees and external consultants should also be enforced when dealing with critical information. The ethical behavior of internal employees should be mandatory to minimize the risk of internal breaches in security, as employees have additional privileges to sensitive information (Dhillon, 2001). An IT security administrator referred: *"I have never been asked to present my criminal records during the hiring process and I have worked in multiple companies before this one."*

Ensure adequate internal communication regarding cyber risks across all the stakeholders and promote internal meetings to ensure that the correct communication paths are created and maximized. A formal risk communication policy should exist in the organization that encourages

employees to discuss and report risks. Being aware of existing risks due to internal communication solidifies the responsibility of every employee. Data owners should communicate the criticality of information to custodians (Krause et al., 2002; Peltier, 2013). Maximizing the involvement of all stakeholders enables the clear definition of accepted risk levels. When adequate internal communication regarding cyber risks is established, it minimizes user panic when a risk situation becomes real. Lack of organizational communication increases gray areas of responsibility, leaving risks without treatment as some important risks remain unknown to top management. Risk reporting should not be viewed as a witch hunt, but their communication be promoted among open defined communication paths. Open organizational communication helps to form a risk management culture (Baskerville, 1991).

As one IT administrator explained: *"new applications appear everyday to be installed in the production servers, there is no communication from the IT development department that new applications are being developed and what are their requirements"*.

Ensure adequate external communication regarding cyber risks to minimize the loss of reputation due to cyber risks. A spokesperson needs be clearly identified and briefed for handling crises, such as data breaches, for example (Valackiene, 2015). This spokesperson has to have the clear objective of minimizing media pressure in cyber risk management, and also acts as a facilitator for minimizing the effect of political decisions that affect cyber risk management. This was demonstrated by an IT director who stated that: *"our risk management priorities change from one day to the other with political decisions that change our entire strategy"*.

Ensure identification of critical information deals with the definition and identification of the critical information within business processes and ensures the evaluation of critical information and defined service criticality levels. This definition allows for the centering of safeguards in critical information, as budgets are invariably limited. A data classification program should be established with a clear definition of who are the information owners and custodians, together with defined data criticality levels (Johnson et al., 2009; Krause et al., 2002). Information systems can only guarantee the application of controls taking into account the defined information classification level. An information or data classification policy has to define the criteria for placing information across a number of defined classification levels and what are the minimum controls to be applied to physical or digital information that has that level (Appleyard, 2005; Peltier, 2013). The policy should include also the responsibilities for employees that deal with information of that level. The information classification process should follow the information across the full lifecycle, being applied when

the information is created, traveling with the information across multiple levels in time, because information may be critical today, but public or useless tomorrow and finally monitoring, if necessary, the information destruction. This prioritization of information results in the maximization of the efficiency of the incident response team, when critical operations are affected by system failures, asset compromises or data breaches.

As a security manager explained: *"I need to know what information is critical to the organization to direct my security investments accordingly"*.

Ensure information confidentiality to prevent sensitive information being leaked to an unauthorized entity. Intellectual property protection is of great concern to organizations (Johnson et al., 2009). This can be ensured by adopting adequate encryption measures when dealing with stored information, by encrypting laptops' hard drives or critical databases. Information transmitted can use secure network protocols, that ensure that the data is encrypted. Data leak protection (DLP) mechanisms can be implemented to prevent leakage by disgruntled employees or external consultants. Implementing an information classification program is also a crucial step for defining information's value and for protecting printed documents (Peltier, 2013).

One interviewed IT security administrator noted: *"I simply don't understand what is the difficulty nowadays in enabling encrypted communication protocols such as SSH or SSL".*

Ensure information availability when access to information is required by an entity. The risk of loss of information needs to be minimized, and adequate backup procedures and data recovery methods should be tested periodically. The transportation of backup information offsite should be evaluated in order to protect against disaster. Business continuity and disaster recovery best practices should be adopted by the organization, which should include the definition of recovery times and point objectives (Whitman et al., 2013). The presence of high availability mechanisms in the infrastructure that supports critical processes is an added protection measure against failures, and protects against denial of service attacks. An IT administrator noted: *"We have an alternative datacenter in the north of the country, that assures business continuity and disaster recovery."*

Ensure information integrity by adopting good change management practices, that protect information from unauthorized modification (Joshi et al., 2001). Change management allows for the tracking of responsibilities and prevents unauthorized and unprepared changes (Cannon et al., 2007). Changes should be planned and a rollback plan should be available in case corruption of data occurs.

Develop cyber risk management competencies which allow employees to recognize cyber risks. The allocation of trained staff for cyber risk management should be ensured. These experts should not only be able to identify technical cyber risks, but must also be able to recognize risks that arise from poorly defined business processes. These competencies are build with formal education and training and with on the job experience (Blakley et al., 2001; Furnell and Thomson, 2009). These competencies can be a source of competitive advantage following a resource based view approach (Barney, 2001; Bharadwaj, 2000; Wade and Hulland, 2004; Wernerfelt, 1995). Moreover, Peppard and Ward (2004) explain: ”an organization’s current capability, based on its existing competencies, will be either an enabler or inhibitor in terms of the goals it can actually achieve”.

Develop a cyber risk awareness program which permits employees to recognize typical cyber risk scenarios and to become alert to deviant behaviors (Drevin et al., 2006; Peltier, 2005; Siponen, 2001, 2000). Awareness contributes significantly to the formation of a conscious care behavior (Safa et al., 2015). People are always the weakest link in any risk management program, and the implementation of a consistent awareness program, which transmits and tests employees periodically about risk management best practices, is a vital key to success in risk mitigation. Awareness programs mitigate the unconscious incompetence of employees, as they are unaware of their responsibilities in information security and risk management (Thomson et al., 2006). An interviewed security consultant explained that: *"People have a natural way of bypassing or dropping control mechanisms, if they don’t recognize the added value. The purpose of control measures should be explained in awareness campaigns"*.

Develop a training program for cyber risk management that includes user cyber risk training and encourages users to become proficient in crisis management procedures. Such training goes beyond an awareness process and prescribes specific procedures that must be followed when dealing with cyber risks. Training moves the employee from a conscious incompetence stage, as he recognizes the skills gap, to a conscious competence stage, as he is able to deal with cyber risks. The continuous practice enables the employee to reach the unconscious competence stage, where he has absorbed the knowledge to fulfill his tasks (Thomson et al., 2006). This training approach increases the perceived usefulness and maximizes the perceived ease of use with the minimization of the learning curve sometimes associated with new technologies and change of processes (Davis, 1989). The need for a specialized license to practice for risk management professionals may also be a differentiation point in the future, as certifications in this area start to mature (Blakley et al., 2001). The certifications advise for a code of conduct that reinforce ethical and professional obligations

in due diligence. A security manager explained: *"Training is everything in our Security Operations Center, to be able to respond as quickly as possible in the prescribed way."*

4.5 Conclusion

This chapter details the use of value focused theory to develop fundamental and means objectives for cyber risk management. It details the methodology used to collect the initial values, transform them into objectives and divide them into different clusters. Clusters are submitted to the WITI test to separate fundamental and means objectives. Each of these objectives is related back to the literature and discussed taking into account the context of respondents. These objectives form the baseline for cyber risk management and are applied within different contexts in the next chapters.

Chapter 5

Cyber Risk Policy Decisions

"He who is prudent and lies in wait for an enemy who is not, will be victorious."

—Sun Tzu, the Art of War

5.1 Introduction

How can a manager take effective risk policy decisions while satisfying the stakeholders interests? This has been the million dollar answer for years in many domains such as environment or military for example. Examples of such complex decisions and proposed decision models in those domains are watershed improvements, nuclear waste disposal or prioritizing military actions (Brine, 2012; Brothers et al., 2009; Merkhofer and Keeney, 1987; Merrick et al., 2005b; Shoviak, 2001). With the growth of technology, a new domain posing new threats rises: the cyber domain. The cyber domain is able to affect the information security of organizations, governments, nations and consequently affect the common life of every individual. How does a policy decision, in that uncharted domain, receive the acceptability of employees, partners, media and costumers? Can that decision be stalled until we have all the necessary information to decide? What is the necessary information? Will it ever arrive? Top management is being pushed to take decisions as soon as possible, as the evolution flow of technology in the cyber domain never stops. Cases of companies going bankrupt due to lack of cyber risk policy decisions, that lead to cases of data breaches, as consequences of cyber attacks are not new (van der Meulen, 2013; Zetter, 2011). Cases of governments harming

other nations with the use of this domain are also not new (Czosseck et al., 2013; Rios et al., 2009). Howard (2007) argues that a good decision is a logical decision based on the uncertainties, values and preferences of the decision maker. The three elements of a decision are: what you can do by listing and evaluating alternatives, what you know, by analyzing the information available, and what you want, taking into account the preferences. Capturing the values from stakeholders becomes a critical step in risk policy decisions, as those values can be conflicting ones and might lead to a different perception of risk. This difference in the perception of risk will hamper security initiatives that mitigate risk, with policy non compliance behaviour evidenced by stakeholders (McFadzean et al., 2006). Wrapp (1984) argues that managers should not force policy decisions when the organization's employees do not understand the need for a policy in that area. A policy will evolve transparently from a set of operating decisions supported by the employees and agreed by stakeholders. This policy should be concise, clear, business driven, supported by top management and define the lines of authority on that subject (Palmer et al., 2001).

This chapter details the creation of multiple real life scenarios for cyber risk policy decision making, capturing respondents perceptions of risk objectives applied in those scenarios. Those objectives are weighted to form a decision model to minimize the cyber risk in organizations and governments, with adequate metrics to evaluate the necessary efforts.

5.2 Defining scenarios

Multiple studies, both from academic and professional sources, explain the importance of the creation of scenarios in risk management to clarify different points of view, to generate discussion, stimulate thinking and to evaluate the real impact of risks in practice (Alberts et al., 2005; Bistarelli et al., 2006; Harris, 2010; Ryan et al., 2012; Spears, 2005).

Using the fundamental risk objectives and their relation to the means objectives, we developed multiple scenarios of real world situations for risk decision makers (Keeney et al., 1990). We first started with the creation of the ideal utopical scenario where all the fundamental objectives were fully satisfied. On the other end there's the bad scenario where every fundamental objective is not obtained. What is the incremental step in each objective from the bad to the good scenario in a real world situation? This mindset is what lead us to the creation of 4 additional intermediate scenarios with significant difference in the application of each objective.

We discussed the scenarios with multiple professors and specialists in the field for validation and multiple evolutionary versions of the scenarios were created, before they were presented to participants in workshops. Following these discussions, there were changes in the means objectives that influence the fundamental objective ”Maximize the protection of human life” to clarify to participants some of the objectives that it included explicitly. We added explicitly ”maximize data privacy”, ”ensure the protection of critical infrastructures” and ”maximize the protection of medical devices” into the scenarios under the topic group for this fundamental objective. We took into account multiple factors for the creation of each scenario: the mandatory or discretionary option of the objective, the formality of the process, the consequence for not following the established process, the complexity or simplicity of the objective, the level of effort for achieving the objective and the scope in which the objective is applied. The scenarios mimic as close as possible different implementations of the chosen objectives in reality, taking into account the information collected from subject matter experts and revised literature about risk management.

The respondents were asked first to rank and weight, using the swing method, the fundamental objectives having the description of the fundamental objective and its means objectives. The next step is to read all the scenarios and rank and swing weight the 4 custom developed scenarios. The good and bad scenarios do not count for the exercise, the good is ranked 1 and has 100 swing weight and the bad is ranked 0 and has 0 swing weight. After having classified the scenarios, each objective is ranked and weighted using the swing method across all the 4 scenarios. There’s no constraint in the exercise for ranking a scenario better overall, but preferring some objectives in other under weighted scenarios. The final step is to rank and weight all fundamental objectives again after seeing the consequences of each objective across multiple scenarios. This last step allows to gather differences in perceptions before and after evaluating each scenario.

The good scenario seen in Table 5.1 is an utopical one, where the achievement of every objective is maximized. Consequences for achieving those objectives are always good, simple and accepted by all.

As it can be seen in Table 5.2, scenario A is characterized by formalization of processes, centralized or external auditing and mandatory policies. Severe consequences for not following policies or for non-compliance, such for example termination of contracts and fines, are also part of this scenario. Although some objectives can be maximized in this scenario, the consequences come with additional complexity of controls. Governance for risk management is seen as critical in this scenario, having established structures inside organizations. Risk knowledge is forced with man-

Fundamental objective	Good scenario
Ensure cyber risk management governance	-Flawless internal (organizational) communication of cyber risks -Flawless external (stakeholders) communication of cyber risks -Cyber risk committee gathers frequently to discuss cyber risks -Cyber risk management integrated with ERM.
Maximize responsibility and accountability for cyber risks	-All employees are vetted for cyber risks. -All IT service providers are responsible for cyber risks -All employees sign Non disclosure agreements (NDA). -All employees are bounded to the security policy -Every cyber risk has a designated owner.
Ensure cyber security quality	-Information Confidentiality is ensured. -Information Integrity is ensured. -Information Availability is ensured. -Adequate access control mechanisms are put in place. -IT infrastructure properly configured.
Maximize cyber risk knowledge	-Training Program for cyber risk management implemented -Employees are aware of cyber risks -Solid competencies in cyber risk management -Mature risk management culture
Maximize compliance	-Cyber risk performance metrics implemented and continuously improved. -Cyber risk management processes are periodically audited and improved. -Monitorization mechanisms of cyber risks implemented. -Requirements of supervisory entities clearly defined and enforced. -Legal requirements clearly defined and enforced. -Adequate adoption of standards and best practices. -Adequate copyright management procedures
Maximize the protection of human life	-Adequate Procedures to reduce human negligence -Adequate protection of critical infrastructures. -Adequate protection of medical devices. -Adequate Protection of data privacy.

Table 5.1: Good scenario

datory training and awareness. Compliance requirements are complex and enforced with fines by authorities. Controls to critical infrastructures and medical devices limit the flexibility of everyday's life.

Scenario B in Table 5.3 is characterized with the formal adoption of processes and control mechanisms. The consequences for non-compliance are not clear and may or may not result in severe actions. The responsibility for risks is starting to grow in critical areas. Complexity of controls is overwhelming and may limit the flexibility of business. Some risk management processes are not integrated in a global business perspective. Risk knowledge is promoted within the organization, but it's optional. Auditing mechanisms are starting to be established.

Scenario C in Table 5.4 has multiple opt-in measures where the entity can choose to comply or

Fundamental objective	Scenario A
Ensure cyber risk management governance	-Formal written internal communication of cyber risks. -Formal written external communication of cyber risks. -Formal periodical meetings of cyber risk committee exist. -Cyber risk management integrated with ERM.
Maximize responsibility and accountability for cyber risks	-All employees are vetted for cyber risks. -All IT service providers are responsible for cyber risks and fines are defined for non-compliance. -Information disclosure will lead to termination of employee contract. -Non-compliance with security policy will lead to termination of employee contract. -Every cyber risk has a designated owner.
Ensure cyber security quality	-Adequate controls to ensure information confidentiality. -Adequate controls to ensure information confidentiality. -Adequate controls to ensure information availability. -Formal access control mechanisms are put in place. -Known baselines are followed and audited for infrastructure configuration.
Maximize cyber risk knowledge	-Periodical training for cyber risk management is mandatory. -Awareness programs are mandatory. -Competencies in cyber risk management must exist and are verified centrally by authorities. -Risk management culture enforced with fines.
Maximize compliance	-The implementation and improvement of cyber risk performance metrics is mandatory. -Cyber risk management processes are centrally audited by authorities. -Monitorization of cyber risks is mandatory. -Requirements of supervisory entities are complex and enforced with fines. -Legal requirements are complex and enforced with fines. -Adoption of standards and best practices is mandatory. -Copyright management subject to continuous auditing and fines.
Maximize the protection of human life	-Human negligence will result in legal action. -Critical infrastructures independent from IT infrastructures. -No IT connectivity for medical devices. -Enforcement of data privacy enforced with fines.

Table 5.2: Custom scenario A

Fundamental objective	Scenario B
Ensure cyber risk management governance	-Informal communication of cyber risks internally with a defined process -Informal communication of cyber risks to external stakeholders with a defined process -Cyber risk committee gathers as needed to discuss urgent cyber risks. -Cyber risk management separated from ERM.
Maximize responsibility and accountability for cyber risks	-Some employees with defined critical functions are vetted for cyber risks. -All IT service providers are responsible for cyber risks but there's no financial compensation for losses. -Information disclosure may lead to termination of employee contract. -Non-compliance with security policy may lead to termination of employee contract. -Some critical cyber risks have designated individual owners.
Ensure cyber security quality	-Complex controls to ensure information confidentiality. -Complex controls to ensure information integrity. -Complex controls to ensure information availability. -Complex access control mechanisms and procedures are put in place. -Known baselines are followed for infrastructure configuration.
Maximize cyber risk knowledge	-Training for cyber risk management is optional.. -Awareness programs are optional. -Competencies in cyber risk management must exist. -Mature risk management culture created with rewarding mechanisms.
Maximize compliance	-Cyber risk performance metrics are defined but are optional to use. -Formal auditing procedures for cyber risks. -Monitorization of cyber risks is mandatory. -Requirements of supervisory entities are clearly defined and enforced with warnings. -Legal requirements are clearly defined and enforced with warnings. -Adoption of standards and best practices is optional.. -Copyright management procedures subjected to auditing.
Maximize the protection of human life	-Human negligence may result in legal action. -Critical infrastructures indirectly connected to IT infrastructures may malfunction and cause human harm. -Complex controlled IT connectivity to access medical devices. -Protection of Data privacy enforced by mandatory standards.

Table 5.3: Custom scenario B

Fundamental objective	Scenario C
Ensure cyber risk management governance	-Informal communication of cyber risks internally with a defined process. -Ad-hoc external Communication of cyber risks. -Cyber risk committee exists ad-hoc with no formal members. -Cyber risk management is leading the creation of ERM
Maximize responsibility and accountability for cyber risks	-Some employees with defined critical functions are vetted for cyber risks. -Some mature IT service providers are responsible for cyber risks but there's no financial compensation for losses. -There is a formal NDA. -There is a formal security policy. -Some critical cyber risks have designated group owners.
Ensure cyber security quality	-Basic technical controls to ensure information confidentiality -Basic technical controls to ensure information integrity -Complex technical controls to ensure information availability -Basic technical access control mechanisms implemented. -Known baselines may be followed for infrastructure configuration.
Maximize cyber risk knowledge	-Ad-hoc training program for cyber risk management -Awareness of cyber risks dependent on the individual. -Technical IT competencies in cyber risk management must exist. -Risk management culture is starting to grow.
Maximize compliance	-Ad-hoc cyber risk performance metrics. -Ad-hoc auditing procedures for cyber risks. -Formal monitorization of cyber risks. -Requirements of supervisory entities are clearly defined but not enforced. -Legal requirements are clearly defined but not enforced. -Ad-hoc adoption of standards and best practices. -Copyright management procedures implemented.
Maximize the protection of human life	-Seldom cases of human negligence are advised with warnings. -Critical infrastructures directly connected to IT infrastructures may malfunction and cause human harm. -Uncontrolled IT connectivity to access medical devices may cause human harm due to device malfunction. -Protection of data privacy guided by best practices.

Table 5.4: Custom scenario C

Fundamental objective	Scenario D
Ensure cyber risk management governance	-Ad-hoc internal Communication of cyber risks -No external communication of cyber risks -Cyber risk committee does not exist. -ERM does not exist.
Maximize responsibility and accountability for cyber risks	-Ad-hoc vetting of employees for cyber risks. -IT Service providers not responsible for cyber risks -NDA does not exist -There is no formal security policy. -Risks have no ownership.
Ensure cyber security quality	-Basic technical controls to ensure information confidentiality -Basic technical controls to ensure information integrity -Complex technical controls to ensure information availability -Basic technical access control mechanisms implemented. -IT Infrastructure configured ad-hoc.
Maximize cyber risk knowledge	-No training program for cyber risk Management -No awareness of cyber risks -Competencies in cyber risk management should exist. -Cyber risk management culture does not exist.
Maximize compliance	-No performance metrics in cyber risk management -No auditing procedures for cyber risks -Technical monitorization of cyber risks. -Ad-hoc requirements of compliance defined by supervisory entities. -Ad-hoc legal requirements defined. -No adoption of standards and best practices. -No copyright management procedures.
Maximize the protection of human life	-Frequent cases of human negligence cause harm to others -Critical infrastructures malfunction causes human harm. -Medical devices malfunction causes human harm due to IT problems. -Protection of personal data occurs ad-hoc.

Table 5.5: Custom scenario D

not. There are some ad-hoc processes and other defined processes that are not enforced by the organization. Consequences of non-compliance result in warnings and ownership stays in a gray area of responsibility, normally dependent from a department or group. Risk mitigation controls have a technical focus, normally staying inside the IT domain and not reaching all the organization. Knowledge of risks depends on every individual background and competence.

Table 5.5 details scenario D, where most of the processes of risk management are not defined and followed ad-hoc. Management recognizes the need to enhance risk management practices, but has other priorities. Risk management governance does not exist and all responsibility and accountability lacks formality. Consequences for non-compliance do not happen. Controls are technically focused and maintained at a basic level. Risk knowledge does not exist. Compliance is taking the first steps with requirements being defined ad-hoc. There are frequent cases where lack

Fundamental objective	Bad scenario
Ensure cyber risk management governance	-No internal communication of cyber risks -No external communication of cyber risks -Does not recognize the need for an cyber risk committee. -Does not recognize the need for an ERM.
Maximize responsibility and accountability for cyber risks	-Vetting of employee for cyber risks does not exist. -IT Service providers not responsible for cyber risks -Does not recognize the need for a NDA -There is no security policy. -Risks have no ownership.
Ensure cyber security quality	-Lack of information confidentiality -Lack of information integrity -Lack of information availability -IT Infrastructure configured ad-hoc. -IT Infrastructure configured ad-hoc.
Maximize cyber risk knowledge	-No training program for cyber risk Management -No awareness of cyber risks -No competencies in cyber risk management. -Cyber risk management culture does not exist.
Maximize compliance	-No performance metrics in cyber risk management -No auditing procedures for cyber risks -Technical monitorization of cyber risks. -No requirements of compliance defined by supervisory entities. -No legal requirements of compliance defined. -No adoption of standards and best practices. -No copyright management procedures.
Maximize the protection of human life	-Frequent cases of human negligence cause harm to others -Critical infrastructures malfunction causes human harm. -Medical devices malfunction causes human harm due to IT problems. -No Protection of data privacy.

Table 5.6: Bad scenario

of risk management causes harm to the human life.

The bad scenario detailed in Table 5.6 shows every objective in a non-existent state. In this scenario management doesn't even know that risk management exists and should have defined objectives.

5.2.1 Respondent profile

Our data collection involved 3 workshops conducted in 2016. Both initial workshops were composed of IT professionals with at least a year experience in IT and previous experience in information security and risk management, normally more focused on IT security.

The first workshop had 24 participants and the second workshop had 19 participants. These workshops had the duration of 1 hour and were conducted in 2 different cities with different respondents.

Some roles present in these workshops were IT Manager, Senior Security Consultant and IT Director for example. The youngest participant was 21 and the oldest was 52. Only 1 woman was present in the first workshop and 2 women were present in the second workshop.

The third workshop or expert panel workshop was composed by specialists in risk management and information security, all specialists must fulfil the requirement of having more that 10 year experience in information security and being involved in risk management decisions. The third workshop had 6 participants and took about 1 hour and 30 minutes. No woman was present in the third workshop. Common roles for this third workshop were CISO, Lead Auditor or Professor for example. The youngest participant was 36 and the oldest was 61.

5.2.2 Data analysis

This section analyzes the data collected from all three workshops. Tables 5.7, 5.8, 5.9 and 5.10 detail the data of the respondents before reading the scenarios and having only a definition of each objective. Tables 5.11, 5.12, 5.13 and 5.14 contain the final data after the participants understand how those objectives are applied in real scenarios. Tables 5.15, 5.16, 5.17 and 5.18 detail the preference of respondents among analyzed scenarios.

The initial results detail the ranking and weighting of objectives without seeing the implementation of objectives in scenarios. In workshop 1, detailed in Table 5.7, the participants ranked the ”maximization of the protection of human life” as the most important objective and in workshop 2, detailed in Table 5.8, the participants ranked the objective ”ensure security quality” as the most important. In Table 5.9, workshop 3 ranked ”ensure risk management governance” as the most important objective. Moreover, during discussion among participants, one specialist in risk management noted: *"Without governance there's no structure for other objectives to be maximized. Adequate governance establishes that baseline for progression"*. This is not the same opinion as participants in workshop 1 and 2 that ranked ”ensure risk governance” as the least important objective.

When analyzing the aggregated results from all workshops in Table 5.10, the most ranked initial result for all workshops was ”maximize the protection of human life”, which was ranked first in workshop 1 and ranked second in workshop 2 and 3. ”Ensure security quality” was ranked second equal to the rank in workshop 1 and decreased the rank from workshop 2, being ranked as the most important objective. ”Maximize risk knowledge” ranked as third most important objective in the consolidated results for all workshops, maintaining the same result in workshop 1 and 2.

Fundamental objective	Importance rank	Median of importance rank	Mean of swing weights
Ensure risk management governance	6	5	62,87
Maximize responsibility and accountability for cyber risks	5	5	57,33
Ensure cyber security quality	2	2	76,58
Maximize cyber risk knowledge	3	3	70,46
Maximize compliance	4	4	67,87
Maximize the protection of human life	1	2	81,96

Table 5.7: Initial results for workshop 1

Fundamental objective	Importance rank	Median of importance rank	Mean of swing weights
Ensure risk management governance	6	5	77,42
Maximize responsibility and accountability for cyber risks	5	4	77,43
Ensure cyber security quality	1	2	88,89
Maximize cyber risk knowledge	3	4	83,21
Maximize compliance	4	4	81,42
Maximize the protection of human life	2	3	84,84

Table 5.8: Initial results for workshop 2

Fundamental objective	Importance rank	Median of importance rank	Mean of swing weights
Ensure risk management governance	1	1	80,43
Maximize responsibility and accountability for cyber risks	3	3	71,43
Ensure cyber security quality	4	3	65,86
Maximize cyber risk knowledge	6	5	58,57
Maximize compliance	5	5	59,28
Maximize the protection of human life	2	2	77,85

Table 5.9: Initial results for workshop 3

Fundamental objective	Importance rank	Median of importance rank	Mean of swing weights
Ensure risk management governance	5	5	70,86
Maximize responsibility and accountability for cyber risks	6	5	66,94
Ensure cyber security quality	2	2	79,76
Maximize cyber risk knowledge	3	3	73,74
Maximize compliance	4	4	71,82
Maximize the protection of human life	1	2	82,48

Table 5.10: Initial results for all workshops

The median of importance rank in workshop 1 for the objectives ”maximize protection of human life” and ”ensure security quality” is the same with the value 2. The average swing weight in workshop 1 for those 2 objectives are 81,96 and 76,58 giving clear advantage to ”maximize protection of human life”. The initial results for workshop 2 have for all objectives relative high means of swing weights ranging from 77,42 to 88,89, when comparing to the initial results of other workshops. In workshop 3 both the objectives ”maximize responsibility and accountability for risks” and ”ensure security quality” have the median rank of 3, but the mean swing weight of 71,43 compared to 65,86 gives advantage to ”maximize responsibility and accountability for risks”.

The final results step gives the participants the option to change initial weights and ranks, after seeing each objective implemented within each different scenario as it can be seen in Tables 5.11, 5.12 and 5.13. The final consolidated weights for all workshops is detailed in table 5.14.

When comparing the initial importance rank from workshop 1 in Table 5.7 with the final importance rank in Table 5.11, it can be seen that participants changed the ranking of 3 objectives after seeing the real implementation in the scenarios. The initial ranking from first to third is maintained, but the ”ensure risk management governance” objective rises from the initial sixth position to the fourth position. Both ”maximize compliance” and ”maximize responsibility and accountability for risks” objectives lost one position, being in the final results in the fifth and sixth position. Some participants explained, that although they understood the context of some objectives in theory, they were not aware of their consequence in practice and the scenarios exercise helped them by increasing that understanding. The mean of all swing weights also increased from the initial to the final results of workshop 1. The median of importance rank from the initial to the final results for the objectives ”ensure risk management governance” and ”maximize responsibility and accountability for risks” decreased from four to five, while the median for the other objectives is maintained. The median of importance rank increased from 5 to 4 from the initial to the final results for the objectives ”ensure risk management governance” and ”maximize accountability and responsibility for risks”.

The participants in workshop 2 maintained their importance rank from the initial to the final results as it can be seen in Table 5.8 and 5.12. The mean of most swing weights increased from the initial to final results of workshop 2, with the unique exception of the objective ”ensure security quality” that decreased from 88,89 initial weight to the final weight of 87,84. In workshop 2 most median of importance ranks were maintained from the initial to the final results, with the exception of the median for the objective ”maximize risk knowledge” that increased from 4 to 3 respectively. The median of importance rank increased from 4 to 3 from the initial to the final results for the objective

Fundamental objective	Importance rank	Median of importance rank	Mean of swing weights
Ensure risk management governance	4	4	70,58
Maximize responsibility and accountability for cyber risks	6	4	67,79
Ensure cyber security quality	2	2	79,04
Maximize cyber risk knowledge	3	3	71,92
Maximize compliance	5	4	70,96
Maximize the protection of human life	1	2	82,13

Table 5.11: Final results for workshop 1

Fundamental objective	Importance rank	Median of importance rank	Mean of swing weights
Ensure risk management governance	6	5	82,58
Maximize responsibility and accountability for cyber risks	5	4	78,63
Ensure cyber security quality	1	2	87,84
Maximize cyber risk knowledge	3	3	85,42
Maximize compliance	4	4	83,74
Maximize the protection of human life	2	3	85,37

Table 5.12: Final results for workshop 2

Fundamental objective	Importance rank	Median of importance rank	Mean of swing weights
Ensure risk management governance	2	2	78,43
Maximize responsibility and accountability for cyber risks	3	2	73,86
Ensure cyber security quality	4	3	69,14
Maximize cyber risk knowledge	6	5	55,71
Maximize compliance	5	4	61,42
Maximize the protection of human life	1	1	75,88

Table 5.13: Final results for workshop 3

Fundamental objective	Importance rank	Median of importance rank	Mean of swing weights
Ensure risk management governance	4	5	76,24
Maximize responsibility and accountability for cyber risks	6	4,5	72,76
Ensure cyber security quality	1	2	81
Maximize cyber risk knowledge	3	3,5	74,78
Maximize compliance	5	4	74,48
Maximize the protection of human life	2	3	82,48

Table 5.14: Final results for all workshops

”maximize risk knowledge”, while all other objectives maintained their median of importance rank. The mean of swing weights for all objectives increased from the initial to the final results, with the exception of the objective ”ensure security quality” that decreased from the initial to the final results.

The participants in workshop 3 in Table 5.13 exchanged the ranking of the first and second ranked objectives from the initial to the final results. ”Maximized the protection of human life” moved to second and ”ensure security quality” moved to the first rank. Even specialists or subject matter experts change their opinion after seeing the implementation of objectives within scenarios, which shows that scenarios help to clearly understand risk objectives, even for the individual with deep knowledge in the subject. The objective ”maximize risk knowledge” received the lowest mean of swing weight across all workshops with 55,71. The median of importance rank for the objective ”maximize protection of human life” decreased from 3 to 2. In workshop 3 the mean of swing weights from the initial to the final results increased for 3 objectives:”ensure security quality”, ”maximize risk knowledge” and ”maximize compliance”. For the remaining 3 objectives the mean of swing weights from the initial to the final results decreased.

The final results for all workshops in Table 5.14, details that all the mean of swing weights increased from the initial results, with the exception of ”maximize the protection of human life” that remained the same. This reinforces the mindset that the swing weights increase after seeing each of the objectives implemented in real scenarios. When comparing the importance ranking of objectives from the initial to the final results, most participants changed the ranking of ”ensure security quality” from the second position in the initial results to the first position in the final results. Following the same mindset ”maximize the protection of human life” dropped one position to the second importance rank. Other changes in the importance rank happened with ”ensure risk management governance” that dropped from the fourth to the fifth position and ”maximize compliance” that moved from the fifth to the fourth position. The means of swing weights, from the initial to the final results, all increased with the exception of the objective ”maximize the protection of human life” in which the mean of swing weights stayed the same with 82,48.

Tables 5.15, 5.16 and 5.17 detail the global scenario ranking individually in each scenario and then globally in all scenarios in Table 5.18. There are no differences in the ranking of scenarios across workshops. All workshops choose scenario A as the most most important custom scenario and declining to scenario D as the worst custom real world scenario. The average swing weights from workshop 1 in scenario A and B were close with 77,46 and 71,25, but it became evident that scenario A is preferred with workshop 2 and the average swing weights between scenario A and

Scenario	Importance rank	Median of importance rank	Mean of swing weights
Good	1	1	100
A	2	2	77,46
B	3	3	71,25
C	4	4	52,63
D	5	5	30,58
Bad	6	6	0

Table 5.15: Global scenario ranking and weighting for workshop 1

Scenario	Importance rank	Median of importance rank	Mean of swing weights
Good	1	1	100
A	2	2	83,84
B	3	3	73,95
C	4	4	47,37
D	5	5	20,68
Bad	6	6	0

Table 5.16: Global scenario ranking and weighting for workshop 2

B with 83,84 and 73,95. In workshop 3, the mean of swing weights from A to B was 75,57 and 66,43 respectively. Some participants in the workshop 1 and 2 discussed that scenario A was too risk controlling for them and that the strict blind application of detailed consequences would limit business and impact negatively employee satisfaction. The median of importance rank mimics the importance rank across all scenarios.

The individual importance rank of objectives across scenarios, allows for participants to rank the objective higher in a different scenario individually, although they ranked that scenario higher or lower globally. For the objective ”ensure risk management governance” in Table 5.19, the importance rank mimics the choice of the global scenario. In the case of the objective ”maximize responsibility and accountability for risks” presented in Table 5.20, the participants ranked that objective in scenario B higher than scenario A, although they selected scenario A as preferred than scenario B globally. The median of importance rank is the same for both scenarios with value 3 and the

Scenario	Importance rank	Median of importance rank	Mean of swing weights
Good	1	1	100
A	2	2	75,57
B	3	3	66,43
C	4	4	42,86
D	5	5	22,86
Bad	6	6	0

Table 5.17: Global scenario ranking and weighting for workshop 3

Scenario	Importance rank	Median of importance rank	Mean of swing weights
Good	1	1	100
A	2	2	78,45
B	3	3	70,79
C	4	4	49,16
D	5	5	33,12
Bad	6	6	0

Table 5.18: Global scenario ranking and weighting for all workshops

Ensure risk management governance	Importance rank	Median of importance rank	Mean of swing weights
Good	1	1	100
A	2	2	81,44
B	3	3	72,4
C	4	4	49,59
D	5	5	31,1
Bad	6	6	0

Table 5.19: Ensure risk management governance ranking and weights across scenarios for all workshops

Maximize responsibility and accountability for cyber risks	Importance rank	Median of importance rank	Mean of swing weights
Good	1	1	100
A	3	3	72,64
B	2	3	72,18
C	4	4	57,11
D	5	5	29,7
Bad	6	6	0

Table 5.20: Maximize responsibility and accountability for cyber risks ranking and weights across scenarios for all workshops

Ensure cyber security quality	Importance rank	Median of importance rank	Mean of swing weights
Good	1	1	100
A	2	2	77,32
B	3	3	69,32
C	4	4	52,16
D	5	5	36,5
Bad	6	6	0

Table 5.21: Ensure cyber security quality ranking and weights across scenarios for all workshops

Maximize cyber risk knowledge	Importance rank	Median of importance rank	Mean of swing weights
Good	1	1	100
A	2	2	75,92
B	3	3	67,8
C	4	4	46
D	5	5	31,88
Bad	6	6	0

Table 5.22: Maximize cyber risk knowledge ranking and weights across scenarios for all workshops

Maximize compliance	Importance rank	Median of importance rank	Mean of swing weights
Good	1	1	100
A	3	3	74,34
B	2	3	73,06
C	4	4	46,18
D	5	5	29,08
Bad	6	6	0

Table 5.23: Maximize compliance ranking and weights across scenarios for all workshops

mean of swing weights is similar with 72,64 for scenario A and 72,18 for scenario B. For the objective ”ensure security quality” in Table 5.21 and for the objective ”maximize risk knowledge” in Table 5.22, the results mimic the values from the global scenario ranking. For the objective ”maximize compliance” in Table 5.23, the participants once again ranked that objective higher in scenario B than in scenario A, although they preferred scenario A to B globally. The median of importance rank is the same for both scenarios with value 3 and the mean swing weights is similar with 74,34 for scenario A and 73,06 for scenario B. For the objective ”maximize the protection of human life” in Table 5.24, the results mimic the preference among global scenario ranking.

Maximize the protection of human life	Importance rank	Median of importance rank	Mean of swing weights
Good	1	1	100
A	2	2	76,42
B	3	3	72,58
C	4	4	48,52
D	5	5	32,42
Bad	6	6	0

Table 5.24: Maximize the protection of human life ranking and weights across scenarios for all workshops

5.3 Risk policy decision making

After having the results from the scenarios evaluation phase, we continue to follow the procedure from Keeney et al. (1990) to establish a model for risk policy decision making. The first step is to recognize a decision problem. In our case the decision problem is how to effectively minimize cyber risks in organizations, as threats and vulnerabilities continue to rise. Decision makers are presented with multiple alternatives for risk mitigation and are urged to decide the best way possible, while taking into account the interests of multiple stakeholders. The second step is the creation of the objectives hierarchy to minimize cyber risk, taking into account the fundamental and means objectives previously identified. The third step is the creation of evaluation measures to be able to evaluate the performance of each objective. The forth step is to weight the value hierarchy taking into account the discussion of the subject with risk management experts. This final step permits the creation of a decision model that is able to evaluate the adequacy of multiple presented alternatives.

5.3.1 Risk objectives hierarchy

The risk objectives hierarchy was created taking as a basis the fundamental-means objectives network previously defined in Figure 4.1. Each means objective can influence more than one fundamental objective in indirect marginal terms, but there's one fundamental objective that is directly affected and depends upon the specific means objective. This mindset was the main criteria for establishing the hierarchy. The hierarchy was discussed with multiple professors and information security risk professionals, and the final result is present in Figure 5.1.

5.3.2 Evaluation measures

The next step involves the creation of attributes or evaluation measures to measure each objective. These evaluation measures permit the quantification of the performance of accomplishment for each of the objectives. In the cyber risk context, if we take the fundamental objective of "Maximize risk knowledge", then an attribute that needs to be measured can be the "Number of people trained in risk management per year". This is a clear example of a measure that is direct or natural, but unfortunately there can also be constructed attributes taking into account for example a likert scale to measure the achievement indirectly. For example a five point likert scale can be established where strongly disagree has the value of 0, disagree has the value of 0,25, neither agree or disagree

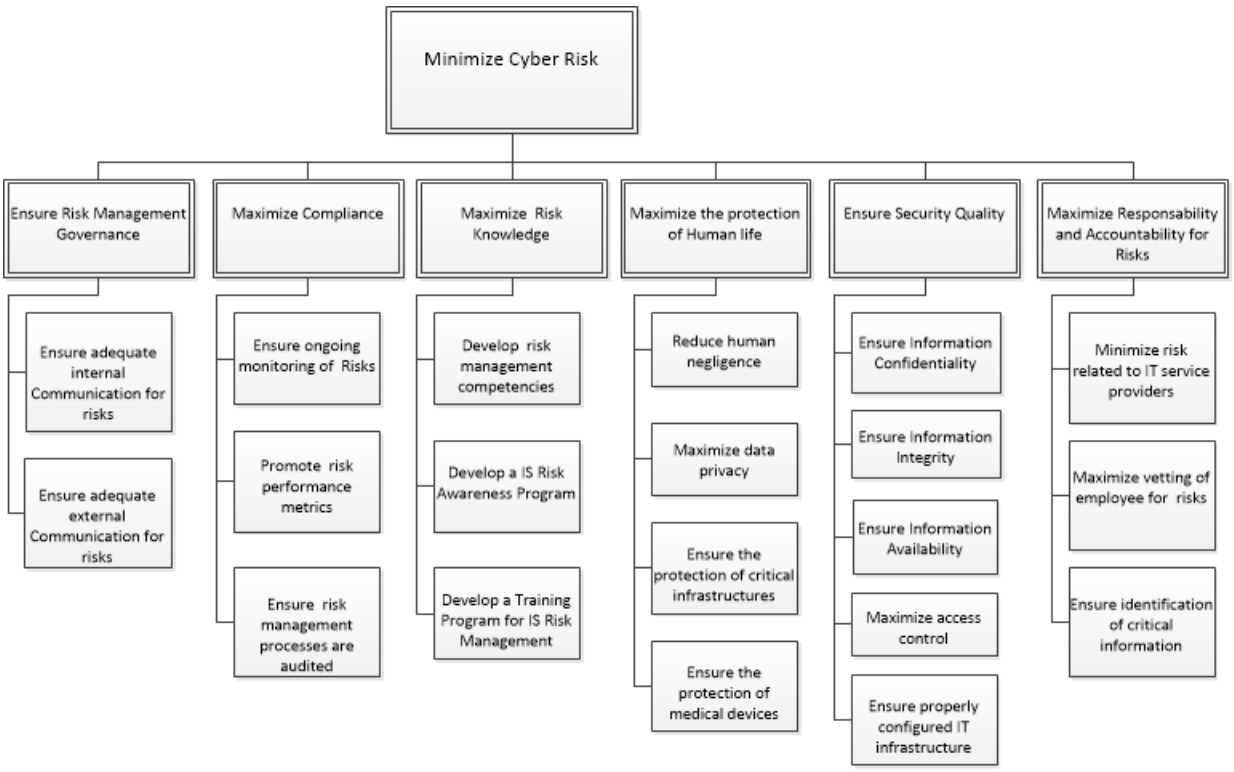

Figure 5.1: Risk hierarchy

the value 0,5, agree the value 0,75 and strongly agree the value of 1. However both Kirkwood (1996) and Keeney (1992) recommend the use of natural attributes as they are normally understood and accepted by stakeholders (Keeney, 2007a; Keeney and Gregory, 2005). Those natural attributes for risk management can be seen in Table 5.25.

5.3.3 Value functions

The attributes in the previous step can be a mixture of different measurement units and different scales, thus we need to unify all measures into one common value function, which is situated between 0 and 1. Taking into account the previous example of “Maximize cyber risk knowledge”, with the attribute “Number of people trained in cyber risk management per year”, we surmise that in this case, the decision maker might well postulate whether he wants at least 50 people to be trained per year, which would lead to 50 people or more being attributed the value 1. If 0 people were trained, then a value 0 would be attributed, as can be seen in Figure 5.2.

Fundamental objective	Attribute
Ensure risk management governance	-Number of risk steering committee meetings per year
Maximize cyber risk knowledge	-Number of awareness programs per year -Number of people trained in cyber risk management per year
Ensure cyber security quality	-Number of information security breaches per year -Number of transactions missing integrity checks per year -Duration of unavailability of services per year
Maximize responsibility and accountability for cyber risks	-Number of identified risks without any treatment -Number of employees suspended due to cyber risks
Maximize compliance	-Number of non-compliance issues detected per year
Maximize the protection of human life	-Number of people harmed due to cyber risks per year

Table 5.25: Evaluation measures

Figure 5.2: Value function

5.3.4 Value hierarchy weights

The objectives were weighted using the swing method (Kirkwood, 1996), whereby a panel of participants in risk management and information security is asked to judge the importance of objectives designed for the global objective of minimizing information security risk. This approach leads to defining a local weighting to each sub-objective in a branch. All the local weightings in a branch sum up to 100%, in order to fulfill the main objective. A multi-tier hierarchy is then evaluated with global weightings, whereby local weightings are multiplied to accomplish the main objective, using an additive function.

For the purpose of weighting the fundamental objectives, we arranged a workshop to foment the discussion and collect the opinion of the attendees regarding the importance of each objective within the model. The workshop was performed within an information security conference in 2014 with the duration of 40 minutes. There were 31 participants with positions such as for example

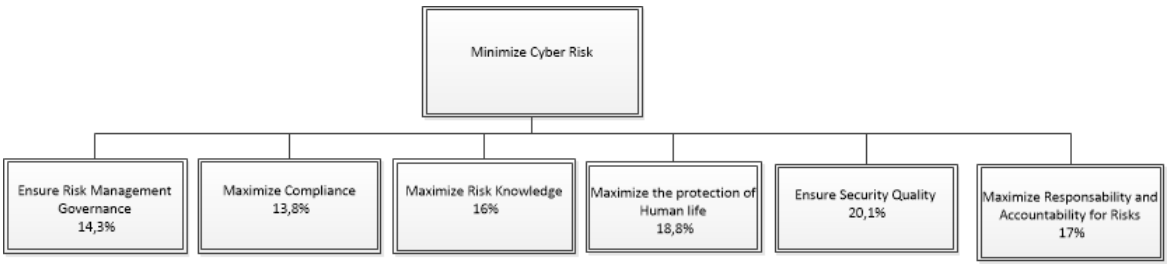

Figure 5.3: Conference workshop risk hierarchy weights in 2014

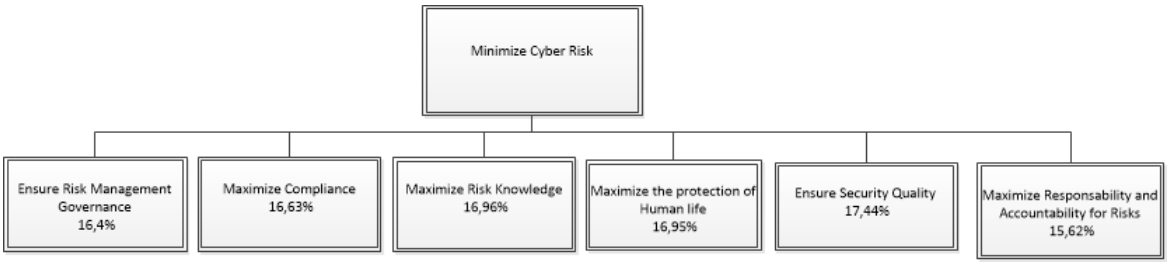

Figure 5.4: Scenarios 3 workshops risk hierarchy weights in 2016

CISO, IT Manager, Auditor, Security Consultant and Professor. In this workshop the participants were provided with a brief description of each objective, but they were not provided with scenarios that show the implementation of each objective.

We also analyzed the results from the 3 workshops detailed in the previous section, after the participants evaluated each scenario. These workshops were conducted in 2016. In this case participants were given different scenarios that show how each objective is implemented in practice and its consequences.

The results of the conference workshop can be seen in Figure 5.3 with all fundamental objectives being weighted to fulfil the strategic objective of minimizing information security risk. The results from the 3 workshops, where the participants also evaluated each scenario, can be seen in Figure 5.4. The remainder of this section discusses the results of each of the objective's weight.

Ensure risk management governance: The weight of this objective in the hierarchy is classified with 14,3% in the overall model captured in the conference workshop, which reflects the lack of risk governance maturity in most organizations in Portugal in 2014. The weight increased in the model from the 3 workshops to 16,4%, this can be noticed with the evolution of governance structures within organizations from 2014 to 2016. Governance is seen by some participants in workshops as the baseline objective that helps to enhance other objectives.

Maximize responsibility and accountability for cyber risks: In the model from the conference

workshop, this objective is weighted with 17% which demonstrates the need to assure adequate responsibility and accountability practices. In the results from the 3 workshops, this objective has the least weight in the overall model, which still reflects common finger-pointing behavior in organizations, when risks materialize. This is still an Achilles' heel problem in current organizations, gray areas of responsibility and accountability continue to grow with the rise of external providers. Even with the delegation of service to external providers, the ultimate responsibility for risk stays in the parent organization and that organization is accountable legally for risks that affect their costumers, such as for example data breaches.

Maximize cyber risk knowledge: In our model this objective represents 16% of the overall weight in the conference workshop and it demonstrates that people skills in risk management are an important objective. They are often left in the background in current organizations, as there are always more critical objectives appearing in risk management that need immediate attention. This objective maintains a similar weight in the 3 workshop model with 16,96%. This objective will tend to be more critical in the future with the rise of open positions in the risk management and security domains without candidates. Only adequate professionals will be able to transmit the value of a mature cyber risk culture to the whole organization, widening the message across multiple departments with different needs. This risk knowledge will be a source of competitive advantage in a growing digital market, where cyber risks will hamper businesses.

Maximize compliance: This objective was the least scored objective in the conference workshop with 13,8%. This score details the significance of compliance in Portugal as the supervision entities are still benevolent in terms of compliance practices, functioning still as advisory when enforcing mandatory requirements. In the 3 workshops model this objective shows an important increase to 16,63%. The maturity of compliance in organizations has shown clear signs of evolution from 2014 to 2016, which is also reflected in the model. This result is aligned with the reinforcement of compliance standards and requirements from supervision entities, although some of them still function without independent auditing that enforces strict compliance.

Maximize the protection of human life: The score of 18,8% details that this objective in risk management is still dormant in our lives at the moment, but it may increase dramatically as examples of human losses turn into a reality with vulnerabilities being exploited in information systems. This weight decreased in the 3 workshops model to 16,95%. The absence of critical news reaching the normal public regarding this topic, maintains this objective in a dormant state out of the spotlight.

Ensure cyber security quality objective aggregates security concepts, including explicitly the in-

formation confidentiality, integrity and availability triad. Being the model weighting workshop conducted within an information security conference we would expect that this objective is the most critical within the model. This is what happened with this objective weighting 20,1% of the model. This objective is still the most weighted objective in the 3 workshops model with 17,44%. Security practices and mechanisms represent the common safeguards to minimize information systems risks and ensuring security quality is a main concern of every information systems professional.

5.4 Discussion

The value focused assessment of cyber risks allows managers to base their decisions on stakeholder's values that can be subject to analytical generalization in different cases. Yin (2003) argues along that line, and states that analytical generalization leads to theoretical propositions. These risk objectives are focused on technical, procedural and social mechanisms. With these objectives an organization can evaluate what are the critical ones for the current business and which safeguards will minimize the current risk level individually.

In a decision context, if we identify objectives as $(O_1, O_2, ...O_n)$ and each sub-objective as measures $(x_1, x_2, ..., x_n)$ to form the vector v to achieve that fundamental objective, with k_i as the weight and v_i as the given desirability, the following value model is established in Equation 5.1:

$$v(x_1, x_2, ..., x_n) = \sum_{i=1}^{n} k_i v_i(x_i) \tag{5.1}$$

The relationship among objectives can be obtained for example: Ensure properly configured IT infrastructure (x_1) influences the access control maximization $(x_2$) that minimizes human negligence (x_3) and leads to a maximization of responsibility and accountability for cyber risks (O_1). This approach allows for the maximization of the chosen objective by controlling the effectiveness of sub objectives with their defined weights.

Risk management values differ taking into account the entity making the decision. This entity should decide what the main priority in risk management is and what the adequate safeguards to minimize the risk are. The risk criticality for an individual is different when comparing to the risk mitigation decision process for a government or for a private organization. For example the fundamental risk to maximize compliance plays a small role at the individual level, but is a critical factor at the organizational level. If someone finds gaps in the measures that define an objective, then

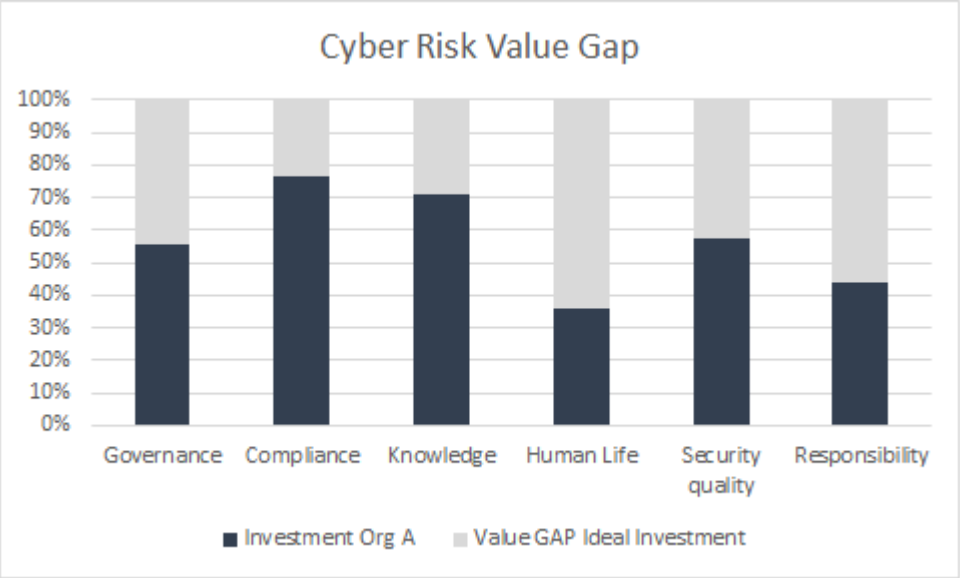

Figure 5.5: Cyber risk value gap

he can spot additional means objectives that allow to maximize that fundamental objective. These fundamental objectives are clear statements of values that were formed based on the current social status when addressing cyber risk management. This approach allows the understanding of values regarding risk management and after that it allows the weighting and prioritization of sometimes conflicting values of stakeholders. The evaluation of alternative investments can be corroborated with the sensitivity analysis to minimize the impact of the weights given to the objectives. With the sensitivity analysis, small differences in the weights of objectives do not force an erroneous decision and the decision maker is able to see the big picture and decide in an adequate manner.

If we take as an example a security investment alternative from organization A to minimize cyber risk, we can evaluate that investment using Equation 5.1. The results can be mapped into the ideal investment. Towards that ideal utopical investment, where all values are maximized to 100% fulfilment of the objectives, the investment from organization A will have a value gap in each of the objectives, as it can be seen in Figure 5.5. This way multiple investment alternatives can be easily compared between them and also towards the ideal utopical solution to measure value gaps. Those investment alternatives can be subjected afterwards to a sensitivity analysis to minimize the subjective nature present in the weights of the decision model. This analysis permits to vary the weights, while maintaining the other values constant and record the change as dots to form a function of the sensitivity of the alternative. This way it's possible to compare multiple alternatives minimizing the importance of the weights in the decision process.

The justification of a decision is also a factor that is enhanced with the use of this value model. The support and communication of a choice is a delicate process within an organization. This model simplifies not only the decision process but also the justification, communication and gathers the motivation to implement the chosen path, with a clear transparency of the decision process. It reduces the common feeling within organizations that management decisions are taken lightly and based on political or personal interests and solves conflicts with the evaluation of value trade-offs. This study focuses on the decision making process by integrating multiple stakeholders' objectives in the model. Bringing stakeholders' objectives into the decision process allows for the decision-maker to justify investments in risk mitigation controls. These controls are evaluated with the primary explicit and implicit concerns of the stakeholders and the relative weight of their objectives. The implicit concerns are revealed as hidden objectives that were not taken into account initially. This allows the refinement of investments to take into account the critical objectives of the organization to minimize risk. Risk management should be viewed as a facilitator process that does not hinder business opportunities, and this value focused approach sustains that mindset with the alignment of business objectives and the risk mitigation decision process. This alignment enhances the speed of decision making as organizations demand that decisions are taken quickly and should not miss business opportunities. Most policy decisions fail and are circumvented due to the lack of support and this cyber risk model simplifies the acceptance of the decision, because the basis for taking the decision is based on values from stakeholders.

5.5 Conclusion

This chapter presents a value decision model for cyber risk management. It uses the objectives from the previous chapter and provides weights for them, taking into account multiple real world scenarios discussed in workshops. The risk hierarchy weights are presented in a longitudional approach captured first in 2014 and later in 2016. We present evaluation measures and value functions that allow to measure the achievement of objectives. The chapter finishes with the discussion of an example of a security investment from an organization and the ability to observe the gap between that security investment and the ideal situation of cyber risk mitigation taking into account the weights of the objectives.

Chapter 6

Risk Management Strategy

"Appear weak when you are strong, and strong when you are weak."

—Sun Tzu, the Art of War

6.1 Introduction

What is strategy? The term has its origins in ancient Greece in the military environment with the word ”Strategos” that is formed from army and leadership. Leading an army not only to win a battle, but winning the war across multiple battles was the main concern at the time in that environment. Quinn (1981) defines strategy as ”the pattern or plan that integrates an organization’s major goals, policies and action sequencies into a coesive whole”. It allocates resources into a viable and unique posture, taking into account the existing internal competencies, external environment changes and moves of the opponents. Ansoff (1987) explains that strategy formulation is ”the logic which guides the process by which an organization adapts to its external environment”. Mintzberg (1987a) presents five definitions for strategy. Strategy as a plan that details a ”conciously intended course of action”. Strategy as a pattern characterized by a stream of actions that ensures consistency in behavior. Strategy as a position situated within a defined but continuously changing environment. Strategy as a perspective, as an ”ingrained way of perceiving the world”. Finally strategy as a ploy to influence others, disrupting them by staying a step ahead in the competing

market. Mintzberg (1987b) explains that ”strategy is needed to focus effort and promote coordination of activity”. More than a collection of individuals and resources there's the need for a collective action. Strategy finds the meaning for the organization in the competing market, nurturing and shaping its organizational culture towards a defined goal. Strategy seeks to act under conditions of stability to position the organization in a path where problems are avoided or easily solvable by blocking unexpected situations and reducing uncertainty. Mintzberg (1988) argues that strategy has both emergent and deliberate behavior. A strategist cannot think of everything a priori and has to leave space for strategy to gradually grow from intended actions and be able to be reoriented if necessary. Porter (1996) explains that strategy aims to create an unique position by leveraging a different set of activities, while making trade-offs in competing and creating fit with internal organizational activities. Moreover, Johnson et al. (2008) state that ”strategy is the direction and scope of an organisation over the long term, which achieves advantage in a changing environment through its configuration of resources and competences with the aim of fulfilling stakeholder expectations.”

With the rise of threats that stay dormant in the cyberspace waiting for the right moment to attack, there's no doubt that strategic approaches to cyber risk management should exist. The creation of a cyber risk management strategy is the main step to protect organizations from operational risks, while maintaining compliance with mandatory standards and existing regulation. This strategy guides risk assessments to organizational assets, where critical information resides. This strategy is focused on helping management decision making towards cyber risks. What should be incorporated in a risk management strategy? How can we incorporate objectives from stakeholders to simplify the acceptance of risk management policies? These trade-offs brought by the objectives of stakeholders, that consequently influence decision making, are a driving force for top management to reconcile their own conflicting interests and contribute to a real perception of risk. Only with this perception of risk is possible to create an adequate risk management strategy (McFadzean et al., 2006).

The definition and analysis of the objectives of stakeholders based on values was captured in previous chapters and based on those values we created a decision model for risk management by ranking and weighting each of the objectives in real world scenarios. Objectives based on values capture the interests of stakeholders and should be included in the organization strategy to increase its success (King, 1978). The strategy is the direction that an organization chooses in order to achieve the proposed objectives. How can those values in the form of objectives be incorporated inside the strategy in a practical form? Each means objective is determinant to achieve a funda-

mental objective, but what is the level of importance and achievable level to each organization? Taking into account these two axis, importance and achievable level, organizations can operationalize each of the means objective in order to maximize the benefits of the fundamental objective and form a strategic approach for cyber risk management. Those objectives were weighted across real world scenarios to form a decision model in the previous chapter. That decision model will help top management by defining priorities for the cyber risk strategy taking into account the management risk tolerance in multiple scenarios. Strategy needs to have principles for its guidance, this chapter presents principles for cyber risk management that can serve as a baseline for organizations to plan their cyber risk strategy.

6.2 Case A

The characterization of the studied organization relied upon 4 sources: information from interviewees, internal documents provided, public information and observation of current practices. All the characterization will ensure that the analyzed organization remains anonymous. The complete period of analysis started in May 2015 and ended in March 2017. This longitudinal research allowed to observe and capture multiple changes over time, some of them proactive in a planned and preventative approach, others reactive to respond to critical events. These changes happen in a continuously changing organizational context affecting people, technology and processes.

This organization is the central authority of a public service in Portugal. Every Portuguese citizen is a client of this authority and it has multiple processes that also include communication with foreign nations. Organizations operating in Portugal are also clients of this authority. The management board is composed by a general director and twelve sub directors. It has 11122 employees according to the analyzed data of 2016. This organization has the following organizational values: ethics, transparency, independence, responsibility, collaboration, professionalism and innovation.

The organization has an employee's code of conduct that details risk management and information security responsibilities. Ensure the information protection with security measures is a main objective of this organization detailed in the activity report of 2016. The policy against corruption also mentions the importance of risk management and information security for this organization. This organization has developed a specific strategic plan in 2015 to ensure information security across all the organization, with specific measures to enhance the maturity of security. This plan focuses the importance of a mature risk management approach.

6.2.1 Context

The external context is characterized by continuous political pressure that influence decision making. The organization resides in an external environment of uncertainty and continuous strategic change due to the economical crisis in Portugal. From a societal point of view, this organization is seen as mature and specialist in its business sector and their activities impact every citizen and organization in their everyday life. Due to this massive impact, the organization is present in the news multiple times and catches everyone's attention. The legal framework of the country also impacts directly this organization. From a technological point of view, this organization is making the necessary efforts to digitally transform legacy processes. This technological change is seen as a critical strategic business objective. Being able to provide services on the Internet to the common citizen and organizations is a major step in the recognition of trust. The organization is seen by the common citizen as a technological innovator in the public sector.

The internal context shows typical characteristics of the public sector in Portugal. The workplace environment is calm and relaxed and initiatives are marked by a top-down leadership by top management. Although management recognizes the need to change some processes, the common employee is not open to changes to its daily activities and it's protected by a strong labor union. Retainment of employed specialists is an issue for the company, as some of them are moving to the private sector or emigrating to other countries due to higher salary packages. The flexibility to recruit new specialists is also limited due to the practices of the public sector. For specific projects there's a high dependence from external consultants' know-how and that knowledge is normally not retained within the organization after the project is finished.

6.2.2 Respondent profile

The respondents were managers, directors or sub directors of the analyzed organization, namely positions such as chief information security officer, chief information officer or IT director. The academic background of the respondents is information systems, information technology, management and accounting. They all have a minimum of 5 years of experience in their sector of specialization. There were 12 respondents that discussed the cyber risk management strategy with the researcher in the form of a formal interview. The interviews were scheduled for 1 hour, but the time was not strictly controlled by the researcher during the interview, with some interviews ending sooner and others ending later taking into account the discourse of the interviewee. If the information collected

required further clarification, the researcher asked the interviewee for another interview in a later time or to suggest members of his team or other individuals to be subjected to the interview process to be able to clarify with more detail those topics. Some of the participants were interviewed multiple times.

6.2.3 Threat analysis

The level of risk is directly influenced by the existing threats (Dhillon, 1995; Whitman, 2003). One common threat group is natural disasters such as flood, earthquake, etc. This threat poses serious risks to information availability and is minimized in this organization with business continuity management and disaster recovery to an alternate site. Threats of failures of IT equipment are also minimized with high availability mechanisms. There is replication of information and offline backups exist to ensure that information is not lost. Deliberate threats from outsiders pose high risks to the organization as the majority of information is confidential and will harm citizens and organizations, if exposed by a data breach. Affecting the integrity of information with a hacking attack might cause financial benefits to a chosen target, so this threat is high. The attack surface to a deliberate threat from a outsider are the online services available to every citizen and organization that are present on the Internet. Although cases of unavailability of some services of this organization are known to have existed in the past, recent infrastructure, communications and security mechanisms have maintained high availability of services in the last years. Deliberate attacks from employees are also a threat to consider, as they have privileged access to confidential information, that if tampered, will bring financial benefits to their family or friends for example. All accesses are monitored and access to information is justified by the employee and later reviewed by management, following the separation of privileges principle. Accidental errors as threats are minimized with application controls, that signal the error immediately. In case a error survives through the application controls, there is automatic and manual analysis of anomalies to detect additional errors. It can be seen by this threat analysis that the level of expertise of attackers can be high due to the financial gains that can be obtained by organized crime. Being a public entity it may be the target of terrorists to cause chaos and spread the message and it may be the target by other nations for intelligence gathering.

6.2.4 Data analysis

The researcher analyzed data from 3 sources: documents (both internal and public information), direct observation and interviews. The researcher consulted public documents available on the organization's website. During interviews, if some individual mentions some document, the researcher asks for a copy of that document for further analysis. Direct observation is a critical source of information, that is not filtered. The researcher took notes from multiple observed situations in the organization. The interview is performed within a defined schedule and the researcher poses open questions and takes extensive notes of the answers of respondents. All those notes and provided documents are later analyzed outside of the organization.

6.2.5 Discussion

This section relates the cyber risk and information security practices from the case study with the information security status quo surveyed in Portugal detailed in AP2SI (2016).

Governance is established in the analyzed organization with the existence of a dedicated information security department. This department still is hierarchically dependent from the IT department, but direct paths of reporting to top management for some critical issues are defined. When comparing with the status of the global practices in Portugal, they are inside the 45,8% of organizations with an information security department and inside the 54% of organizations where the information security department is inside the IT department. In the survey 58% of respondents say that their information security department has direct report to top management.

Top management commitment to cyber risk management and information security is formally written in the business strategic plan, with this organization being part of the 71,6% employees that pointed out in the survey that their organizations had top management commitment.

The analyzed organization has periodical information security audits. This affirmation is shared by 23% of the respondents of the survey. The organization details security requirements in clauses to partners. This practice is shared by 65% of the management respondents in the survey.

This organization has an information security policy and 55,2% of respondents from the survey point out that their organizations have an information security policy too. This policy is reviewed annually or when major changes happen. The survey details that in Portugal only 7,1% of organizations have reviewed their information security policy. The organization formally defines the responsibilities of

employees regarding information security and risk management. This behavior is the same as pointed out in the survey by 53% of organizations.

This organization is pursuing an information security management system certification to be part of the 28,4% of organizations that have such a certification in Portugal.

This organization is inside the 30% of organizations that have an awareness program in place. This organization faces problems in hiring specialists in this field. The survey details that only 6,9% of respondents point out that hiring in this field is easy.

The primary concerns revealed from interviewees in the analyzed organization are similar to those pointed out in the survey: unable to provide agreed service, unavailability of systems and public exposure of organizational information.

6.3 Developing strategy

A risk management decision model cannot be applied directly without considering a defined risk management strategy capturing the unique context of every organization. In this section we propose the development of a cyber risk management strategy by taking into account the previous defined objectives that emerged from the values of stakeholders. We took as the basis the development of a strategic grid used in the management and information systems literature (McFarlan and McKenney, 1983; Ward and Peppard, 2002), to create a grid that takes into account the importance level and achievable level of each of the means objectives to accomplish each of the fundamental objectives. The prioritization of each of the means objectives includes resource allocation, necessary effort measurement, cost benefits analysis and will influence the outcome of the fundamental objective, which may be different from organization A to organization B. In risk management strategic planning, an organization should map the four zones of the grid to award the appropriate weights to each of the means objective. These weights allow the maximization of the fundamental objective, taking into account the strategy of the organization and the current internal and external context. This approach can be easily integrated with common methods for strategic planning such as SWOT and PESTEL for example.

The results of this section characterize the priorities of each of the means objective in the case study A. The fundamental objective ”ensure security quality”, detailed in Figure 6.1 is influenced by the objectives: ”maximize access control”, ”ensure properly configured IT infrastructure”, ”ensure

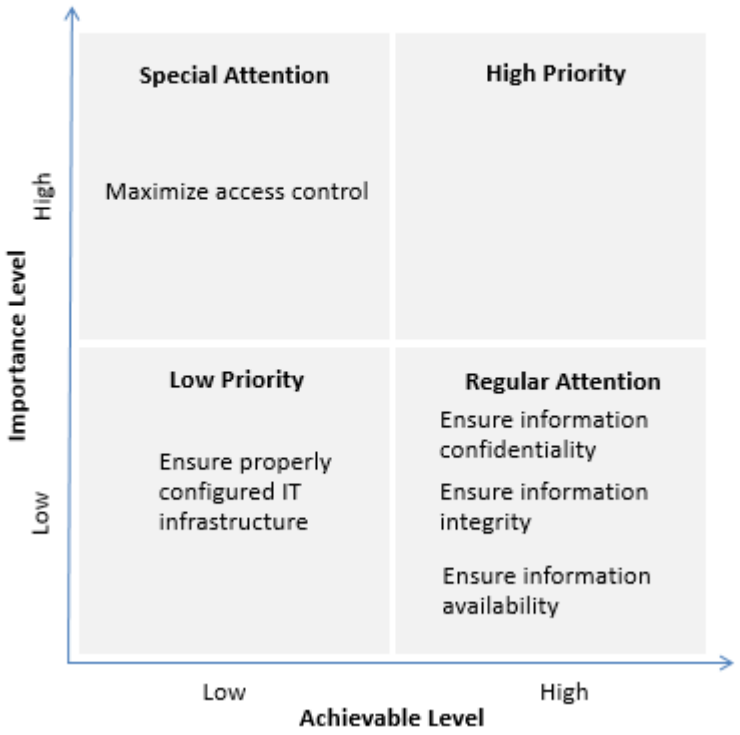

Figure 6.1: Ensure security quality

information confidentiality", "ensure information integrity" and "ensure information availability". The respondents pointed out that the objective "ensure properly configured IT infrastructure" is an on-going effort with low priority and that is difficult, if not impossible, to ensure a perfect configured IT infrastructure. This priority and lack of perfection is explained with the rise of shadow IT for example (Fürstenau and Rothe, 2014; Silic and Back, 2014). The CIA triad is dealt with regular attention with control mechanisms, that should be improved frequently, following the comparison of the cat and mouse duel, being the organization the cat and a potential attacker the mouse. This regular attention performed on the CIA triad results in the organization having no known data breach or integrity loss until the current time. The availability of information is assured with an alternative site and periodical synchronization of information exists. Regarding unavailability of IT service, there are only minor losses of service to be reported by the analyzed organization. The theme of access control is a critical topic inside this organization that needs special attention. This organization has a large piece of external organizations from which it receives and sends critical information, so adequate access control with continuous monitorization is vital. Some specialized services

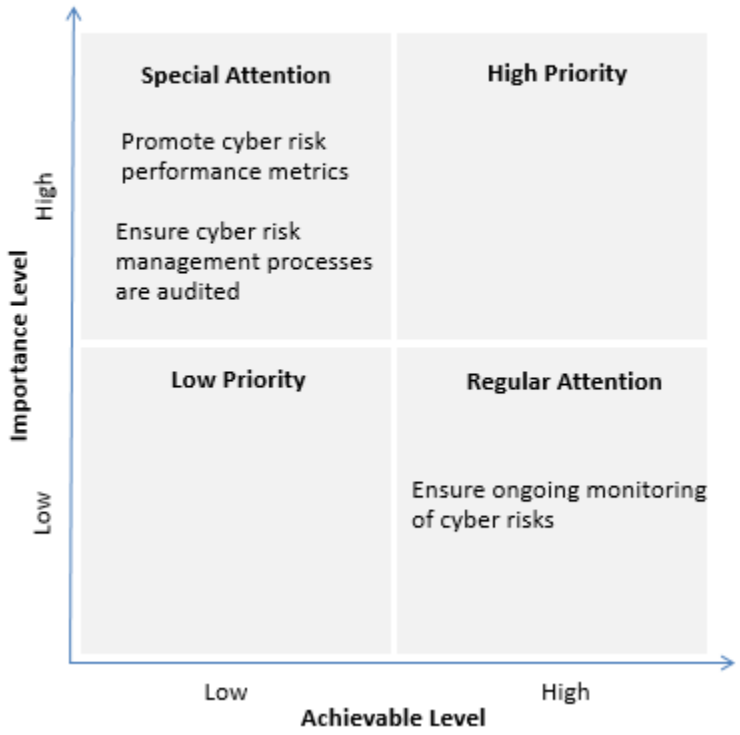

Figure 6.2: Maximize compliance

and custom development solutions are assured by external consulting teams, so adequate access control aligned with strong identity management practices is implemented. This ensures that the consultant has access to the information he needs, following the least privilege principle, and that access is removed when he leaves the project.

The fundamental objective ”maximize compliance” presented in Figure 6.2 is influenced by the means objectives ”promote cyber risk performance metrics”, ”ensure cyber risk management processes are audited” and ”ensure ongoing monitoring of cyber risks”. Being a public entity, case study A is not under mandatory standards like SOX, Basel or Solvency (ISACA, 2014; ITGI, 2007), but is under legal compliance requirements applied to the Portuguese public sector. In case study A the respondents considered that ”ensure ongoing monitoring of cyber risks” is an objective that requires continuous attention, although it’s easy to maintain after an initial significant effort to define and implement the process. Moreover with the risk monitoring process implemented, there is the regular need to see if the risk has changed, after business changes happen. Is the risk still accept-

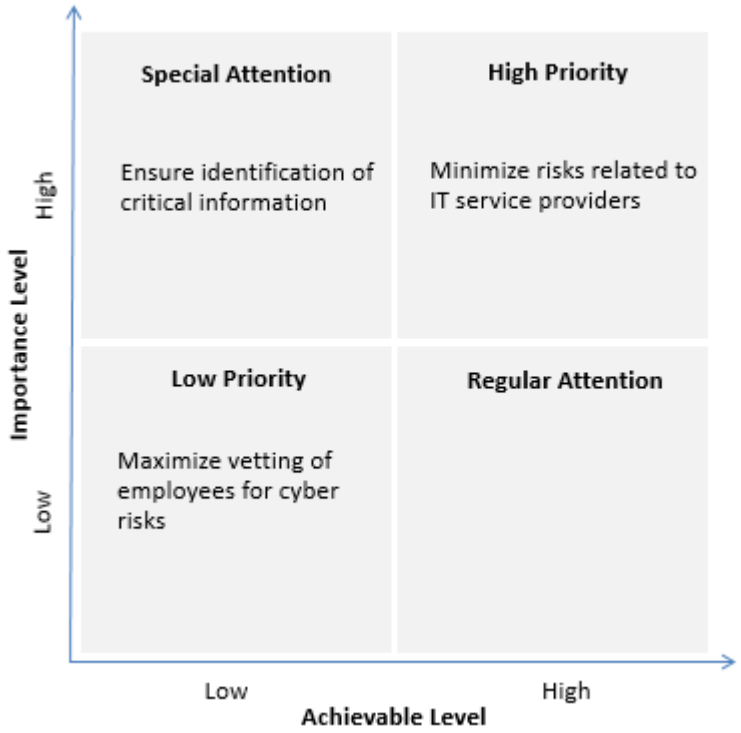

Figure 6.3: Maximize accountability and responsibility for cyber risks

able by top management after the change? Do we need to implement additional security controls to mitigate the risk? Another important aspect of compliance is the ability to measure results. These measures are performed by accomplishing the objective ”promote cyber risk performance metrics”, that contributes to the continuous improvement of the risk management process. This objective needs special attention from management to evaluate if the proper metrics are defined in the first place and to review the metrics periodically to adapt to current business needs (Bodin et al., 2005; Gordon and Loeb, 2002a; Slayton, 2015). Compliance should be transparent to supervision entities and verified by an independent entity. This is what the means objective ”ensure cyber risk management processes are audited” defends for the risk management practice and in case study A that procedure is enforced periodically with special attention by conducting internal and external audits in defined periods. The continuous monitorization and control is verified by independent entities to ensure adequate due care (Johnson, 2002; Straub and Welke, 1998).

The fundamental objective ”maximize accountability and responsibility for cyber risks”, detailed in Figure 6.3 is affected by the following means objectives: ”minimize risks related to IT service providers”, ”ensure identification of critical information” and ”maximize vetting of employees for cyber

risks". "Minimize risks related to IT service providers" is considered by respondents as the critical objective for maximizing accountability and responsibility. This mindset rises with the vast majority of projects being executed by external consultants with the accountability and responsibility for risks remaining in a gray area between both parties, sometimes due to misalignment of perceptions (Dhillon et al., 2016b). This problem has been minimized with security and cyber risk management requirements being included in contracts and service level agreements. An attacker might exploit a vulnerability in an IT service provider in order to affect multiple clients, including case study A or target the IT service provider to get access exclusively to case study A (Salmela, 2008). "Ensure identification of critical information" is a baseline step in every organization to be able to prioritize security initiatives and in the case study A, a classification policy exists that determines the criticality of information (Appleyard, 2005; Peltier, 2013). This criticality is dealt with due diligence by the custodian of information, in this case the IT department, and controlled by the information owners, advised by the security department. The respondents pointed out that some departments follow the policy with more due care than others and in their opinion this different behavior relies on the risk awareness of the head of department. Being a public organization, the vetting of employees for cyber risks is enforced initially, by including in the process, the crime history report of the potential employee during the hiring process. There are non-disclosure clauses in the contract and the security policy is provided to the employee, but the respondents pointed out, that in the public administration employment process it is very difficult to fire or suspend an employee, even with sufficient evidences of non-compliance or deviant behavior. A process for misconduct is triggered, but the results lead, most of the times, to nothing in practice.

The fundamental objective "maximize cyber risk knowledge", detailed in Figure 6.4 is influenced by the means objectives: "develop cyber risk awareness program", "develop cyber risk management competencies" and "develop training program for cyber risk management". Cyber risk knowledge should be nurtured inside the organizational culture by empowering the employee to understand cyber risks (Karabacak and Ozkan, 2010; Spears and Barki, 2010; Veiga and Eloff, 2007, 2010). With the actual world context of lack of security and risk management trained human resources, the respondents pointed out the need to "develop cyber risk management competencies" as a high priority (AP2SI, 2016) . The chosen path of the analyzed organization on this point has been to develop these competencies internally with tutoring, but respondents also pointed out that they are thinking of partnering with some high educational institutions to increase competencies beyond the actual level by bringing additional knowledge from the outside of the organization. Most of the

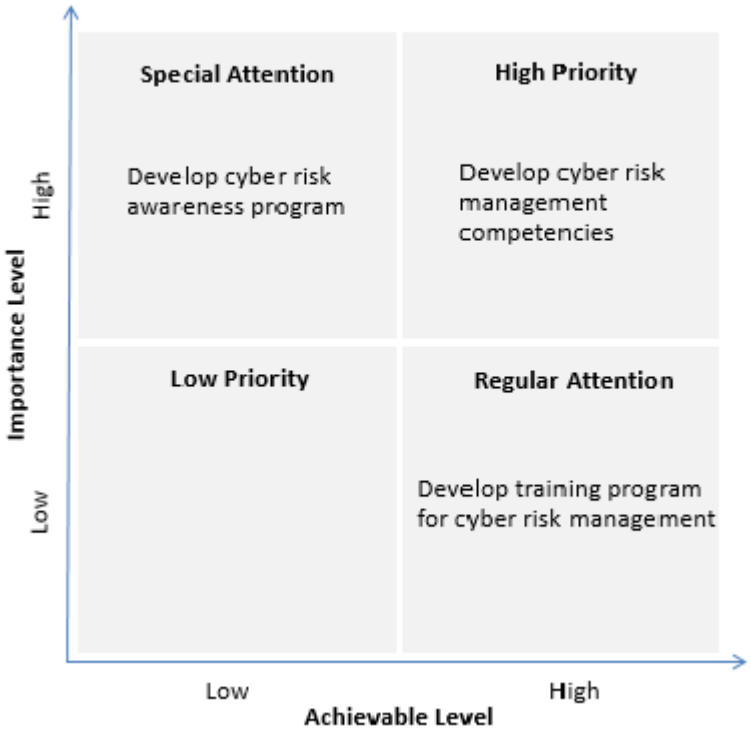

Figure 6.4: Maximize cyber risk knowledge

employees working in the security department are young in age and have higher education, but there's still a senior segment with lack of competencies. They also pointed out, that by being a public company, they are tied to the hiring practices of the public sector that pay below the average for specialized position such as security and risk management. They foresee that building solid competencies in this area will be a challenge for most public organizations and the solution will be relying in external consultants, managing the risks known by that approach. They have an ongoing awareness program that includes a risk module, but that program still doesn't reach all the employees and has been reformulated multiple times without being delivered completely, which may generate know-how gaps between employees that participated in the program at different times. That's why the cyber awareness objective needs special attention in the analyzed case study, to mitigate the weakest link in security, namely the human behind the technology (Drevin et al., 2006; Furnell and Thomson, 2009; Reid and Niekerk, 2014; Siponen, 2001, 2000).

The means objective "develop training program for cyber risk management" is being dealt as effective as possible by the organization with budget restrictions. These restrictions hamper the

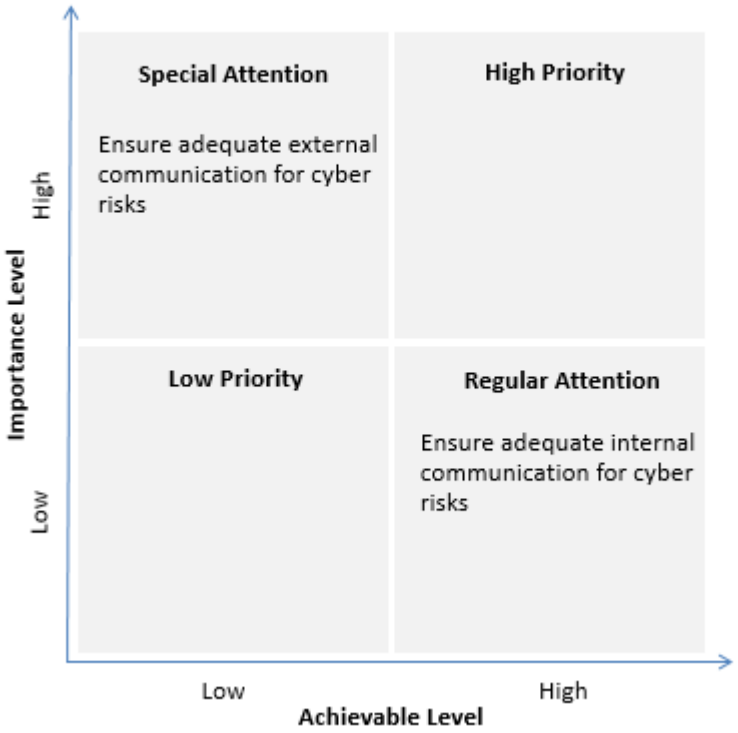

Figure 6.5: Ensure risk management governance

external training in specific specialized tasks due to the high cost by external training and certification organizations. Professional certifications are carried out by employees on their own. Being a large organization, this provides the possibility of internal training among employees to fulfil specific tasks. The updating of know-how is performed with informal training sessions available online or the participation in conferences of a specialized subject, but that updating is based on the employee's individual effort and interests.

The fundamental objective "ensure risk management governance", detailed in Figure 6.5 is influenced by "ensure adequate external communication for cyber risks" and "ensure adequate internal communication for cyber risks". "Ensure adequate internal communication for cyber risks" is enforced at the highest level regularly with the security committee that includes the directors from key areas such as internal audit or human resources, having the general director as chairman in the sessions. These sessions occur periodically and risk management reports are analyzed and consequent initiatives for risk mitigation are defined (ISACA, 2007). The internal organizational

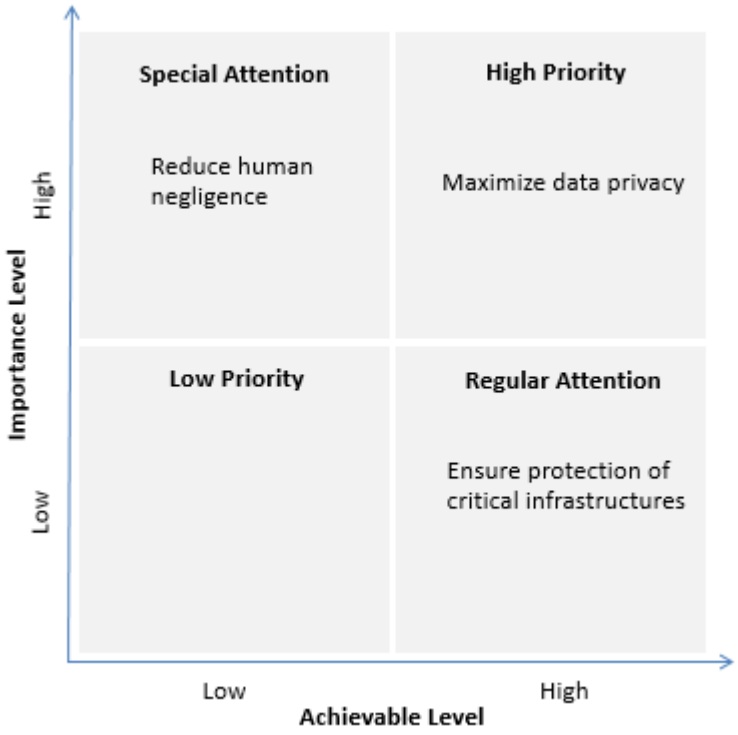

Figure 6.6: Maximize the protection of human life

communication of risks is also promoted within the awareness program by detailing the existing process for communicating risks and the contacts available to help on that subject. Communication is reinforced with the workflow application used in the case study, that has the necessary steps and makes the information flow across departments with defined deadlines for action.

”Ensure adequate external communication for cyber risks” has been a subject of special attention, because this organization is critical in the citizen’s context, with every news that is presented in the media affecting the trust in the public sector. Being an organization influenced by the government and other public partners, the external communication regarding cyber risks has to be clear and leave no space for misinterpretations. The business continuity program that the organization implemented helps on that matter with a formal policy that details who speaks with whom and when and what type of information should be transmitted to the media and other external parties (Saleem et al., 2008; Valackiene, 2015; Whitman et al., 2013).

The fundamental objective ”maximize the protection of human life”, as seen in Figure 6.6, deals with means objectives such as: ”reduce human negligence”, ”maximize data privacy, ”ensure the

protection of medical devices" or "ensure protection of critical infrastructures". "Ensure the protection of medical devices" is not applicable to this organization. "Reduce human negligence" has been a subject that needs special attention in the analyzed organization, as some employees have access to critical information that may harm citizens. The main remaining question has been the scope that should be followed in applying the least privilege principle, that dictates that employees should only have the access required to perform their duties. If a too strict application of the least privilege is applied, some employees will lose the flexibility necessary to fulfil their tasks in an adequate time frame to give quick answers to partners and citizens. If a too loose application of the principle happens, this might lead to negligence by accidentally accessing and changing information. Nonetheless, the least privilege principle is controlled additionally by following the separation of privileges or also called four eyes principle, where someone else controls that the access was legitimate (Backhouse and Dhillon, 1999; Saltzer and Schroeder, 1975). This organization maintains some critical infrastructures that may be a target for hacktivists, unfriendly nations and cyber crime. These perceived threats are known by the respondents and they point out that they do devote regular attention to protect their infrastructures. They have a business continuity program that was implemented taking into account that their infrastructures are critical.

"Maximize data privacy" is a central theme in Europe with the new general data protection regulation (EU, 2016). This regulation is mandatory for all organizations that process personal data from European citizens and enforces security requirements to deal with personal data. This includes non European union organizations that control or process personal information from European citizens. Organizations are obliged to report data breaches that affect personal data to supervision entities. This regulation includes the right to be forgotten and right to data portability principles that will have impact in the current processes of organizations. Right to be forgotten allows the user to request that his data is deleted and right to data portability allows the user to ask for his information in a standard format to be able to migrate to a different service provider. This need for standardization among data formats will require an additional effort from organizations. Two other principles of this regulation are privacy by design, with privacy requirements being implemented in the initial system design, and privacy by default, in which a system applies privacy mechanisms by default and the user has the option to opt-out. The regulation mandates the creation of a new business function: the data protection officer. This individual will be accountable for the data protection in the organization. This function is mandatory for the public sector and the analyzed organization is evaluating all the necessary efforts to accommodate the new business function. The regulation

follows the mindset of a risk based approach for privacy, by proposing as requirements the need to perform privacy impact assessments. Privacy impact assessments identify risks to privacy rights and prioritize them based on the probability and impact, following the common approach used in risk assessment and in business impact analysis. This allows the recommendation of risk mitigation controls to ensure the protection of personal data. These privacy impact assessments occur before processing personal data and when major changes to the processes dealing with that data are performed.

6.4 Principles

This section identifies key principles for cyber risk management, taking into account the enunciated objectives from subject matter experts in the field, the weighting agreed in the decision model and lessons learned from the risk management strategy captured in the case study. These principles serve as a baseline for organizations to improve their cyber risk management practices. These principles integrate people, processes and technology in an organizational environment (Kiely and Benzel, 2006).

To establish a cyber risk management strategy in an organization, we should first establish its structure. Top management should see this topic as critical and devote adequate commitment and support (ISACA, 2007). This topic has struggled to find his path into the board room, but nowadays, with permanent security breaches in the news, customers and partners demand greater security levels and consequently force this topic into the top management's agenda. Create the risk management function and fit that function within the hierarchy with adequate transparency and independence. Establish the internal communication channels within the organization. Establish the reporting path to top management for the new established function and define formal communication paths to departments (Valackiene, 2015). Decisions should be taken taking into account the interests from stakeholders, so it's critical to create a risk committee to discuss and decide risk mitigation initiatives in a timely manner. This function will also define the policies for communication with partners and media. The processes for cyber risk management should be integrated within the existing business processes, namely the enterprise risk management framework (Chatzipoulidis et al., 2010; Fakhri et al., 2015). This ensures that all critical processes will be part of cyber risk assessments. Taking into account this context, the following Principle 1 for cyber risk management is formed:

Risk governance shall be supported by top management with established communication channels and integrated within business processes.

One task common to all risk management strategies is the periodical assessment of risk. This risk assessment is dependent on the definition of the criticality of information. Resources are finite, so we should focus risk mitigation in the information, which is critical for business. Information classification helps on that matter, by establishing different levels of information criticality and defining control mechanisms applied to each type of information (Appleyard, 2005; Peltier, 2013). Information classification should be considered as a critical input for risk assessments (Johnson et al., 2009). Risk affects an information asset, taking into account the existing threats, the probability of the attack's success and its impact to the organization. Threat analysis or threat modelling is the second step in a risk assessment, as threats are not equal to each type of information. Having the multiple threats affecting each information asset, what is the probability of a successful attack? That probability is difficult to estimate with the desired accuracy, but we can gather information based on world reports and organizational attack history. The final step is the estimation of the impact on business, taking into account that the attack was successful. Business impact analysis reports, that are requisites for business continuity and disaster recovery, can provide us an initial help, although they are mostly focused in information availability. This impact is collected in workshops with the business owners. Principle 2 is stated as:

Critical information shall be continuously identified and monitored, along with the existing threats, their probability and impact.

Defining who does what and when has to be defined to ensure the success of cyber risk management. Using RACI charts is a common way to define Responsibility and Accountability, along with the need to be Consulted and Informed of actions (ISACA, 2007). Defining owners for risks ensure that no gray areas of responsibility occur. These owners are responsible for accepting residual risk and if that risk is not acceptable, define risk treatment measures. Common ownership of risks often fall under responsibility of the head of department. Middle management positions, such as head of department, are known to have a heterogeneous perception of risk very dependent on the each individual own risk perception (Johnson and Goetz, 2007). This uniformization of risk perception has to be initially levelled and monitored. The risk perception has to reach top management and the risk management topic has to find its way into the board's agenda, making top management accountable for a lack of proactive risk management approach (Ezingeard et al., 2004). The most common risk treatment measure is the mitigation of risk with the implementation

of security controls. Policies should be known and followed by employees and external parties. The formal process of binding a entity to the compliance of a policy should be mandatory (Herath and Rao, 2009; Höne and Eloff, 2002; Palmer et al., 2001). The same mindset should be applied to non-disclosure agreements. Risk and security requirements, in the form of extra clauses, should be defined in IT service contracts to establish adequate responsibility of third parties, as globalization and outsourcing continues to increase. This leads to Principle 3:

Responsibility and accountability for cyber risks shall be ensured by establishing ownership, binding policies and formalizing requirements.

When analyzing cyber risks we take as basis the confidentiality, integrity and availability of information (Chowdhuri and Dhillon, 2012). These three factors affect the status of the information, being it processed, communicated or stored (McCumber, 2004). Who is granted access to it and when, is the role of authentication and authorization, with adequate access control mechanisms that also permit auditability (Housley and Aboba, 2007). So, Principle 4 is:

Security shall be obtained by preserving the information confidentiality, integrity and availability and adequate access control.

Focusing on people's behavior is crucial, when changing processes and applying new control mechanisms. Most people have a natural way of resisting to changes and that behavior should be dealt with adequate attention (Ward and Daniel, 2006). Using a positive approach, beyond strictly binding policies, by explaining the need to change is a step towards success (Spears and Barki, 2010). The clarification of new processes and why they are needed is the role of awareness programs, in which employees and external parties recognize the normal expected behavior and learn how to spot deviant behavior in scenario situations (Siponen, 2001, 2000). Training programs teach how to perform certain tasks. Employees should be subjected to training programs to augment their competences and be recognized internally with the desired skills. Awareness programs to all employees and training program forming subject matter experts are the path to be able to form an organizational culture that embraces cyber risk management practices (Furnell and Thomson, 2009). Consequently this creates the necessary cyber risk knowledge, so Principle 5 is obtained:

Cyber risk knowledge shall increase with the implementation of awareness and training programs that reinforce competencies and nurture a risk management organizational culture.

Compliance is a known way to force organizations to act in due care to deal with known risks in our society (ISACA, 2014; ITGI, 2007; Von Solms and von Solms, 2006). Following the current

legal framework and answer to the requirements of supervisory entities has to be seen as expected ethical practice. This need to control allows to establish clear frames around existing cyber risks by measuring their compliance using accepted metrics (Brotby, 2009; Brotby and Hinson, 2013). The transparency and independence principles of compliance are assured with adequate auditing practices to current risk management processes (Straub and Welke, 1998). The continuous auditing can be assured by an internal auditing team that provides support to an external auditing team that evaluates the risk status periodically. This mindset leads to Principle 6:

Compliance shall be obtained by satisfying legal and regulatory supervisory requirements with adequate measurement and auditing.

There's no doubt that human life should be preserved at all costs. With the rise of the cyber domain, we are witnessing that malicious actions that should have been contained within that domain, are having repercussions outside of that domain and harming individuals in their daily life (Baskerville and Portougal, 2003; Von Solms and Van Niekerk, 2013). Nation states are also being targeted inside the cyber domain for information warfare and intelligence gathering. The rise of computing power and the digital footprint, brought additional risks related to privacy such as profiling (Son and Kim, 2008). Data breaches happen all the time with sensitive information being exposed from users and organizations. Malicious behaviours such as bullying and stalking that were clearly identified and monitored in our world, have migrated into a new domain were that control is lacking (Dhillon et al., 2016a). Finally Principle 7 is:

Human life shall be preserved by ensuring protection from malicious cyber practices that have consequences in the physical world.

Table 6.1 summarizes the multiple activities for each principle that should be taken into account as critical success factors in the definition and implementation of the strategy (Rockart, 1978). This allows organizations to establish the roadmap of activities for cyber risk management focusing in the critical areas and being able to establish risk profiles taking into account their industry requirements. These critical success factors can be subjected to benchmarking for cyber risk management practices and can lead to the implementation of maturity models to evaluate cyber risk management processes such as ISO 15504 or CMMI (Barafort et al., 2006; CMMI, 2010; ISO, 2004).

Some of those factors may not be directly applied in organizations taking into account their industry or business sector. For example the critical success factor "Identify and protect medical e-health devices" will be critical in the health industry, but negligent in the banking sector. Similarly in another example, the critical success factor "Identify and protect critical infrastructures" applies to our case

Principle	Critical success factors	Literature Support
P1	-Ensure top management commitment -Establish a risk committee -Define internal organizational communication policies -Define external communication policies -Integrate cyber risk management within the enterprise risk management framework	Chatzipoulidis et al. (2010); Fakhri et al. (2015); ISACA (2007); Valackiene (2015)
P2	-Establish a process to identify and monitor critical information -Establish a process to evaluate current information threats, their probability and impact	Appleyard (2005); Johnson et al. (2009); Peltier (2013)
P3	-Define responsibility and accountability in contracts with IT providers -Establish clear ownership for identified cyber risks -Bind employees and enternal consultants to non-disclosure agreements -Bind employees and external consultants to existing security policies	Ezingeard et al. (2004); Herath and Rao (2009); Höne and Eloff (2002); ISACA (2007); Johnson and Goetz (2007); Palmer et al. (2001)
P4	-Preserve the confidentiality, integrity and availability of information -Implement and monitor access control mechanisms according to identity management policies -Establish configuration baselines for the IT infrastructure and monitor their compliance	Chowdhuri and Dhillon (2012); Housley and Aboba (2007); McCumber (2004)
P5	-Establish an awareness program that includes all employees and external consultants -Develop a training program to form solid competencies in cyber risk management -Nurture a cyber risk management organizational culture	Furnell and Thomson (2009); Siponen (2001, 2000); Spears and Barki (2010); Ward and Daniel (2006)
P6	-Develop and monitor cyber risk metrics -Establish periodical auditing of cyber risk management process to ensure continuous improvement -Implement and monitor the compliance of requirements from supervisory entities -Implement and monitor the compliance from current legislation	Brotby (2009); Brotby and Hinson (2013); ISACA (2014); ITGI (2007); Straub and Welke (1998); Von Solms and von Solms (2006)
P7	-Enable control mechanisms to minimize human negligence -Make data privacy protection an organizational theme with adequate controls -Identify and protect critical infrastructures -Identify and protect medical e-health devices -Prevent cyberstalking and cyberbullying	Baskerville and Portougal (2003); Dhillon et al. (2016a); Son and Kim (2008); Von Solms and Van Niekerk (2013)

Table 6.1: Critical success factors for cyber risk management

study being a public organization, safeguarding citizen's critical information, but it does not apply directly to the retail industry.

The positioning of the cyber risk management means objectives within each fundamental objective and defining their importance and achievable level allows case study A to develop priorities and form a clear path for developing their cyber risk strategy. Based on that knowledge gathered within the case study, rooted in research literature and discussed with security specialists, we develop cyber risk management principles that help other organizations to define their risk management strategy. Those cyber risk management principles are sustained by specific critical success factors that help to implement each of the principles in organizations. The critical success factors embrace 3 main areas that should be changed together: technology, processes and people.

6.5 Conclusion

In this chapter we present the cyber risk management strategy of a chosen case study. The strategy is formed taking into account the importance and achievable level of the means objectives to fulfil the fundamental objectives for cyber risk management. This provides alignment with the defined business strategy of the chosen case study, as the respondents position those objectives based on their opinion and relate with the case study context. Principles for cyber risk management are presented based on the results of the cyber risk management strategy from the case study, cyber risk decision model and defined cyber risk management objectives. These principles are supported by the literature and critical success factors to accomplish the principles are also provided to guide organizations in the definition of their cyber risk management strategy.

Chapter 7

Risk benefits management

"Opportunities multiply as they are seized."

—Sun Tzu, the Art of War

7.1 Introduction

In the previous chapters we have defined objectives for cyber risk management, presented a model for decision making towards cyber risk management and used that mindset to define a strategy to be adapted by organizations for cyber risk management. This chapter goes a step further by detailing how can that strategy be controlled to ensure that the benefits derived from the investment objectives, that were the basis for the decision process, are realized during execution, following the benefits management approach from Ward and Daniel (2006, 2012). This approach ensures that the decisions and actions taken during the investment implementation will lead to the realization of the identified business benefits. It surpasses the common situation of the overstating of benefits in the business case to force approval of an investment, with a solid plan that details initiatives and the change management necessary to realize those benefits. This overstating of benefits leads to projects that cannot be successful and consequently risk management and the necessary security investment to mitigate risk are seen by top management as costs, that should be minimized and do not bring added value to the organization.

The monitoring of the investment or project should not only focus in efficiency by implementing the solution with optimized time, resources and cost, but also ensure that the effectiveness is accomplished with the realization of benefits for business. The benefits management approach can be aligned with different project management methodologies (Karamitsos et al., 2010).

If security investments are decided taking into account the decision model according to a risk management strategy, the risk management objectives detailed in the value focused thinking approach should be included as investment objectives in the benefits management approach. The investment objectives paint the desired picture if the project is successful, but benefits may or may not be realized by the company, even if the security project is delivered on time and optimizing costs. That's why business changes are necessary and change enablers should be triggered to promote an internal need to change. These investments in information security for risk mitigation should not be viewed solely in a technical perspective as an enabler, but also take into account organizational, structural, behavioral and social aspects for business benefits realization (Dhillon, 2004). Moreover, Peppard and Ward (2004) explain that: "Strategic management is about making informed choices based on an understanding of both the relative benefits of different options and the organization's ability to deliver those benefits".

7.2 Case study

The organization analyzed for risk benefits management in this chapter is the same Case A used in the previous chapter. The existence of multiple security investments along with a defined risk management strategy makes that organization the perfect case for analysis. Furthermore along that mindset, is the context of the organization with the explicit due care for risk management, detailed in their business strategy as a priority to be ensured. The pursuit of an external certification for the existing information security management system reinforces the need to evaluate, if the security investments are bringing the necessary benefits to the business.

Risk management guides the overall vision that prioritizes the investments according to defined risks, based on the objectives of stakeholders and taking into account the critical business information. Taking into account this mindset, cyber risk management can be classified as strategic effort in the analyzed organization. That strategic position of cyber risk management can be explained with the importance of the theme in the current business activities and the continuing vital importance

of the theme in the future activities of the organization (McFarlan and McKenney, 1983; Ward and Daniel, 2006).

The unit of analysis is the organization as a whole, focusing on benefits of security investments to mitigate cyber risk. The sources of information are interviews, analysis of public and confidential information in the form of documents and direct observation by the researcher. The respondent profile is top and middle management, most of them, more related to information security and information technology. In the benefits management analysis there were 12 interviews across multiple departments to capture the global sentiment of the organization. The interview process follows a script with open questions that allow respondents to reflect on past experiences and transmit the context of the organization within their responses. This context allows to capture the information with more granularity, being able to notice typical interactions concerning the theme in the analyzed organization.

7.2.1 Interview script

The interview script for benefits management includes open questions that allow interviewees to reflect on the organization context and speak freely about their experiences.

1. What is your current business role?
2. What is your professional background?
3. What do you understand of the term “Benefits Management”?
4. Do you have a portfolio of security investments?
5. What are the main security investments in your organization?
6. Who’s involved in the investment decision making process?
7. What are the business drivers that enable new security investments? (PESTEL)
8. Project Selection. Please describe me this project.
9. What is your role in this project?
10. What are the main objectives of this project?
11. What are the business benefits of this project?

12. Are the project stakeholders identified?
13. How are the stakeholders involved?
14. Is there an organizational change management process?
15. Are there any tasks that promote the need to change?
16. What were the major business changes in the project? (DoingNewThings, DoingThingsBetter, StopDoingThings)
17. What were the inhibitors during the project? How were they solved?
18. What are the lessons learned from this investment? Good and bad news.

7.3 Benefits management

The research process started by analyzing existing business drivers that were the trigger for the investment in risk management safeguards. The next step is to gather the investment objectives from stakeholders, taking into account the previously analyzed business drivers. One step outside of the traditional benefits management process was to look back to the value focused thinking process and analyze if any of the elicited objectives was not included in the means or fundamental objectives. Despite some different wordings and afterwards clarification of the meaning of some proposed objectives by participants, there was no new objective that falled outside of the previous collected objectives based on values seen in Figure 4.1. If the objectives are accomplished, what will the business benefits be? What is the value increase for business with this investment? That's the next question in the process, finding out each business benefit according to different stakeholders involved directly or indirectly in the investment. New or adapted IT applications are put in place to support the risk management process, and triggers, or enablers, that force organizational changes are implemented. The last and perhaps most difficult part in the process is the recognition of stakeholders, including specifically the employees, that ongoing business changes need to materialize in order to realize benefits. This collection of business changes is more difficult to implement, as some employees do not see the changes happening or simply try to stay outside of the business change management path. The documentation analyzed in the case study helped a lot in this part, as some mandatory changes were explicitly written there. As the benefits started to solidify with the ongoing project, other benefits, that remained hidden in the first place, started to

be noticed by employees. Risk management not only permits the realization of benefits, but more than that, it ensures that hidden disbenefits that harm business do not materialize or happen with controlled minimum impact.

7.3.1 Business drivers

The business drivers establish the need to invest in order to change the business for the better, taking into account business factors such as competitive advantage for example. They exist whether the decision to invest is taken or not. The business drivers can be internal or external and can be identified in a SWOT or PESTEL analysis for example (Ward and Peppard, 2002). These drivers are tied to the business strategy of the organization. The relation between investments objectives for risk management derived from the value focused thinking approach and business drivers is present in Figure 7.1.

In our research one business driver is e-government. UN (2016) argues that e-government improves the relationship between people and the government, by making public services accessible and responsive to the population needs. This improved relationship enhances the transparency and accountability of public services. E-government also contributes to bridge the digital divide or gap, by integrating people with less knowledge in technological areas. With the focus of the Portuguese government in e-government initiatives that promote the contact with the citizen and organizations via online services offered in the Internet, it became clear that these services brought additional risks. Moreover, the exchange of critical digital information between multiple government services raises the risk of information misuse and the aggregation of information increases traceability. These risks have to be mitigated with risk management investments, that deploy additional security controls.

The simplification of citizen processes, named simplex program, brought additional risks with the direct access to critical information and the ability to request and perform actions on that information. The need to simplify processes and maintain operational excellence with the adequate quality of service is a requisite of the simplex program. For the common citizen and organizations this brings clear benefits by being able to access information without having to travel to the citizen's service office, but to the organization providing that service, it has to ensure that the threats to that information are minimized. The threat surface increases dramatically from having access to an information system inside the citizen's service office, to the access of such a system online in the

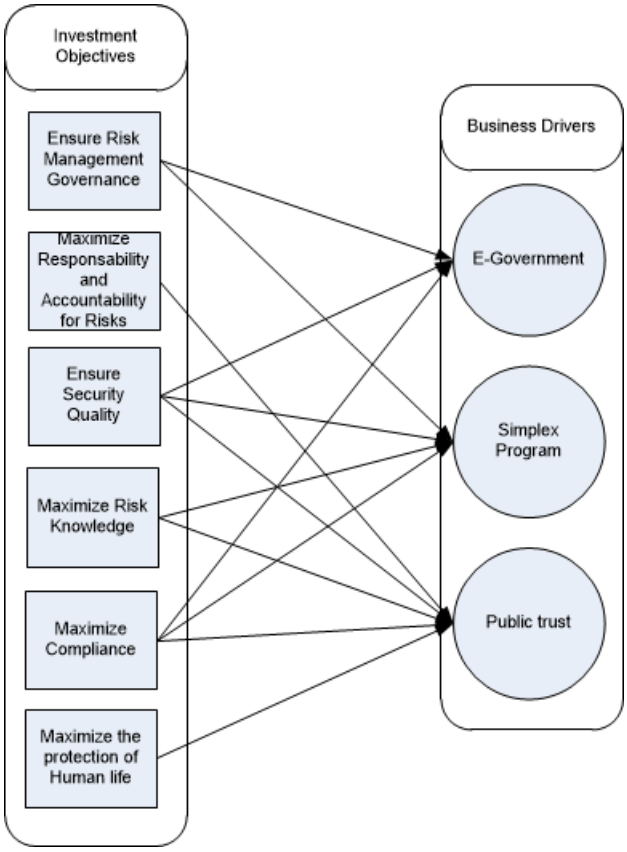

Figure 7.1: Business drivers for risk management investments

Internet, as anyone in the world might try to attack it.

Being a public service, the massive disclose or tampering of that critical information poses the threat of state or nation secrets being disclosed and the nation reputation is consequently affected. The trust in public service and the consequent trust in the nation state has to be preserved.

7.3.2 Business benefits

This subsection enumerates the business benefits realized in the case study. The business benefits can be mapped into the different perspectives of the Business Scorecard (Kaplan and Norton, 1996): financial, customer, learning and growing and internal business processes. When used in this context, business scorecard is transformed into a benefits scorecard (Melton et al., 2011).

This organization deals with critical information from the all citizens and organizations in Portugal, so the protection of business information is a clear intangible benefit. This benefit ensures the protection of nation secrets and the information of each organization and citizen. It contributes for

the maintenance of law and eases civil unrest. Regarding the business scorecard perspective the major focus is enhancing the internal business processes to protect critical business information. An IT subdirector explained:*"Sensitive information is our core business, all employees had a module in an e-learning awareness program last month focused just on that topic."*

Trusted as having information due care will maintain the good reputation of the organization among all citizens and all organizations. Trust is a critical factor that contributes to the use of online services (Lacohée et al., 2006). This benefit is centered on the external perception of clients, that deposit critical information on the hands of this organization that acts as a custodian, according to the government laws. The information should be consulted and used only for the defined purposes in which it was collected, ensuring privacy. It contributes for the maintenance of law and eases civil unrest. Regarding the business scorecard perspectives this benefit deals with the perception of costumers. An interviewed IT subdirector noted: *"Our organization has been an example of citizen's trust in the public sector."*

Access to online services eases the load of face to face contacts from citizens and organizations, via the multiple citizen's service offices across the country, and they can consult and modify information during non-working times. This will lead to optimization of operational resources and will generate cost savings. Multiple operations regarding logistics are also performed online, which simplifies the process for organizations and provides centralized control necessary for business operations agility with adequate validation and dependability. This benefits influences the financial and costumer perspectives of the business scorecard. An IT subdirector explained: *"Our clients, the citizens, are not used anymore to wait on queues to access physically our services, they do it online when they want to."*

Ensure compliance will limit the sanctions or fines from supervisors and cases going to courts by claims of citizens and organizations. This benefit will lead to the optimization of legal resources and will generate cost savings. This benefit influences the financial factor of the business scorecard, the learning and growing by gaining knowledge of the compliance requirements and the refinement of the internal business processes to respond to compliance requirements. The CISO explained: *"We are taking the necessary precautions to analyze the compliance requirements of the new General Data Protection Regulation."*

Auditability of performed actions is necessary to monitor and prove to employees, citizens and organizations that the designated information was consulted or altered. It ensures the principle of transparency to the public, by detailing what the action is, when is was made , by whom and from

which device. This auditability allows correlation of events to relate with other incidents and be subjected to automatic fraud detection with the use of big data fraud analysis mechanisms. This benefit is part of the internal business processes perspective of the business scorecard. A technical manager explained: *"Having to justify an access to critical information, is a deterrent control that triggers the mindset in the employee that the monitorization of accesses is put in place."*

7.3.3 Business changes

The organizational business changes are the main catalysts for business benefits to be realized, as they change business processes and models, create new governance and control structures and shape behaviors.

The establishment of the security committee, that meets regularly to analyze risk assessment reports and monitors security initiatives, empowers the risk management strategy by showing support from top management (Vermeulen and Von Solms, 2002). The security committee gathers multiple members from top management across different areas to have a global view of information security inside the organization. Performing risk assessments on a periodical basis also contributes to maximize benefits, as the reports are analyzed by top management and security controls are implemented to mitigate the risk. The implementation of defined controls is monitored using a follow-up approach with defined ownership, milestones and deadlines.

New projects must include security requirements to be ensured throughout the project, according to detected risks and the information security team is involved from the beginning following the classical System Development Lifecycle approach.

Security policies are put in place and reviewed at least annually taking into account the business context and the existence of new requirements. They are distributed to employees and periodical security awareness sessions occur. The policies ensure the support of top management and detail the importance of risk management, business continuity, security awareness, responsibility and accountability, promote the communication regarding security issues, keep the balance between security and usability and control the access to sensitive information. This balance between usability and security is a critical factor in the adoption of security by humans (Furnell, 2005; Saltzer and Schroeder, 1975). Best practices are created and made available to citizens and organizations concerning information security to mitigate risks. External consultants are also binded to the security policies detailed by clauses in service agreements or project contracts. These external consultants

also participate in security awareness sessions.

Risk management and security processes are aligned with best practices and existing standards to ensure the organization maintains the adequate security maturity. This also ensures that the organization is able to pursue new or maintain existing security certifications. Security professionals receive external training on new standards and best practices and apply that knowledge afterwards on the field.

7.3.4 Change enablers

Enabling changes are initiatives that foment the desire to change the status quo within the organization. These are normally characterized by training sessions, definition of measures or definition of new roles.

External audits motivate business changes, because the external auditors bring an independent and critical vision to the organization. That vision of the status quo (AS-IS) and desired future state (TO-BE) elicit multiple recommendations to minimize the gap between those two states. That gap is transformed into a roadmap of activities, some of them transformed into projects, that enhance the maturity of the organization and promote necessary changes. External audits have the ability to benchmark similar organizations and classify them with maturity models that allow them to know which domains to improve to be classified a step higher in the maturity stairway.

Awareness campaigns focus on changing the mindset of the common employee, so that he can spot risky behaviours that may bring harm to the organization. These campaigns are the formal contact and discussion of existing security policies and procedures. They detail the formal communication channels and expected behaviour, when some risks are detected or materialize. Awareness is a major step to the creation of an internal security culture, that projects trust to the citizen. Understanding why changes are necessary, eases the resistance from employees to accept changes in current processes. An IT director explained:*"After an awareness training ends, we see a shift in the employee behavior, starting to see the point in security control. That does not last forever, but at least there's a change."*

Security training focuses not on the common employee, but on specific risk management or security functions. This training teaches professionals how to do a specific task, for example how to adequate develop security policies to be accepted by employees. Some of this training, normally provided by external entities, includes a certification with the passing of a test and certifies

that the professional has the necessary know-how to perform a specific designed task or function. Training prepares not only employees to implement prevention and detection controls, but also prepares them to respond to security incidents, according to the defined practices while acting under pressure.

This organization has a strategic performance indicator for information security in the strategic plan, the presence of information security in the strategic plan shows evidence of top management support and motivates employees to achieve the desired result. This commitment of top management is a critical success factor in order to achieve necessary business changes (Vermeulen and Von Solms, 2002).

An IT manager explained: *"Putting an indicator for information security in a written form in the strategic plan, shows the clear commitment of top management on this topic, things will have to change."*

The organization is in the process of certification for its Information Security Management System following the ISO 27001 standard. This certification process sets the pace for necessary changes in risk management and information security practices throughout the organization. The broad scope of the standard with its multiple domains forces significant business changes for organizations wishing to be certified. The standard introduces requirements dependent on top management with adequate governance structures and it goes down to the technical level with requirements for security operations for example.

Although multiple change enablers or facilitators exist, there are a number of inhibitors, that will influence negatively the business changes (Coombs, 2015). These inhibitors should also be identified to be avoided or minimized and their status monitored. A strong resistance to change is present in all organizations of the public sector and although considered a source of innovation in the public sector, this organization is not different in its basis. Some employees worked in the analyzed organization all their lifes and have done some tasks in their own way. These changes will take time to solidify and become integrated within the organizational culture. Some changes may need some renewal of mindsets with some employees being retired and new employees coming in. The continuous maintenance of external audits should be dealt with adequate attention, by changing the pool or company of external auditors that provide a different point of view from the previous auditors. The same auditors should not audit the same scope repeatedly. Limited budget may also hamper external audits as the periodicity of the audits may be widened. Pursuing an initial certification for an Information Security Management System according to ISO 27001 provides a boost

to change, but after successful certification some organizations may lower efforts until the time of the renewal of the certification, this is a point that should be taken into account, as it affects negatively some business benefits. Awareness campaigns should be continuously updated with new material taking into account new risks and security training should monitor the needed capabilities of resources and include new training needs and certifications in the training plan for employees.

7.3.5 IT Enablers

Information technology supports and enables business changes across organizations. It increases the performance of traditional business process, creates new models of business and stops legacy behaviors. IT on its own does not provide business benefits, if the necessary organizational changes do not happen.

The risk management application allows for monitoring assets and their risk level. This application allows for reports of the current risk status and is able to adapt these reports to specific compliance formats. The information from risk assessments is updated in this application.

The vulnerability management application allows for continuous security testing of defined assets in an intrusion testing approach. It is supported by an external group of ethical hackers that uses that application to report new vulnerabilities identified. As the CISO noted: *"The traceability inside the application eases my daily work".*

The workflow application follows change management practices in an ITIL approach. It reports actions necessary to correct vulnerabilities across departments and the implementation of additional security controls to mitigate risk, functioning as the formal communication channel with adequate auditability and history. It allows the easy follow up of the status of each initiative.

Multiple IT security applications enforce technical controls to ensure risk minimization. Common applications are anti-virus, firewall, intrusion detection systems, access control management, public key infrastructure or log monitorization for example. These applications are responsible to implement the recommended controls defined by the policies and standards across the existing information systems, as most information is stored and processed by them. Information is protected according to the defined levels and associated controls introduced in the data classification process. An IT subdirector stated: *"We are beginning to enforce network access control (NAC) across all buildings."*

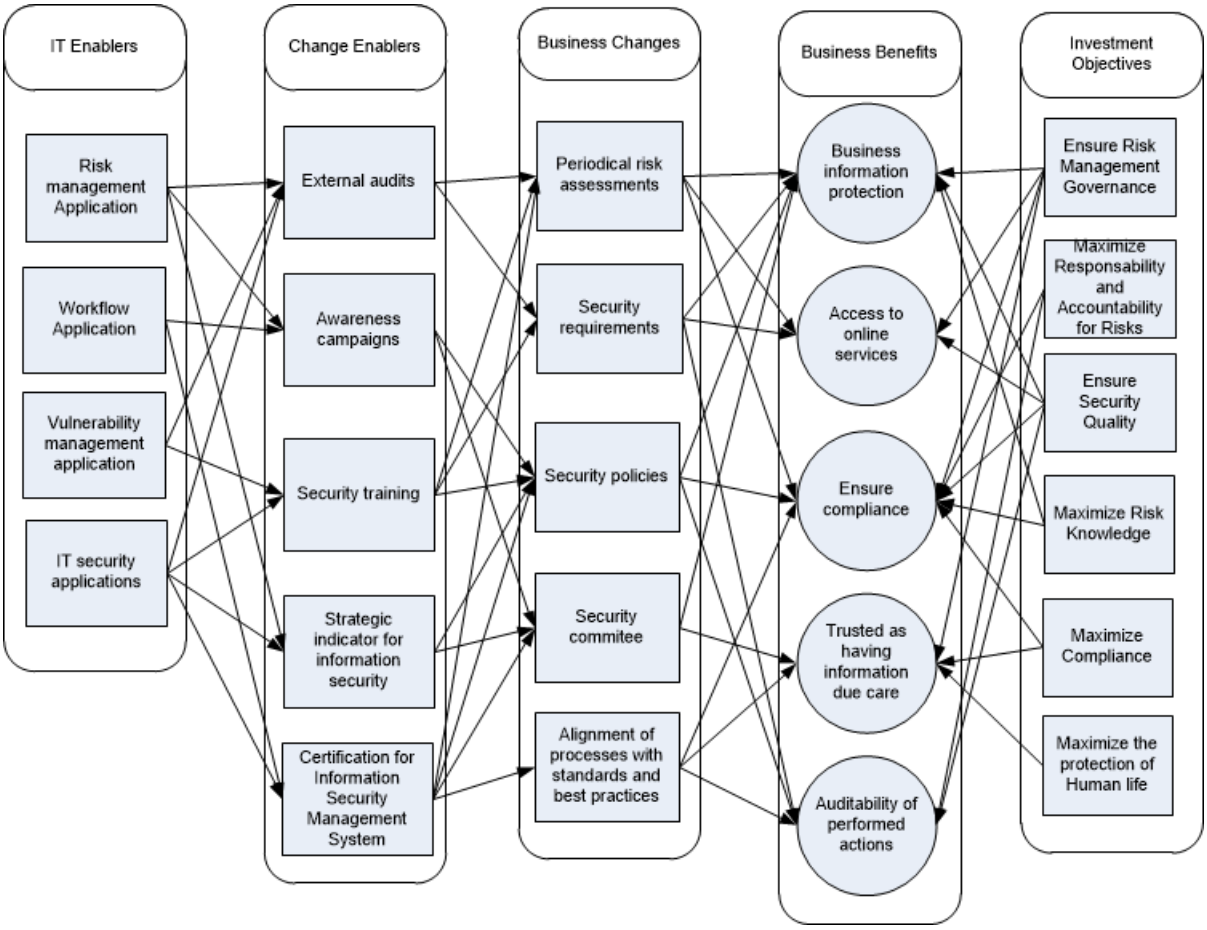

Figure 7.2: Benefits dependency network

7.3.6 Benefits dependency network

The benefits dependency network present in Figure 7.2 details the relationship among previously detailed objects. The analysis of the network begins with detailing the investment objectives. The investment permits the realization of business benefits. For those business benefits to be maximized, they have to be supported by information technology enablers. IT on its own does not provide immediate benefits, business changes have to happen. Enablers for business changes have to trigger the organizational desire to change. After the business implements the desired changes, it is possible to observe the business benefits of the chosen investment.

Hidden benefits not initially identified may also be realized. These are the benefits that are not obvious in the first place when the project begins, but start to be noticed as the project reaches a maturity state. Risk management investments are known to improve communication acting as a common language between management and technical professionals. The initial training required

Business Benefits	Benefit owner
Business information protection	Managing director
Access to online services	IT Director
Ensure compliance	Internal audit director
Trusted as having information due care	Communication and marketing director
Auditability of performed actions	Internal audit director

Table 7.1: Ownership of benefits

and the know-how gained with such complex processes will provide the necessary basis for new specialized profiles of employees to grow. These processes are formal in nature and require that adequate documentation is put in place. Technical professionals tend to leave the documentation in a low priority, so this investment will enhance the level of documentation of information systems supported by the documentation of policies and the alignment of processes with standards and best practices.

7.3.7 Ownership

Establishing clear ownership of each of the item in the benefits dependency network is a critical step towards the maximization of the desired benefits. Active involvement, rather than passively seeing the project being implemented, is also achieved by establishing ownership. Most of the times the owner of the change is not the owner of the benefits, so the change does not occur as planned and the benefit is not realized. When this situation of distinct ownership happens, it's important to establish a adequate cooperation between these two parties to ensure that the owner of the change is really committed to establish change and involved also in the benefit for the organization. Those parties will try to establish a win-win relationship. These owners should be senior level staff with adequate power to make things happen. Operational staff should be involved from the beginning participating and giving feedback to the project team, as some of these projects may be implemented by external consultants. The common feeling of operational staff that the project is being implemented by an external team for them should be minimized as possible. Operational staff and project members should not be designated as owners of initiatives. In case of external suppliers or partners responsible for the project, a project risk sharing approach can be setup to identify penalties in case that the benefits are not realized.

The benefit owners and change owners are detailed in Tables 7.1 and 7.2.

Business Changes	Change owner
Periodical risk assessments	Security director
Security requirements	Security director
Security Policies	Human resources director
Security Committee	Managing Director
Alignment of processes with standards and best practices	Security director

Table 7.2: Ownership of changes

7.3.8 Measuring benefits

As it can be seen in Table 7.3, this case study risk management seeks to improve how things are done in a continuous improvement cycle. We are not analyzing a new system, but seeking to minimize the risk from already existing services. New services will include security requirements to mitigate known baseline risks and will be subjected to risk assessments to identify and evaluate new risks. Ensure compliance can be measured in a financial manner, with the valuation of monetary losses due to fines or sanctions applied by supervisory entities. Capital reserves due to risks of non-compliance can be mandatory for organizations. Trusted as having information due care can be captured by including questions on this matter in citizens and organizations targeted surveys. Protect business information can be measured with metrics such as: number of successful security incident responses, number of attacks detected, number of risks with mitigation actions completed. Auditability of performed actions can be measured in a positive manner with number of performed legitimate actions monitored or in a negative manner with number of illegitimate actions detected. This measure will be collected automatically by logging systems and due to high number of actions, a sample of those actions will be verified manually by auditors periodically. Access to online services focuses on business continuity practices, having defined metrics such as Recovery time objective (RTO) and Recovery point objective (RPO) in case of disasters for example. Other metrics related with availability can be tied to service management practices with formal service level agreements.

7.4 Discussion

This section discusses the risk management benefits, relating with the necessary risk mitigation security investments and existing literature. The integration of the value focused thinking and benefits management approaches as a consolidated framework is also discussed.

Degree of explicitness	Do new things	Do things better	Stop doing things
Financial		-Ensure compliance Measure target: 0 euros loss per year in fines	
Quantifiable		-Access to online services Measure target: 99,999% availability per year	
Measurable		-Auditability of performed actions Measure target: 0 illegitimate actions detected per year -Protect business information Measure target: 0 risks with no mitigation actions per year -Trusted as having information due care Measure target: satisfied or 4 in a 5 Likert scale from yearly survey	
Observable			

Table 7.3: Benefits classification

Ensure compliance is a key benefit for all stakeholders of a modern organization, as organizations should be aligned with the current legal obligations and mandatory standards from supervision entities. This benefit also influences the trust in the organization with the existence of public reports of compliance. Compliance requirements will tend to increase due to the globalization of business and prepared organizations with established compliance practices will be able to differentiate themselves from other with less mature compliance practices.

Access to online services should be ensured by the organization, to ease the burden of citizen's offices face to face meetings. The benefit gained with the simplification of the process with the online access given to the their clients, also decreases the support of calls to the helpdesk services. The services are supported with online help menus and frequently asked questions. Every technology has a learning curve and resistance to the use of online services is perceived (Davis, 1989), in this case, from the older slice of the population. Online access to services allows for flexibility of accessing time and also promotes mobility, enhancing the opinion of the client regarding a service that he is forced to use by the government.

Auditability of performed actions ensures transparency and accountability. These monitored actions are focused on clients, as they may access and change data in online services, and also on employees, that should only access and change data according to their professional duties. This

traceability allows for quick clarification of misunderstandings regarding existing submitted data and the actions performed on it. This enhances the organizational agility, when law enforcement and other supervision entities need access to these traceable records.

Business information protection supports the argument that information is a source of competitive advantage (Porter and Millar, 1985). This is not critical in the case of the analyzed case study, as this public organization functions in a monopolization environment in Portugal. Nonetheless, all organizations deposit critical business information in the custody of this organization, and if that information is leaked, it may limit or damage their competitive advantage. This public organization also has specific processes in their business area that influence the competitiveness of the country in the globalized world. This organization has an information classification process in place according to the Portuguese SEGNAC security levels for previously classified data or the data will labelled confidential, internal or public, if not previously classified. The information owners define the classification level and custodians will protect the information based on that level. The auditing of the assurance of the information classification process is provided by the security department.

Trusted as having information due care ensures the well being of the country, because this organization stores critical information from citizens and organizations. Moreover, as Von Solms and von Solms (2006) state: ”Information has grown to become the lifeblood of many organizations today”. It is mandatory by law to supply critical business information from citizens and organizations to the analyzed organization and if this organization is not perceived as trustworthy, it would cause serious problems in the daily life of citizens, organizations and, in the end, the normal operations of the country. Negligence in information due care should not happen, as it might trigger lawsuits, generate civil unrest and cause massive damage to citizens and organizations.

It can be seen by the information presented in this chapter that the benefits management approach allows organizations to maximize the business benefits from security investments to mitigate cyber risk. It changes the traditional project management practice to focus not only in efficiency with the optimization of resources, cost and time, but also in effectiveness by identifying and controlling the business benefits that should be realized with the security investment. This benefits management approach was not conducted formally in the chosen organization with the focus staying within the traditional project management approach to achieve efficiency. Being able to include benefits management in the business case, simplifies the selling of the project to top management and obtains the top management commitment during the project implementation. This commitment is vital to be able to trigger the organizational desire to change and to be able to conduct the necessary

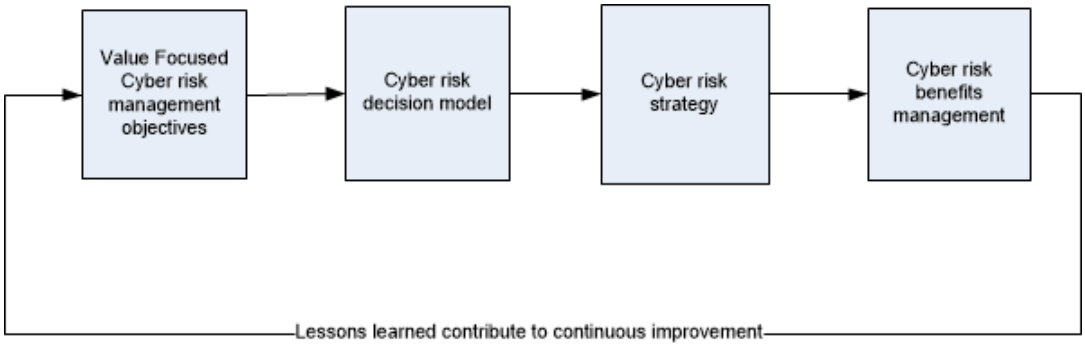

Figure 7.3: Cyber risk management lifecycle

business changes to maximize benefits.

Throughout this work the participants of the analyzed organization recognized the value of the benefits management approach in security investments, but some of them confessed that they think that this approach would not be implemented in future projects due to the lack of internal knowledge and because most of the new projects are managed by external project managers that use their own organizational project management practices.

Value focus thinking (Keeney, 1992) and benefits management theories (Ward and Daniel, 2006) fit almost seamlessly together, as they complement each other. Value focused theory and the presented decision model allow to decide on the best solution to mitigate risk among multiple alternatives, while taking into account the values from stakeholders. Value focused thinking is centered on decision making. Benefits management is used afterwards after the selection of the alternative, when detailing the benefits that should be realized, based on the value focused objectives of the investment. Benefits management is centered on project management. Benefits management allows for planning the benefits before the project starts and monitoring the benefits during project execution, with adequate attention to business change management.

The lessons-learned phase of the benefits management process allows the creation of continuous improvement cycle both for benefits management, already included in the traditional benefits management process, and also to refine the cyber risk management objectives gathered with value focused thinking. With the refinement of the objectives it is possible to improve the cyber risk decision model and further align the cyber risk strategy to current organizational needs. The cyber risk strategy uses the risk decision model to evaluate new required security investments and the benefits management approach ensures that the business benefits from that investments are actually realized. That cyber risk management lifecycle can be seen in Figure 7.3.

7.5 Conclusion

This chapter presents the benefits management of security investments to mitigate cyber risks in a chosen case study. It details the business drivers aligned with investment objetives that consider the implementation of security investments to mitigate cyber risk. Business benefits that are planned to be realized with the investments are identified. Business benefits from investments cannot be realized without the implementation of business changes. These business changes are triggered by IT and change enablers that are also detailed in this research. The interaction across these multiple objects is detailed in the benefits dependency network and clear ownership and measures are defined for those objects.

The integration of value focused thinking and benefits management is proven to be of added value due to the complementarity of both approaches. This allows to close the cyber risk management lifecycle that begins with the definition of cyber security objectives based on the values of stakeholders, followed by the use of those objectives in a cyber risk decision model. Those objectives simplify the definition of a cyber risk management strategy rooted in cyber risk principles. Based on that strategy, the implementation of security investments to mitigate risk allow the maximization of desired business benefits, using the planning and monitorization practices of the benefits management approach.

Chapter 8

Conclusions

"The supreme art of war is to subdue the enemy without fighting."

—Sun Tzu, the Art of War

8.1 Overview

This thesis analyzes the full lifecycle of cyber risk management. It details objectives for risk mitigation grounded by stakeholders values. These objectives are used in a decision model to evaluate alternatives for security investments. Using the objectives and the basis of the decision model the cyber risk management strategy of an organization is evaluated in a case study approach. Using the lessons learned from the gathering of objectives, from the workshops to form the decision model and from the case study, principles for cyber risk management are developed. Finally, after a decision to invest in security controls is taken based on a defined cyber risk management strategy, there's the need to control and realize business benefits from that security investment. A cyber risk benefits management analysis is performed in the same case study environment, to evaluate the benefits from security investments with the ultimate goal of risk mitigation.

Going back to the initial research questions, the first question ”What are the objectives based on values for cyber risk management decision making?” is answered with the gathering of those values in the form of objectives. These values are divided into means and fundamental objectives to achieve risk mitigation. These values are refined and used throughout the whole research to

develop a decision model for cyber risk management, as input to form the cyber risk management strategy and as investment objectives to evaluate the benefits from security investments.

The second research question is ”How do those objectives influence a cyber risk management strategy?”. This question is answered within a case study where the researcher asks participants to prioritize the means objectives taking into account the maximization of the achievement from the fundamental objective. Based on the lessons learned from the creation of a cyber risk strategy within the case study, this research proposes cyber risk principles that help organizations to develop a cyber risk management strategy.

The third research question is ”How can an organization maximize the benefits from security investments to mitigate cyber risks?”. This is the focus of the last part of the research, relating the cyber risk management objectives gathered using value focused thinking into the benefits management approach. Using these risk objectives in benefits management as investment objectives makes absolute sense, because risk management is the practice understood by top management that is able to generate security investments. It can be seen in the analyzed case study that guiding security investments with risk management values from stakeholders, allows for organizations to maximize business benefits, as long as adequate changes are implemented. These changes are supported by technology and enabled by changing triggers that foment the organizational desire to change. This benefits management approach allows to control the realization of benefits from security investments, namely also intangible benefits, that economic practices such as the evaluation of ROSI lack of, by focusing uniquely on costs.

It can be seen by this research that adequate cyber risk management practices, simplify the manager’s decision making process to justify security investments and also contribute to the realization of business benefits with the solid monitorization of the implementation of those investments. Cyber risk management is positioned as a common language between the technical jargon of information security and the business, simplifying the understanding of important security issues in current organizations to top management.

8.2 Research contributions

One important step in any research is the contribution to enhance the body of knowledge in a certain field, in this case, cyber risk management and the multiple domains of information security.

This section details theoretical, practical and methodological contributions across those domains of knowledge.

8.2.1 Theoretical contributions

This research is focused on two baseline theories: value focused thinking and benefits managements. These theories are applied for the first time in the context of cyber risk management to evaluate security investments. First, the research revises the multiple areas in literature with real examples where these theories were previously used.

The research integrates both theories in a consolidated cycle that starts with the collection of values to create risk objectives using value focused thinking, provides the theoretical relationships between those objectives, uses those objectives in the creation of a decision model based on real scenarios, defines principles for the creation of a cyber risk strategy and finally closes the cycle with the use of benefits management theory to evaluate the benefits of the implementation of security investments to mitigate risk. These investments follow the cyber risk management objectives that were the basis for the decision process in the first place.

To mitigate an existing knowledge gap, the objectives for cyber risk management are theoretically grounded with the support of the literature, developed empirically from multiple sources and tested in workshops and within a case study.

8.2.2 Methodological contributions

From a methodological point of view, this research is grounded in qualitative research. It uses interviews, workshops, direct observation and document analysis as sources of information. It combines and discusses different points of view under the theme of cyber risk management both from experts in the field and other participants with different knowledge. By capturing data from different time frames, it allows to notice the evolution of the subject under analysis.

This research provides an extensive literature review of cyber risk management and evaluation of security investments to mitigate risk. It details current research gaps and provides a way forward to improve knowledge in the the fields of cyber risk management and information security.

8.2.3 Practical contributions

This research provides cyber risk managements objectives, grounded on stakeholders values, to minimize cyber risk. Finding out what real stakeholders value in cyber risk management is a new contribution to the existing knowledge gap regarding this uncharted topic. These objectives entail not only a technical point of view, but also focus on managerial organizational issues captured into formal and informal controls. These objectives are segmented by their relationship into fundamental and means objectives.

Based on those objectives, a decision model for cyber risk management is developed. The justification of security investments to mitigate risk is always a difficult battle, as these investments may seem useless without no tangible value to the business, according to some sceptical stakeholders. By using this decision model based on values, the decision maker can justify the investments to stakeholders, as the basis for the investment was their elicited values in the first place. This simplifies the decision process in cyber risk management, as it tends to increase in complexity with the progress of the technology dependency in organizations.

The decision model was created taking into account different scenarios that detail the application of cyber risk objectives across real practical situations. These scenarios allow for decision makers to see the real consequences of different weights across chosen objectives and their impact on the practical context of organizations.

This research presents cyber risk management principles that can be used as a baseline for the development of a cyber risk strategy for organizations. In a world where cyber threats are increasing, every organization should have a strategy to minimize risk and prioritize security investments. The means objectives used to maximize the achievement of fundamental objectives are positioned in a strategic grid to guide the strategic development for cyber risk.

This research provides a benefits management approach for cyber risk management investments. After the decision process based on strategy occurs, there's the need to evaluate if the initial benefits, that drove the investment, are actually realized during project execution. Following this mindset, we evaluate the business benefits that are realized in security investments to mitigate cyber risk.

This research also raises cyber risk awareness of still neglected areas in enterprises and the current society. These areas have evolved dramatically in the last years, without adequate attention from top management and some segments of society, due to their complexity and due to their preventive context. This preventive context that ensures business as usual remains unnoticed until a

serious risk causes harm to the organization. Cyber risk management bridges the communication between the technical jargon of information security and business, simplifying the management's understanding of complex concepts.

8.3 Research limitations

The enumeration of limitations foments the inner reflexion of the constrained results by the researcher as a continuous improvement cycle and allows to frame the themes for further future research.

First of all, information security and cyber risks are sensitive topics in organizations. Some organizations prefer to stay in their black-boxes with security by obscurity instead of opening the door to researchers in these areas. The researcher had serious problems in locating and gaining access to a useful case study. Some organizations denied access upfront, by stating that these topics cannot be discussed with external individuals, although the organization would be anonymized and a non disclosure agreement would be signed by the researcher. Other organizations forwarded the research participation request to top management and the answer did not arrive, even after multiple contacts. Some organizations that opened the door to participate in the research showed a very low maturity in these areas, that after some initial interviews, the researcher decided that those organizations will not provide sufficient added value to the research. Those organizations do not have risk management practices and are starting to take their first steps in the IT security field. Other organizations that agreed to participate, had serious problems with the availability of individuals to be interviewed or limited the access to internal documents on these topics, in those cases the researcher opted to leave those organizations out of the study, due to the lack of access to critical information.

Recording the interviews was also a limitation, some interviewees refused to have the interview recorded. Others were absolutely participative, until the researcher asked if the interview could be recorded. They agreed feeling constrained, but the information collected lacked examples and context during recording. After the recording stopped, these type of interviewees gave the needed context and examples. These topics under analysis are sensitive and after careful analysis by the researcher after some initial interviews, he opted to finish recordings and concentrate on taking as much notes as possible. This change in approach proved to be successful in capturing contextual details, that otherwise would not have been captured with the recording enabled.

Gathering specialists on information security and cyber risks together in one room to conduct workshops was very difficult, as some confirmed individuals did not appear on the last minute. From those that participated in the workshops, the feedback arising from the discussion of the topic was good and the time frame was respected. The sample from the interviews and workshops may not be representative of all business sectors or industries, with some industries being represented with a bigger slice.

This research uses an unique case study with a very specific context inside the Portuguese public administration. Although the cyber risk objectives and the cyber risk decision model had participants from other industries, the practical applicability to develop a cyber risk strategy and the evaluation of security investments to mitigate cyber risk was applied in that specific case-study.

The results of this study are not directly generalizable, if applied in other organizational contexts. They are not generalizable in the statistical sense, but they are generalizable to theory (Yin, 2003). Theory based and empirically grounded research cannot be generalizable directly to other contexts (Lee and Baskerville, 2003).

Another limitation is the introduction of the researcher's bias in the process. Bringing preconceived ideas and previous experience, while capturing and analyzing captured information is inevitable, although the researcher tried to minimize that flaw consciously. The research involved as participants in the study, following a purposive sample, individuals with knowledge about the referred topics, but it is possible that their understanding does not reflect the current status quo.

8.4 Future research

From this thesis, multiple future research paths arise. The first is to extend the applicability of cyber risk management objectives, as a basis for a risk strategy, in other business sectors or industries. The evaluation of benefits of security investments can also be applied in the future to other industries.

The development of all the value functions and the addition of other measures to evaluate the objectives can be a path of future research regarding the cyber risk management decision model. Analyzing the variances of the weights given to the cyber risk objectives in the decision model across multiple industries, to find out specific cyber risk management weighting criteria for each industry or business sector, can also be a path for further research. Performing the same analysis

in different countries and comparing the results will also enhance this research. Another path, is using different weighting techniques, like for example AHP, instead of the swing method to weight cyber risk management objectives in the decision model and compare the results.

Further validation of the cyber risk management objectives across larger samples, using surveys instead of interviews, can also be a future direction for research. Comparing the values in the form of cyber risk objectives, captured from employees of an organization versus the values of third parties that work or indirectly influence that organization can also be a path for further research.

Apply the benefits management approach, based on these cyber risk management objectives, to larger security programs in multiple organizations.

Evaluate the cyber risk management principles, as a basis to form a cyber risk strategy, in other organizations in the same or different countries.

Test the integration of the value-focused thinking theory together with the benefits management theory across other fields of study, to form the continuous improvement cycle from the decision making process to the realization of business benefits from the chosen investments.

Bibliography

Aagedal, J., F. den Braber, T. Dimitrakos, B. Gran, D. Raptis, and K. Stolen: 2002, 'Model-based risk assessment to improve enterprise security'. In: *Proceedings Sixth International Enterprise Distributed Object Computing Conference, EDOC '02.* pp. 51 – 62.

Acquisti, A., A. Friedman, and R. Telang: 2006, 'Is there a cost to privacy breaches? An event study.'. In: *Workshop on the Economics of Information Security (WEIS)*.

Ahlemann, F., F. Hesselmann, J. Braun, and K. Mohan: 2013, 'Exploiting Is/It Projects' Potential-Towards A Design Theory For Benefits Management'. *European Conference of Information Systems* (Paper 210).

Albakri, S. H., B. Shanmugam, G. N. Samy, N. B. Idris, and A. Ahmed: 2014, 'Security risk assessment framework for cloud computing environments'. *Security and Communication Networks* **7**(11), 2114–2124.

Albert, C. and A. J. Dorofee: 2001, 'Octave criteria, version 2.0'. *Software Engineering Institute, Carnegie Mellon University*.

Alberts, C., A. Dorofee, J. Stevens, and C. Woody: 2003, 'Introduction to the OCTAVE Approach'. *Pittsburgh, PA, Software Engineering Institute, Carnegie Mellon University*.

Alberts, C., A. Dorofee, J. Stevens, and C. Woody: 2005, 'OCTAVE-S Implementation Guide, Version 1'. Technical report, CMU/SEI-2004-HB-003, ADA453304). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

Alberts, C. J. and A. Dorofee: 2002, *Managing information security risks: the OCTAVE approach*. Addison-Wesley Longman Publishing Co., Inc.

Alcalde, B., E. Dubois, S. Mauw, N. Mayer, and S. Radomirović: 2009, 'Towards a decision model

based on trust and security risk management'. In: *Proceedings of the Seventh Australasian Conference on Information Security-Volume 98*. pp. 61–70.

Almeida, J. C. P. and M. J. Romão: 2010, 'Benefits Management For an E-Invoice Process'. *Portuguese Journal of Management Studies* **15**(2).

Alshawi, S., Z. Irani, and L. Baldwin: 2003, 'Benchmarking information technology investment and benefits extraction'. *Benchmarking: An International Journal* **10**(4), 414–423.

Amancei, C.: 2011, 'Practical methods for information security risk management'. *Informatica Economica* **15**(1), 151.

Ansoff, H. I.: 1987, 'The emerging paradigm of strategic behavior'. *Strategic Management Journal* **8**(6), 501–515.

AP2SI: 2016, '1º Inquérito Aberto à Segurança da Informação nas Instituições em Portugal'. AP2SI.

Appleyard, J.: 2005, 'Information Classification: A Corporate Implementation Guide'. *HF Tipton, & M. Krause, Information Security Management Handbook*.

Ashurst, C. and N. Doherty: 2014, 'Benefits-Led IT: Building The Organisational Capability–A Longitudinal Perspective'. *UK Academy for Information Systems Conference Proceedings*.

Ashurst, C. and N. F. Doherty: 2003, 'Towards the formulation of a best practice framework for benefits realisation in IT projects'. *Electronic Journal of Information Systems Evaluation* **6**(2), 1–10.

Ashurst, C., N. F. Doherty, and J. Peppard: 2008, 'Improving the impact of IT development projects: the benefits realization capability model'. *European Journal of Information Systems* **17**(4), 352–370.

Averill, J. D., R. D. Peacock, R. L. Keeney, and P. D. Gallagher: 2009, *Rethinking egress: A vision for the future*, Vol. Technical Note 1647. US Department of Commerce, National Institute of Standards and Technology.

Backhouse, J. and G. Dhillon: 1999, 'Working towards Principles for Information Security Management in the 21st Century'. *The LSE Computer Security Research Centre*.

Bandyopadhyay, K., P. P. Mykytyn, and K. Mykytyn: 1999, 'A framework for integrated risk management in information technology'. *Management Decision* **37**(5), 437–445.

Barafort, B., J.-P. Humbert, and S. Poggi: 2006, 'Information Security Management and ISO/IEC 15504: the link opportunity between Security and Quality'. In: *SPICE Conference, Luxembourg*, Vol. 140.

Barclay, C. and D. Logan: 2013, 'Towards an Understanding of the Implementation & Adoption of Massive Online Open Courses (MOOCs) in a Developing Economy Context'. *Proceedings of SIG GlobDev Sixth Annual Workshop, Milano, Italy*.

Barclay, C. and K.-M. Osei-Bryson: 2008, 'The project objectives measurement model (POMM): An alternative view to information systems project measurement'. *Electronic Journal of Information Systems Evaluation* **11**(3), 139–154.

Barclay, C. and K.-M. Osei-Bryson: 2009, 'Determining the contribution of IS projects: an approach to measure performance'. In: *42nd Hawaii International Conference on System Sciences, HICSS'09.* pp. 1–10.

Barney, J. B.: 2001, 'Resource-based theories of competitive advantage: A ten-year retrospective on the resource-based view'. *Journal of management* **27**(6), 643–650.

Barrese, J. and N. Scordis: 2003, 'Corporate risk management'. *Review of Business* **24**(3), 26–30.

Barzilay, M.: 2013, 'A simple definition of cybersecurity'. ISACA.

Baskerville, R.: 1991, 'Risk analysis: an interpretive feasibility tool in justifying information systems security'. *European Journal of Information Systems* **1**(2), 121–130.

Baskerville, R.: 1993, 'Information systems security design methods: implications for information systems development'. *ACM Computing Surveys (CSUR)* **25**(4), 375–414.

Baskerville, R. L. and V. Portougal: 2003, 'A possibility theory framework for security evaluation in national infrastructure protection'. *Journal of Database Management (JDM)* **14**(2), 1–13.

Beckers, K., M. Heisel, B. Solhaug, and K. Stølen: 2014, 'ISMS-CORAS: A structured method for establishing an ISO 27001 compliant information security management system'. In: *Engineering Secure Future Internet Services and Systems*. Springer, pp. 315–344.

Beebe, N. L. and V. S. Rao: 2010, 'Improving organizational information security strategy via meso-level application of situational crime prevention to the risk management process'. *Communications of the Association for Information Systems* **26**(1), 17.

Benbasat, I., D. K. Goldstein, and M. Mead: 1987, 'The case research strategy in studies of information systems.'. *MIS Quarterly* **11**(3).

Bharadwaj, A. S.: 2000, 'A resource-based perspective on information technology capability and firm performance: an empirical investigation'. *MIS Quarterly* pp. 169–196.

Bhaskar, R.: 1978, *A Realist Theory of Science*. Sussex, UK: Harvester Press, second edition.

Bistarelli, S., F. Fioravanti, and P. Peretti: 2006, 'Defense trees for economic evaluation of security investments'. In: *Proceedings of the The First International Conference on Availability, Reliability and Security, ARES 2006, The International Dependability Conference - Bridging Theory and Practice, April 20-22 2006, Vienna University of Technology, Austria*. pp. 416–423, IEEE Computer Society.

Blakley, B., E. McDermott, and D. Geer: 2001, 'Information security is information risk management'. In: *Proceedings of the 2001 workshop on New security paradigms*. pp. 97–104.

Bodin, L. D., L. A. Gordon, and M. P. Loeb: 2005, 'Evaluating information security investments using the analytic hierarchy process'. *Communications ACM* **48**(2), 78–83.

Bodin, L. D., L. A. Gordon, and M. P. Loeb: 2008, 'Information security and risk management'. *Communications ACM* **51**(4), 64–68.

Böhme, R.: 2010, 'Security metrics and security investment models'. In: *International Workshop on Security*. pp. 10–24.

Böhme, R. and T. Nowey: 2008, 'Economic security metrics'. In: *Dependability metrics*. Springer, pp. 176–187.

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

Bojanc, R. and B. Jerman-Blažič: 2008b, 'Towards a standard approach for quantifying an ICT security investment'. *Computer Standards & Interfaces* **30**(4), 216–222.

Bojanc, R. and B. Jerman-Blažič: 2013, 'A quantitative model for information-security risk management'. *Engineering Management Journal* **25**(2), 25–37.

Bojanc, R., B. Jerman-Blažič, and M. Tekavčič: 2012, 'Managing the investment in information security technology by use of a quantitative modeling'. *Information Processing & Management* **48**(6), 1031–1052.

Bond, S. D., K. A. Carlson, and R. L. Keeney: 2008, 'Generating objectives: Can decision makers articulate what they want?'. *Management Science* **54**(1), 56–70.

Boote, D. N. and P. Beile: 2005, 'Scholars before researchers: On the centrality of the dissertation literature review in research preparation'. *Educational researcher* **34**(6), 3–15.

Bradley, G.: 2010, *Benefit Realisation Management: A practical guide to achieving benefits through change*. Gower Publishing, Ltd.

Breese, R.: 2012, 'Benefits realisation management: Panacea or false dawn?'. *International Journal of Project Management* **30**(3), 341–351.

Brine, E. G.: 2012, 'Prioritizing Foreign Military Engagements: A Multi Objective Decision Analysis Using Value Focused Thinking'. Technical report, DTIC Document.

Brotby, W. K.: 2009, *Information security management metrics:A definitive guide to effective security monitoring and measurement*. CRC Press.

Brotby, W. K. and G. Hinson: 2013, *PRAGMATIC Security Metrics: Applying Metametrics to Information Security*. CRC Press.

Brothers, A. J., S. V. Mattigod, D. M. Strachan, G. H. Beeman, P. K. Kearns, A. Papa, and C. Monti: 2009, 'Resource-limited multiattribute value analysis of alternatives for immobilizing radioactive liquid process waste stored in Saluggia, Italy'. *Decision Analysis* **6**(2), 98–114.

Butler, S.: 2002, 'Security attribute evaluation method: a cost-benefit approach'. In: *Proceedings of the 24rd International Conference on Software Engineering, ICSE 2002.* pp. 232 –240.

Butler, S. A. and P. Fischbeck: 2001, 'Multi-Attribute Risk Assessment'. Technical report, Proceedings of Symposium on Requirements Engineering for Information Security.

Caldeira, M.: 2000, 'Critical Realism: A philosophical perspective for case study research in management studies'. *Episteme, Ano II* (5-6), 73–88.

Caldeira, M. and G. Dhillon: 2010, 'Are we really competent?: Assessing organizational ability in delivering IT benefits'. *Business Process Management Journal* **16**(1), 5–28.

Caldeira, M., A. Serrano, R. Quaresma, C. Pedron, and M. Romão: 2012, 'Information and communication technology adoption for business benefits: A case analysis of an integrated paperless system'. *International Journal of Information Management* **32**(2), 196–202.

Caldeira, M. M. and M. J. Romão: 2002, 'Estratégias de investigação em sistemas de informação organizacionais–a utilização de métodos qualitativos'. *Portuguese Journal of Management Studies* **7**(1), 77–97.

Caldeira, M. M. and J. M. Ward: 2003, 'Using resource-based theory to interpret the successful adoption and use of information systems and technology in manufacturing small and medium-sized enterprises'. *European journal of information systems* **12**(2), 127–141.

Campbell, K., L. A. Gordon, M. P. Loeb, and L. Zhou: 2003, 'The economic cost of publicly announced information security breaches: empirical evidence from the stock market'. *Journal of Computer Security* **11**(3), 431–448.

Cannon, D., D. Wheeldon, S. Taylor, and O. of Government Commerce UK: 2007, *ITIL:IT service management practices; ITIL v3 core publications Service operation*. The Stationery Office.

Caralli, R. A., J. F. Stevens, L. R. Young, and W. R. Wilson: 2007, 'Introducing octave allegro: Improving the information security risk assessment process'. Technical report, DTIC Document.

Catton, W. R.: 1954, 'Exploring Techniques for Measuring Human Values'. *American Sociological Review* **19**(1), 49–55.

Catton, W. R.: 1959, 'A theory of value'. *American Sociological Review* **24**(3), 310–317.

Cavusoglu, H., B. Mishra, and S. Raghunathan: 2004a, 'The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers'. *International Journal of Electronic Commerce* **9**(1), 70–104.

Cavusoglu, H., B. Mishra, and S. Raghunathan: 2004b, 'A model for evaluating IT security investments'. *Communications of the ACM* **47**(7), 87–92.

Cavusoglu, H., S. Raghunathan, and W. T. Yue: 2008, 'Decision-theoretic and game-theoretic approaches to IT security investment'. *Journal of Management Information Systems* **25**(2), 281–304.

Chai, S., M. Kim, and H. R. Rao: 2011, 'Firms' information security investment decisions: Stock market evidence of investors' behavior'. *Decision Support Systems* **50**(4), 651–661.

Chang, J. C.-J., G. Torkzadeh, and G. Dhillon: 2004, 'Re-examining the measurement models of success for internet commerce'. *Information Management* **41**(5), 577–584.

Chatzipoulidis, A., I. Mavridis, and T. Kargidis: 2010, 'Developing Strategic Perspectives for Enterprise Risk Management Towards Information Assurance'. In: *Proceedings of the 9th European Conference on Information Warfare and Security: ECIW2010*. p. 35.

Chen, P.-Y., G. Kataria, and R. Krishnan: 2011, 'Correlated failures, diversification, and information security risk management'. *MIS Quarterly* **35**(2), 397–422.

Chivers, H.: 2006, 'Information modeling for automated risk analysis'. In: *Communications and Multimedia Security*. pp. 228–239.

Chivers, H., J. A. Clark, and P.-C. Cheng: 2009, 'Risk profiles and distributed risk assessment'. *Computers & Security* **28**(7), 521–535.

Chowdhuri, R. and G. Dhillon: 2012, 'Understanding Information Security.'. *Journal of Information System Security* **8**(2).

Chowdhury, M. J. M., R. Matulevičius, G. Sindre, and P. Karpati: 2012, 'Aligning mal-activity diagrams and security risk management for security requirements definitions'. In: *Requirements Engineering: Foundation for Software Quality*. Springer, pp. 132–139.

CMMI: 2010, 'Cmmi for development (cmmi-dev)'. Technical report, Version 1.3, Technical Report, CMU/SEI-2010-TR-033, Software Engineering Institute.

Coles, R. S. and R. Moulton: 2003, 'Operationalizing IT risk management'. *Computers & Security* **22**(6), 487–493.

Coombs, C. R.: 2015, 'When planned IS/IT project benefits are not realized: a study of inhibitors and facilitators to benefits realization'. *International Journal of Project Management* **33**(2), 363–379.

Coss, D. L., G. Dhillon, and I. Udeh: 2015, 'Strategic Planning Objectives for Venture Capitalist Investments in Emerging Information Technologies: A value-focused perspective'. *The Journal of Entrepreneurial Finance* **17**(1), 27–64.

Cremonini, M. and P. Martini: 2005, 'Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA).'. In: *Workshop on the Economics of Information Security*.

Czosseck, C., R. Ottis, and A.-M. Talihärm: 2013, 'Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security'. *Case Studies in Information Warfare and Security: For Researchers, Teachers and Students* **72**.

Daher, S. F. D., A. Cabral Seixas Costa, and A. Teixeira de Almeida: 2013, 'Assessing value-based objectives for developing business-IT strategies'. In: *Enterprise Systems Conference (ES)*. pp. 1–6.

Dai, W., Q. Zhu, C. Wang, and Y. Zeng: 2012, 'Risk Management Model of Information Security in IC Manufacturing Industry'. *Journal of Computers* **7**(2), 317.

Damianides, M.: 2005, 'Sarbanes-Oxley and IT governance: New guidance on IT control and compliance'. *Information Systems Management* **22**(1), 77–85.

Daneva, M.: 2006, 'Applying Real Options Thinking to Information Security in Networked Organizations'. Technical report, Centre for Telematics and Information Technology, University of Twente. Enschede, The Netherlands.

Darke, P., G. Shanks, and M. Broadbent: 1998, 'Successfully completing case study research: combining rigour, relevance and pragmatism'. *Information systems journal* **8**(4), 273–289.

Davis, F. D.: 1989, 'Perceived usefulness, perceived ease of use, and user acceptance of information technology'. *MIS Quarterly* pp. 319–340.

De Villiers, M.: 2005, 'Three approaches as pillars for interpretive information systems research: development research, action research and grounded theory'. In: *Proceedings of the 2005 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries*. pp. 142–151.

Dhillon, G.: 1995, 'Interpreting the management of information systems security'. Ph.D. thesis, The London School of Economics and Political Science (LSE).

Dhillon, G.: 2001, 'Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns'. *Computers & Security* **20**(2), 165–172.

Dhillon, G.: 2004, 'Realizing benefits of an information security program'. *Business Process Management Journal* **10**(3), 260.

Dhillon, G. and J. Backhouse: 2000, 'Information system security management in the new millennium'. *Communications of the ACM* **43**(7), 125–128.

Dhillon, G., J. Bardacino, and R. Hackney: 2002, 'Value Focused Assessment of Individual Privacy Concerns for Internet Commerce.'. In: *International Conference on Information Systems*. p. 67.

Dhillon, G., C. Challa, and K. Smith: 2016a, 'Defining Objectives for Preventing Cyberstalking'. In: *IFIP International Information Security and Privacy Conference*. pp. 76–87.

Dhillon, G. and R. Chowdhuri: 2013, 'Individual values for protecting identity in social networks'. *Thirty Fourth International Conference on Information Systems,Milan*.

Dhillon, G., R. Syed, and F. de Sá-Soares: 2016b, 'Information security concerns in IT outsourcing: Identifying (in) congruence between clients and vendors'. *Information & Management*.

Dhillon, G. and G. Torkzadeh: 2006, 'Value-focused assessment of information system security in organizations'. *Information Systems Journal* **16**(3), 293–314.

Dimopoulos, V., S. Furnell, M. Jennex, and I. Kritharas: 2004, 'Approaches to IT Security in Small and Medium Enterprises.'. In: *Australian Information Security Management (AISM)*.

Dioubate, B. M., A. Molok, N. Nuha, S. Talib, M. Tap, and A. Osman: 2015, 'Risk assessment model for organizational information security'. *ARPN Journal of Engineering and Applied Sciences* **10**(23), 17607–17613.

Dobbins, D. L.: 2015, 'Analysis of Security Concerns & Privacy Risks of Childrens Smart Toys'. *Telecommunications Management Summer*.

Doherty, N. F., C. Ashurst, and J. Peppard: 2012, 'Factors affecting the successful realisation of benefits from systems development projects: findings from three case studies'. *Journal of Information Technology* **27**(1), 1–16.

Doherty, N. F., N. Dudhal, C. Coombs, R. Summers, H. Vyas, M. Hepworth, and E. Kettle: 2008, 'Towards an Integrated Approach to Benefits Realisation Management–Reflections from the Development of a Clinical Trials Support System'. *Electronic Journal Information Systems Evaluation* **11**(2), 83–90.

Doherty, N. F. and H. Fulford: 2006, 'Aligning the information security policy with the strategic information systems plan'. *Computers & Security* **25**(1), 55–63.

Dowland, P., S. Furnell, H. Illingworth, and P. L. Reynolds: 1999, 'Computer crime and abuse: A survey of public attitudes and awareness'. *Computers & Security* **18**(8), 715–726.

Drevin, L., H. A. Kruger, and T. Steyn: 2006, 'Value-Focused Assessment of Information Communication and Technology Security Awareness in an Academic Environment'. In: S. Fischer-Hübner, K. Rannenberg, L. Yngström, and S. Lindskog (eds.): *Security and Privacy in Dynamic Environments, Proceedings of the IFIP TC-11 21st International Information Security Conference (SEC 2006), 22-24 May 2006, Karlstad, Sweden*, Vol. 201 of *IFIP*. pp. 448–453, Springer.

DSS, P.: 2016, 'Payment Card Industry Data Security Standard version 3.2'.

Duarte, B. P. and A. Reis: 2006, 'Developing a projects evaluation system based on multiple attribute value theory'. *Computers & operations research* **33**(5), 1488–1504.

Dubé, L. and G. Paré: 2003, 'Rigor in Information Systems Positivist Case Research: Current Practices, Trends, and Recommendations'. *MIS Quarterly* **27**(4), pp. 597–636.

Dubé, L. and G. Paré: 2001, 'Case research in information systems: current practices, trends, and recommendations'. *Cahier du GReSI no* **1**, 12.

Dubois, É., P. Heymans, N. Mayer, and R. Matulevičius: 2010, 'A systematic approach to define the domain of information system security risk management'. In: *Intentional Perspectives on Information Systems Engineering*. Springer, pp. 289–306.

Easton, G.: 2010, 'Critical realism in case study research'. *Industrial Marketing Management* **39**(1), 118–128.

Eisenhardt, K. M.: 1989, 'Building theories from case study research'. *Academy of management review* **14**(4), 532–550.

Eisenhardt, K. M. and M. E. Graebner: 2007, 'Theory building from cases: opportunities and challenges'. *Academy of management journal* **50**(1), 25–32.

Eloff, J., L. Labuschagne, and K. Badenhorst: 1993, 'A comparative framework for risk analysis methods'. *Computers & Security* **12**(6), 597 – 603.

EU: 2016, 'General Data Protection Regulation'. Official Journal of the European Union.

Ezingeard, J.-N., M. Bowen-Schrire, and D. Birchall: 2004, 'Triggers of change in information security management'. In: *ISOneWorld Conference, Las Vegas, NV*.

Fakhri, B., N. Fahimah, J. Ibrahim, et al.: 2015, 'Information security aligned to enterprise management'. *Middle East Journal of Business* **10**(1), 62–66.

Fang, F., M. Parameswaran, X. Zhao, and A. B. Whinston: 2014, 'An economic mechanism to manage operational security risks for inter-organizational information systems'. *Information Systems Frontiers* **16**(3), 399–416.

Farwell, J. P. and R. Rohozinski: 2011, 'Stuxnet and the future of cyber war'. *Survival* **53**(1), 23–40.

Feng, N. and X. Yu: 2012, 'A data-driven assessment model for information systems security risk management'. *Journal of Computers* **7**(12), 3103–3109.

Feng, N. and C. Zheng: 2014, 'A cooperative model for IS security risk management in distributed environment'. *The Scientific World Journal* **2014**.

Fenz, S. and A. Ekelhart: 2010, 'Verification, validation, and evaluation in information security risk management'. *IEEE Security & Privacy* (2), 58–65.

Fenz, S., A. Ekelhart, and T. Neubauer: 2011, 'Information Security Risk Management: In which security solutions is it worth investing?'. *Communications of the Association for Information Systems* **28**(1), 329–356.

Fischhoff, B., P. Slovic, and S. Lichtenstein: 1979, 'Weighing the Risks: Risks: Benefits which Risks are Acceptable?'. *Environment: Science and Policy for Sustainable Development* **21**(4), 17–38.

Fitzgerald, K. J.: 1995, 'Information security baselines'. *Information Management & Computer Security* **3**(2), 8–12.

Flick, U.: 2008, *Designing qualitative research*. Sage.

Fontana, A. and J. Frey: 1994, 'The art of science'. *The handbook of qualitative research* pp. 361–76.

Franqueira, V. N. L., S. H. Houmb, and M. Daneva: 2010, 'Using real option thinking to improve decision making in security investment'. In: *Proceedings of the 2010 international conference on On the move to meaningful internet systems - Volume Part I*. Berlin, Heidelberg, pp. 619–638, Springer-Verlag.

Furnell, S.: 2005, 'Why users cannot use security'. *Computers & Security* **24**(4), 274–279.

Furnell, S.: 2008, 'End-user security culture: a lesson that will never be learnt?'. *Computer Fraud & Security* **2008**(4), 6–9.

Furnell, S., P. Bryant, and A. D. Phippen: 2007, 'Assessing the security perceptions of personal Internet users'. *Computers & Security* **26**(5), 410–417.

Furnell, S. and N. Clarke: 2012, 'Power to the people? The evolving recognition of human aspects of security'. *Computers & Security* **31**(8), 983–988.

Furnell, S. and K.-L. Thomson: 2009, 'From culture to disobedience: Recognising the varying user acceptance of IT security'. *Computer Fraud & Security* **2009**(2), 5–10.

Fürstenau, D. and H. Rothe: 2014, 'Shadow IT systems: Discerning the good and the evil'.

Futcher, L. and R. von Solms: 2007, 'SecSDM: a model for integrating security into the software development life cycle'. In: *Fifth World Conference on Information Security Education*. pp. 41–48.

Futcher, L. and R. von Solms: 2013, 'A Risk-Based Approach to Formalise Information Security Requirements for Software Development'. In: *Information Assurance and Security Education and Training*. Springer, pp. 257–264.

Goel, S. and H. A. Shawky: 2009, 'Estimating the market impact of security breach announcements on firm values'. *Information & Management* **46**(7), 404–410.

Goettelmann, E., N. Mayer, and C. Godart: 2014, 'Integrating Security Risk Management into Business Process Management for the Cloud'. In: *IEEE 16th Conference on Business Informatics (CBI)*, Vol. 1. pp. 86–93.

Golden-Biddle, K. and K. Locke: 1993, 'Appealing work: An investigation of how ethnographic texts convince'. *Organization Science* **4**(4), 595–616.

Gomes, J., M. Romão, and M. Caldeira: 2013, 'The Benefits Management and Balanced Scorecard Strategy Map: How They Match'. *International Journal of IT Business Alignment and Governance* **4**(1), 44–54.

Gomes, J. and M. Romão: 2013, 'How benefits management helps balanced scorecard to deal with business dynamic environments'. *Tourism & Management Studies* **9**(1), 129–138.

Gomes, J. and M. Romão: 2014, 'Advantages and limitations of performance measurement tools: The Balanced Scorecard'. In: *7th IADIS Information Systems Conference (IS 2014) ISBN 978-989-8704-04-7*. pp. 19–26.

Gomes, J., M. Romão, H. Carvalho, and M. Caldeira: 2014, 'Organizational Maturity and Projects Performance: The Mediation of Benefits Management'. In: *10th International Conference on Web Information Systems and Technologies - Barcelona*. pp. 375–380.

Gordon, L. A. and M. P. Loeb: 2002a, 'The economics of information security investment'. *ACM Transactions on Information and System Security* **5**(4), 438–457.

Gordon, L. A. and M. P. Loeb: 2002b, 'Return on information security investments: Myths vs. Realities'. *Strategic Finance* **84**, 26–31.

Gordon, L. A. and M. P. Loeb: 2006, 'Budgeting process for information security expenditures'. *Communications ACM* **49**(1), 121–125.

Greenwell, R., X. Liu, and K. Chalmers: 2014, 'Benefits management of cloud computing investments.'. *International Journal of Advanced Computer Science and Applications (IJACSA)* **5**(6).

Gregory, R., J. Arvai, and T. McDaniels: 2001, 'Value-focused thinking for environmental risk consultations'. *Research in Social Problems and Public Policy* **9**, 249–273.

Gregory, R. and R. L. Keeney: 1994, 'Creating policy alternatives using stakeholder values'. *Management Science* **40**(8), 1035–1048.

Guba, E. G., Y. S. Lincoln, et al.: 1994, 'Competing paradigms in qualitative research'. *Handbook of qualitative research* **2**, 163–194.

Harris, S.: 2010, *CISSP all-in-one exam guide*. McGraw-Hill, Inc.

Henderson, J. C. and H. Venkatraman: 1993, 'Strategic alignment: Leveraging information technology for transforming organizations'. *IBM systems journal* **32**(1), 472–484.

Henrie, M.: 2013, 'Cyber Security Risk Management in the SCADA Critical Infrastructure Environment'. *Engineering Management Journal* **25**(2), 38–45.

Herath, T. and H. R. Rao: 2009, 'Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness'. *Decision Support Systems* **47**(2), 154–165.

Hirschheim, R.: 1985, 'Information systems epistemology: An historical perspective'. *Research methods in information systems* pp. 13–35.

Hirschheim, R., H. K. Klein, and K. Lyytinen: 1995, *Information systems development and data modeling: conceptual and philosophical foundations*. Cambridge University Press.

Höne, K. and J. H. P. Eloff: 2002, 'Information security policy: what do international information security standards say?'. *Computers & Security* **21**(5), 402–409.

Housley, R. and B. Aboba: 2007, 'Guidance for authentication, authorization, and accounting (AAA) key management'. Technical report.

Howard, R. A.: 2007, 'Advances in Decision Analysis, chap. 3: The Foundations of Decision Analysis Revisited'.

Howcroft, D. and E. M. Trauth: 2004, 'The choice of critical information systems research'. In: *Information Systems Research*. Springer, pp. 195–211.

Im, G. P. and R. L. Baskerville: 2005, 'A longitudinal study of information system threat categories: the enduring problem of human error'. *ACM SIGMIS Database* **36**(4), 68–79.

In, H. P., Y.-G. Kim, T. Lee, C.-J. Moon, Y. Jung, and I. Kim: 2005, 'A security risk analysis model for information systems'. In: *Proceedings of the Third Asian simulation conference on Systems Modeling and Simulation: theory and applications*. Berlin, Heidelberg, pp. 505–513, Springer-Verlag.

Irani, Z. and P. Love: 2013, *Evaluating Information Systems*. Taylor & Francis.

Irani, Z. and P. E. Love: 2001, 'The propagation of technology management taxonomies for evaluating investments in information systems'. *Journal of Management Information Systems* **17**(3), 161–178.

ISACA: 2007, 'Cobit Framework 4.1'. http://www.isaca.org.

ISACA: 2014, *IT Control Objectives for Sarbanes-Oxley: Using COBIT 5 in the Design and Implementation of Internal Controls Over Financial Reporting*. ISACA.

Ishiguro, M., H. Tanaka, K. Matsuura, and I. Murase: 2006, 'The effect of information security incidents on corporate values in the Japanese stock market'. In: *International Workshop on the Economics of Securing the Information Infrastructure (WESII)*.

ISO: 2004, 'ISO 15504-1: Information technology - Process assessment - Part 1 Concepts and vocabulary'.

ISO: 2009, '31000:2009 Risk management–Principles and guidelines'. *International Organization for Standardization, Geneva, Switzerland*.

ISO: 2011, 'ISO 27005: 2011 - Information technology–Security techniques–Information security risk management'.

ISO: 2012, 'ISO 27032: 2012 - Information technology–Security techniques–Guidelines for cybersecurity'.

ITGI: 2007, *IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance*. ISACA.

Johnson, C. N.: 2002, 'The benefits fo PDCA'. *Quality Progress* **35**(5), 120.

Johnson, G., K. Scholes, and R. Whittington: 2008, *Exploring corporate strategy: text & cases*. Pearson Education.

Johnson, M. E. and E. Goetz: 2007, 'Embedding information security into the organization'. *IEEE Security & Privacy* **5**(3).

Johnson, M. E., E. Goetz, and S. L. Pfleeger: 2009, 'Security through Information Risk Management.'. *IEEE Security & Privacy* **7**(3), 45–52.

Jonvik, T., B. Feng, I. Jorstad, et al.: 2008, 'Simple strong authentication for internet applications using mobile phones'. In: *IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference*. pp. 1–5.

Joshi, J. B., W. G. Aref, A. Ghafoor, and E. H. Spafford: 2001, 'Security models for web-based applications'. *Communications of the ACM* **44**(2), 38–44.

Jourdan, Z., R. K. Rainer Jr, T. E. Marshall, F. N. Ford, et al.: 2010, 'An Investigation Of Organizational Information Security Risk Analysis'. *Journal of Service Science (JSS)* **3**(2).

Jurison, J.: 1996, 'Toward more effective management of information technology benefits'. *The Journal of Strategic Information Systems* **5**(4), 263–274.

Kaliski Jr, B. S. and W. Pauley: 2010, 'Toward Risk Assessment as a Service in Cloud Environments.'. In: *HotCloud*.

Kannan, K., J. Rees, and S. Sridhar: 2007, 'Market reactions to information security breach announcements: An empirical analysis'. *International Journal of Electronic Commerce* **12**(1), 69–91.

Kaplan, R. S. and D. P. Norton: 1996, *The balanced scorecard: translating strategy into action*. Harvard Business Press.

Karabacak, B. and S. Ozkan: 2010, 'A Collaborative Process Based Risk Analysis for Information Security Management Systems'. In: *Proceedings of the 5th International Conference Information Warfare and Security*. p. 182.

Karabacak, B. and I. Sogukpinar: 2005, 'ISRAM: information security risk analysis method'. *Computers & Security* **24**(2), 147 – 159.

Karamitsos, I., C. Apostolopoulos, and M. Al Bugami: 2010, 'Benefits Management Process Complements Other Project Management Methodologies'. *Journal of Software Engineering and Applications* **3**, 839.

Keeney, R. L.: 1988, 'Structuring objectives for problems of public interest'. *Operations Research* **36**(3), 396–405.

Keeney, R. L.: 1992, *Value-Focused Thinking: A Path to Creative Decisionmaking*. Harvard University Press.

Keeney, R. L.: 1994a, 'Creativity Decision Making with Value-Focused Thinking'. *Sloan Management Review/Summer* pp. 33–41.

Keeney, R. L.: 1994b, 'Using values in operations research'. *Operations Research* **42**(5), 793–813.

Keeney, R. L.: 1996, 'Value-focused thinking: Identifying decision opportunities and creating alternatives'. *European Journal of Operational Research* **92**(3), 537–549.

Keeney, R. L.: 1999, 'The Value of Internet Commerce to the Customer'. *Management Science* **45**(4), 533–542.

Keeney, R. L.: 2001, 'Modeling values for telecommunications management'. *IEEE Transactions on Engineering Management* **48**(3), 370–379.

Keeney, R. L.: 2004, 'Making better decision makers'. *Decision Analysis* **1**(4), 193–204.

Keeney, R. L.: 2007a, 'Developing Objectives and Attributes'. *Advances in decision analysis: From foundations to applications* p. 104.

Keeney, R. L.: 2007b, 'Modeling Values for Anti-Terrorism Analysis'. *Risk Analysis* **27**(3), 585–596.

Keeney, R. L.: 2012, 'Value-focused brainstorming'. *Decision Analysis* **9**(4), 303–313.

Keeney, R. L. and R. S. Gregory: 2005, 'Selecting attributes to measure the achievement of objectives'. *Operations Research* **53**(1), 1–11.

Keeney, R. L., J. F. Lathrop, and A. Sicherman: 1986, 'An Analysis of Baltimore Gas and Electric Company's Technology Choice'. *Operations Research* **34**(1), 18–39.

Keeney, R. L. and D. Von Winterfeldt: 2010, 'Identifying and structuring the objectives of terrorists'. *Risk Analysis* **30**(12), 1803–1816.

Keeney, R. L. and D. von Winterfeldt: 2011, 'A value model for evaluating homeland security decisions'. *Risk Analysis* **31**(9), 1470–1487.

Keeney, R. L., D. Von Winterfeldt, and T. Eppel: 1990, 'Eliciting public values for complex policy decisions'. *Management Science* **36**(9), 1011–1030.

Khansa, L. and D. Liginlal: 2009, 'Quantifying the Benefits of Investing in Information Security'. *Communications ACM* **52**(11), 113–117.

Khidzir, N. Z., A. Mohamed, and N. H. H. Arshad: 2010, 'Information Security Risk Management: An Empirical Study on the Difficulties and Practices in ICT Outsourcing'. In: *Second International Conference on Network Applications Protocols and Services (NETAPPS)*. pp. 234–239.

Kiely, L. and T. V. Benzel: 2006, 'Systemic security management'. *IEEE Security & Privacy* **4**(6).

King, W. R.: 1978, 'Strategic planning for management information systems'. *MIS Quarterly* pp. 27–37.

Kirkwood, C. W.: 1996, *Strategic Decision Making: Multiobjective Decision Analysis with Spreadsheets*. Wadsworth Publishing Company.

Kissel, R.: 2013, 'Glossary of key information security terms'. *NIST Interagency Reports NIST IR* **7298**(3).

Klein, H. K. and M. D. Myers: 1999, 'A set of principles for conducting and evaluating interpretive field studies in information systems'. *MIS Quarterly* pp. 67–93.

Ko, M. and C. Dorantes: 2006, 'The impact of information security breaches on financial performance of the breached firms: an empirical investigation'. *Journal of Information Technology Management* **17**(2), 13–22.

Kolkowska, E. and G. Dhillon: 2013, 'Organizational power and information security rule compliance'. *Computers & Security* **33**, 3–11.

Kotter, J. P.: 1995, 'Leading change: Why transformation efforts fail'. *Harvard business review* **73**(2), 59–67.

Kotulic, A. G. and J. G. Clark: 2004, 'Why there aren't more information security research studies'. *Information & Management* **41**(5), 597–607.

Krause, M., H. F. Tipton, and W. Hugh Murray: 2002, 'Ownership and Custody of Data'. In: *Information Security Management Handbook, Fourth Edition, Volume 4*. Auerbach Publications, pp. 461–472.

Lacohée, H., A. D. Phippen, and S. M. Furnell: 2006, 'Risk and restitution: Assessing how users establish online trust'. *Computers & Security* **25**(7), 486–493.

Lai, L. K. H. and K. S. Chin: 2014, 'Development of a Failure Mode and Effects Analysis Based Risk Assessment Tool for Information Security'. *Industrial Engineering and Management Systems* **13**(1), 87–100.

Lalanne, V., M. Munier, and A. Gabillon: 2013, 'Information security risk management in a world of services'. In: *International Conference on Social Computing (SocialCom),*. pp. 586–593.

Langley, A., H. Mintzberg, P. Pitcher, E. Posada, and J. Saint-Macary: 1995, 'Opening up decision making: The view from the black stool'. *Organization Science* **6**(3), 260–279.

Laudon, K. C. and J. P. Laudon: 1995, *Management information systems: organization and technology*. Prentice-Hall, Inc.

Lee, A. S.: 1989, 'A Scientific Methodology for MIS Case Studies'. *MIS Quarterly* **13**(1), 33–50.

Lee, A. S.: 1991, 'Integrating positivist and interpretive approaches to organizational research'. *Organization science* **2**(4), 342–365.

Lee, A. S.: 2004, 'Thinking about social theory and philosophy for information systems'. *Social theory and philosophy for information systems* pp. 1–26.

Lee, A. S. and R. L. Baskerville: 2003, 'Generalizing generalizability in information systems research'. *Information systems research* **14**(3), 221–243.

Leon, O. G.: 1999, 'Value-Focused Thinking versus Alternative-Focused Thinking: Effects on Generation of Objectives'. *Organizational Behavior and Human Decision Processes* **80**(3), 213–227.

Levy, Y. and T. J. Ellis: 2006, 'A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research.'. *Informing Science* **9**.

Lichtenstein, S.: 1996, 'Factors in the selection of a risk assessment method'. *Information Management & Computer Security* **4**(4), 20–25.

Liebenau, J. and J. Backhouse: 1990, *Understanding information: An introduction*. Palgrave Macmillan.

Lin, C. and G. Pervan: 2003, 'The practice of IS/IT benefits management in large Australian organizations'. *Information & Management* **41**(1), 13–24.

Lin, C., G. Pervan, and D. McDermid: 2000, 'Research on IS/IT investment evaluation and benefits realization in Australia'. In: *Challenges of Information Technology Management in the 21st Century, 2000 Information Resources Management Association International Conference, Anchorage, Alaska, USA, May 21-24, 2000*. pp. 359–362.

Lin, C., G. Pervan, and D. McDermid: 2005a, 'IS/IT investment evaluation and benefits realization issues in Australia'. *Journal of research and practice in information technology* **37**(3), 235–251.

Lin, K. H., C. Lin, and H.-Y. Tsao: 2005b, 'IS/IT investment evaluation and benefit realization practices in Taiwanese SMEs'. *Journal of Information Science and Technology* **2**(4).

Lippmann, R., K. Ingols, C. Scott, K. Piwowarski, K. Kratkiewicz, M. Artz, and R. Cunningham: 2006, 'Validating and restoring defense in depth using attack graphs'. In: *MILCOM 2006-2006 IEEE Military Communications conference*. pp. 1–10.

Lo, C.-C. and W.-J. Chen: 2012, 'A hybrid information security risk assessment procedure considering interdependences between controls'. *Expert Systems with Applications* **39**(1), 247–257.

Locher, C.: 2005, 'Methodologies for evaluating information security investments-What Basel II can change in the financial industry'. In: *European Conference on Information Systems*. pp. 122–132.

Longstaff, T., C. Chittister, R. Pethia, and Y. Haimes: 2000, 'Are we forgetting the risks of information technology?'. *Computer* **33**(12), 43 –51.

López, D. and O. Pastor: 2013, 'Comprehensive Approach to Security Risk Management in Critical Infrastructures and Supply Chains'. *Information & Security: An International Journal* **29**(1).

Love, P. E. and Z. Irani: 2004, 'An exploratory study of information technology evaluation and benefits management practices of SMEs in the construction industry'. *Information & Management* **42**(1), 227–242.

Madlmayr, G., J. Langer, C. Kantner, and J. Scharinger: 2008, 'NFC devices: Security and privacy'. In: *Third International Conference on Availability, Reliability and Security, ARES 08.* pp. 642–647.

Matsuura, K.: 2008, 'Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model.'. In: *Workshop on the Economics of Information Security (WEIS)*.

Maxwell, J. A.: 2008, 'Designing a qualitative study'. *The Sage handbook of applied social research methods* pp. 214–253.

May, J., G. Dhillon, and M. Caldeira: 2013, 'Defining value-based objectives for ERP systems planning'. *Decision Support Systems* **55**(1), 98–109.

Mayer, N., J. Aubert, H. Cholez, and E. Grandry: 2013, 'Sector-based improvement of the information security risk management process in the context of telecommunications regulation'. In: *Systems, Software and Services Process Improvement*. Springer, pp. 13–24.

McCumber, J.: 2004, *Assessing and managing security risk in IT systems: A structured methodology*. CRC Press.

McFadzean, E., J.-N. Ezingeard, and D. Birchall: 2006, 'Anchoring information security governance research: sociological groundings and future directions'. *Journal of Information System Security* **2**(3), 3–48.

McFadzean, E., J.-N. Ezingeard, and D. Birchall: 2007, 'Perception of risk and the strategic impact of existing IT on information security strategy at board level'. *Online Information Review* **31**(5), 622–660.

McFarlan, F. W. and J. L. McKenney: 1983, *Corporate information systems management: The issues facing senior executives*. Irwin Professional Publishing.

Melton, T., J. Yates, and P. Iles-Smith: 2011, *Project Benefits Management: Linking projects to the Business*. Butterworth-Heinemann.

Meng, M.: 2013, 'The research and application of the risk evaluation and management of information security based on AHP method and PDCA method'. In: *6th International Conference on*

Information Management, Innovation Management and Industrial Engineering (ICIII), Vol. 3. pp. 379–383.

Merkhofer, M. W. and R. L. Keeney: 1987, 'A multiattribute utility analysis of alternative sites for the disposal of nuclear waste'. *Risk Analysis* **7**(2), 173–194.

Merrick, J. R., M. Grabowski, P. Ayyalasomayajula, and J. R. Harrald: 2005a, 'Understanding Organizational Safety Using Value-Focused Thinking'. *Risk Analysis* **25**(4), 1029–1041.

Merrick, J. R., G. S. Parnell, J. Barnett, and M. Garcia: 2005b, 'A multiple-objective decision analysis of stakeholder values to identify watershed improvement needs'. *Decision Analysis* **2**(1), 44–57.

Miles, M. B. and A. M. Huberman: 1994, *Qualitative data analysis: An expanded sourcebook*. Sage.

Mingers, J.: 2002, 'Real-izing Information Systems: Critical Realism as an Underpinning Philosophy for Information Systems.'. In: F. Miralles and J. Valor (eds.): *International Conference on Information Systems*. p. 27, Association for Information Systems.

Mintzberg, H.: 1987a, 'The strategy concept I: Five Ps for strategy'. *California management review* **30**(1), 11–24.

Mintzberg, H.: 1987b, 'The strategy concept II: another look at why organizations need strategies'. *California management review* **30**(1), 25–32.

Mintzberg, H.: 1988, 'Crafting Strategy'. *The McKinsey Quarterly. McKinsey & Company Inc., Summer88* (3), p71–90.

Mintzberg, H. and F. Westley: 2001, 'Decision making: It's not what you think'. *MIT Sloan Management Review* **42**(3), 89.

Mishra, S. and G. Dhillon: 2008, 'Defining Internal Control Objectives for Information Systems Security: A Value Focused Assessment'. In: *European Conference on Information Systems*. pp. 1334–1345.

Morais, D. C., L. H. Alencar, A. P. Costa, and R. L. Keeney: 2013, 'Using value-focused thinking in Brazil'. *Pesquisa Operacional* **33**(1), 73–88.

NIST: 2011, 'SP 800-39. Managing Information Security Risk: Organization, Mission, and Information System View'. Technical report, National Institute of Standards & Technology, Gaithersburg, MD, United States.

NIST, J. T. F. T. I.: 2010, 'SP 800-37 Rev. 1. Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach'. Technical report, National Institute of Standards & Technology, Gaithersburg, MD, United States.

Njenga, K. and I. Brown: 2010, 'The Case for Improvisation in Information Security Risk Management'. In: *E-Government, E-Services and Global Processes*. Springer, pp. 220–230.

Nogeste, K.: 2008, 'Start From the Very Beginning: Define Expected Benefits, Outcomes and Outputs in the Project Business Case'. In: *5th Annual Project Management Australia Conference*. pp. 18–20.

OGC: 2005, 'Managing Benefits: An Overview'. Technical report, Office for Government and Commerce.

Orlikowski, W. J. and J. J. Baroudi: 1991, 'Studying information technology in organizations: Research approaches and assumptions'. *Information systems research* **2**(1), 1–28.

Ozkan, S. and B. Karabacak: 2010, 'Collaborative risk method for information security management practices: A case context within Turkey'. *International Journal of Information Management* **30**(6), 567–572.

Paivarinta, T. and W. Dertz: 2008, 'Pre-determinants of implementing IT benefits management in Norwegian municipalities: cultivate the context'. In: *Electronic Government*. Springer, pp. 111–123.

Paivarinta, T., W. Dertz, and L. S. Flak: 2007, 'Issues of Adopting Benefits Management Practices of IT Investments in Municipalities: A Delphi Study in Norway'. In: *40th Annual Hawaii International Conference on System Sciences, HICSS 2007.* pp. 103–103.

Palmer, M. E., C. Robinson, J. C. Patilla, and E. P. Moser: 2001, 'Information security policy framework: best practices for security policy in the e-commerce age'. *Information Systems Security* **10**(2), 1–15.

Paquette, S., P. T. Jaeger, and S. C. Wilson: 2010, 'Identifying the security risks associated with governmental use of cloud computing'. *Government Information Quarterly* **27**(3), 245–253.

Paré, G.: 2004, 'Investigating information systems with positivist case research'. *The Communications of the Association for Information Systems* **13**(1), 57.

Parnell, G. S., D. W. Hughes, R. C. Burk, P. J. Driscoll, P. D. Kucik, B. L. Morales, and L. R. Nunn: 2013, 'Invited Review Survey of Value-Focused Thinking: Applications, Research Developments and Areas for Future Research.'. *Journal of Multi-Criteria Decision Analysis* **20**(1/2), 49 – 60.

Pather, S. and D. Remenyi: 2004, 'Some of the philosophical issues underpinning research in information systems: from positivism to critical realism'. In: *Proceedings of the 2004 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries*. pp. 141–146.

Peltier, T. R.: 2005, 'Implementing an Information Security Awareness Program.'. *Information Systems Security* **14**(2), 37–49.

Peltier, T. R.: 2013, *Information security fundamentals*. CRC Press.

Peppard, J., R. Lambert, and C. Edwards: 2000, 'Whose job is it anyway?: organizational information competencies for value creation'. *Information Systems Journal* **10**(4), 291–322.

Peppard, J. and J. Ward: 2004, 'Beyond strategic information systems: towards an IS capability'. *The Journal of Strategic Information Systems* **13**(2), 167–194.

Peppard, J., J. Ward, and E. Daniel: 2007, 'Managing the realization of business benefits from IT investments'. *MIS Quarterly Executive* **6**(1), 1–11.

Pereira, L., F. d. S. Soares, and M. Caldeira: 2012, 'Information systems security outsourcing key issues: a service providers' perspective'. In: *Proceedings of the European Conference on Information Systems 2012*.

Pereira, T. and H. Santos: 2009, 'An ontology based approach to information security'. In: *Metadata and Semantic Research*. Springer, pp. 183–192.

Pina, P., M. Romão, and M. Oliveira: 2013, 'Using benefits management to link knowledge management to business objectives'. *VINE: Journal of Information and Knowledge Management Systems* **43**(1), 22–38.

Poolsappasit, N., R. Dewri, and I. Ray: 2012, 'Dynamic security risk management using bayesian attack graphs'. *IEEE Transactions on Dependable and Secure Computing* **9**(1), 61–74.

Porter, M. E.: 1996, 'What Is Strategy?'. *Harvard Business Review* p. 2.

Porter, M. E. and V. E. Millar: 1985, 'How information gives you competitive advantage'.

Porter, S.: 1993, 'Critical Realist Ethnography: The Case of Racism and Professionalism in a Medical Setting'. *Sociology* **27**(4), 591–609.

Posthumus, S. and R. Von Solms: 2004, 'A framework for the governance of information security'. *Computers & Security* **23**(8), 638–646.

Pramatari, K. and A. Theotokis: 2009, 'Consumer acceptance of RFID-enabled services: a model of multiple attitudes, perceived system characteristics and individual traits'. *European Journal of Information Systems* **18**(6), 541–552.

Purdy, G.: 2010, 'ISO 31000: 2009 setting a new standard for risk management'. *Risk analysis* **30**(6), 881–886.

Purser, S. A.: 2004, 'Improving the ROI of the security management process'. *Computers & Security* **23**(7), 542–546.

Quinn, J. B.: 1981, 'Formulating strategy one step at a time'. *The journal of business strategy* **1**(3), 42.

Ramanujam, V., N. Venkatraman, and J. C. Camillus: 1986, 'Multi-objective assessment of effectiveness of strategic planning: a discriminant analysis approach'. *Academy of management Journal* **29**(2), 347–372.

Reid, R. and J. V. Niekerk: 2014, 'From information security to cyber security cultures'. In: *Information Security for South Africa*.

Remenyi, D. and M. Sherwood-Smith: 1998, 'Business benefits from information systems through an active benefits realisation programme'. *International Journal of Project Management* **16**(2), 81–98.

Renn, O.: 1998, 'Three decades of risk research: accomplishments and new challenges'. *Journal of Risk Research* **1**(1), 49–71.

Rios, M. J., S. T. de Magalhães, L. Santos, and H. Jahankhani: 2009, 'The Georgias Cyberwar'. In: *International Conference on Global Security, Safety, and Sustainability*. pp. 35–42.

Rockart, J. F.: 1978, 'Chief executives define their own data needs.'. *Harvard business review* **57**(2), 81–93.

Ryan, J. J., T. A. Mazzuchi, D. J. Ryan, J. L. De la Cruz, and R. Cooke: 2012, 'Quantifying information security risks using expert judgment elicitation'. *Computers & Operations Research* **39**(4), 774–784.

Safa, N. S., M. Sookhak, R. Von Solms, S. Furnell, N. A. Ghani, and T. Herawan: 2015, 'Information security conscious care behaviour formation in organizations'. *Computers & Security* **53**, 65–78.

Safa, N. S., R. Von Solms, and S. Furnell: 2016, 'Information security policy compliance model in organizations'. *Computers & Security* **56**, 70–82.

Sahinoglu, M.: 2005, 'Security meter: A practical decision-tree model to quantify risk'. *IEEE Security & Privacy* (3), 18–24.

Saleem, K., S. Luis, Y. Deng, S.-C. Chen, V. Hristidis, and T. Li: 2008, 'Towards a business continuity information network for rapid disaster recovery'. In: *Proceedings of the 2008 international conference on Digital government research*. pp. 107–116.

Salmela, H.: 2008, 'Analysing business losses caused by information systems risk: a business process analysis approach'. *Journal of Information Technology* **23**(3), 185–202.

Saltzer, J. H. and M. D. Schroeder: 1975, 'The protection of information in computer systems'. *Proceedings of the IEEE* **63**(9), 1278–1308.

Saluja, U. and D. N. B. Idris: 2015, 'Statistics Based Information Security Risk Management Methodology'. *International Journal of Computer Science and Network Security (IJCSNS)* **15**(10), 117.

Samy, G. N., R. Ahmad, and Z. Ismail: 2010, 'A framework for integrated risk management process using survival analysis approach in information security'. In: *Sixth International Conference on Information Assurance and Security (IAS)*. pp. 185–190.

Sapountzis, S., K. Harris, and M. Kagioglou: 2008, 'Benefits Management and Benefits Realisation–A Literature Review'. *HaCIRIC, The University of Salford, UK*.

Sapountzis, S., K. Yates, M. Kagioglou, and G. Aouad: 2009, 'Realising benefits in primary healthcare infrastructures'. *Facilities* **27**(3/4), 74–87.

Sayer, R.: 1984, *Method in social science: a realist approach*, Hutchinson university library. Hutchinson.

Schechter, S. E.: 2004, 'Toward Econometric Models of the Security Risk from Remote Attacks'. *IEEE Security and Privacy* **3**, 2005.

Schneier, B.: 2008, 'The psychology of security'. *Africacrypt* pp. 50–79.

Schwabe, G. and P. Banninger: 2008, 'IT-Benefits-Management in the Swiss Financial Sector'. In: *Proceedings of the 41st Annual Hawaii International Conference on System Sciences*. pp. 456–456.

Serra, C. E. M.: 2016, *Benefits Realization Management: Strategic Value from Portfolios, Programs, and Projects*. CRC Press.

Shanks, G.: 2007, 'Guidelines for conducting positivist case study research in information systems'. *Australasian Journal of Information Systems* **10**(1).

Sharma, S. and G. Dhillon: 2009, 'Is Risk Analysis: A Chaos Theoretic Perspective'. *Issues in Information Systems* **10**(2), 552–560.

Shedden, P., R. Scheepers, W. Smith, and A. Ahmad: 2011, 'Incorporating a knowledge perspective into security risk assessments'. *Vine: the journal of information and knowledge management systems* **41**(2), 152–166.

Sheng, H., F. F.-H. Nah, and K. Siau: 2005, 'Strategic implications of mobile technology: A case study using value-focused thinking'. *The Journal of Strategic Information Systems* **14**(3), 269–290.

Sheng, H., K. Siau, and F. F.-H. Nah: 2010, 'Understanding the values of mobile technology in education: a value-focused thinking approach'. *ACM SIGMIS Database* **41**(2), 25–44.

Shoviak, M. J.: 2001, 'Decision analysis methodology to evaluate integrated solid waste management alternatives for a remote Alaskan air station'. Technical report, DTIC Document.

Silic, M. and A. Back: 2014, 'Shadow IT–A view from behind the curtain'. *Computers & Security* **45**, 274–283.

Silva, M. M., A. P. H. de Gusmão, T. Poleto, L. C. e Silva, and A. P. C. S. Costa: 2014, 'A multidimensional approach to information security risk management using FMEA and fuzzy theory'. *International Journal of Information Management* **34**(6), 733–740.

Siponen, M.: 2001, 'Five dimensions of information security awareness'. *Computers and society* **31**(2), 24–29.

Siponen, M. T.: 2000, 'A conceptual foundation for organizational information security awareness'. *Information Management & Computer Security* **8**(1), 31–41.

Slayton, R.: 2015, 'Measuring Risk: Computer Security Metrics, Automation, and Learning'. *IEEE Annals of the History of Computing* **37**(2), 32–45.

Slovic, P., M. L. Finucane, E. Peters, and D. G. MacGregor: 2004, 'Risk as Analysis and Risk as Feelings: Some Thoughts about Affect, Reason, Risk, and Rationality'. *Risk Analysis* **24**(2), 311–322.

Smith, G. S.: 2004, 'Recognizing and preparing loss estimates from cyber-attacks'. *Information Systems Security* **12**(6), 46–57.

Smith, M. L.: 2006, 'Overcoming theory-practice inconsistencies: Critical realism and information systems research'. *Information and organization* **16**(3), 191–211.

Son, J.-Y. and S. S. Kim: 2008, 'Internet users' information privacy-protective responses: A taxonomy and a nomological model'. *MIS quarterly* pp. 503–529.

Spears, J. L.: 2005, 'A holistic risk analysis method for identifying information security risks'. In: *Security Management, Integrity, and Internal Control in Information Systems*. Springer, pp. 185–202.

Spears, J. L. and H. Barki: 2010, 'User Participation in Information Systems Security Risk Management'. *MIS Quarterly* **34**(3), 503–522.

Stake, R.: 1998, 'Case Studies'. *In:Norman Denzin & Yvonna Lincoln. Strategies of Qualitative Inquiry.London, New Delhi: Sage*.

Stewart, A.: 2004, 'On risk: perception and direction'. *Computers & Security* **23**(5), 362–370.

Straub, D. W. and R. J. Welke: 1998, 'Coping with systems risk: security planning models for management decision making'. *MIS Quarterly* **22**(4), 441–469.

Stroie, E. R. and A. C. Rusu: 2011, 'Security Risk Management-Approaches and Methodology'. *Informatica Economica* **15**(1), 228.

Suh, B. and I. Han: 2003, 'The IS risk analysis based on a business model'. *Information & Management* **41**(2), 149–158.

Sun, L., R. P. Srivastava, and T. J. Mock: 2006, 'An Information Systems Security Risk Assessment Model Under the Dempster-Shafer Theory of Belief Functions'. *Journal Management Information Systems* **22**(4), 109–142.

Tatsumi, K. and M. Goto: 2009, 'Optimal Timing of Information Security Investment: A Real Options Approach.'. In: *Workshop on the Economics of Information Security (WEIS)*.

Taylor, R. G.: 2015, 'Potential Problems with Information Security Risk Assessments'. *Information Security Journal: A Global Perspective* **24**(4-6), 177–184.

Telang, R. and S. Wattal: 2005, 'Impact of software vulnerability announcements on the market value of software vendors-an Empirical investigation'. *Available at SSRN 677427*.

Thapa, D. and D. Harnesk: 2014, 'Rethinking the Information Security Risk Practices: A Critical Social Theory Perspective'. In: *47th Hawaii International Conference on System Sciences*. pp. 3207–3214.

Thomson, K.-L., R. von Solms, and L. Louw: 2006, 'Cultivating an organizational information security culture'. *Computer Fraud & Security* **2006**(10), 7–11.

Tiganoaia, B.: 2012, 'Comparative study regarding the methods used for security risk management'. *Scientific Bulletin-Nicolae Balcescu Land Forces Academy* **17**(2), 149.

Tillmann, P., P. Tzortzopolous, S. Sapountzis, C. Formoso, and M. Kagioglou: 2012, 'A Case Study On Benefits Realization And Its Contributions For Linking Project Outputs To Outcomes'. *Proceedings for the 20th Annual Conference of the International Group for Lean Construction*.

Torkzadeh, G. and G. Dhillon: 2002, 'Measuring Factors that Influence the Success of Internet Commerce'. *Information Systems Research* **13**(2), 187–204.

Tsai, Y. C., J. C. Yeh, et al.: 2010, 'Perceived risk of information security and privacy in online shopping: A study of environmentally sustainable products'. *African Journal of Business Management* **4**(18), 4057–4066.

Tsao, H., K. H. Lin, and C. Lin: 2004, 'An investigation of critical success factors in the adoption of B2BEC by Taiwanese companies'. *Journal of American Academy of Business* **5**(1), 198–202.

UN: 2016, 'E-Government Survey 2016: E-Government in support of sustainable development'. Technical report, United Nations.

Valackiene, A.: 2015, 'Efficient corporate communication: decisions in crisis management'. *Engineering Economics* **66**(1).

van der Meulen, N.: 2013, 'DigiNotar: Dissecting the First Dutch Digital Disaster'. *Journal of Strategic Security* **6**(2), 46.

Van Deursen, N., W. J. Buchanan, and A. Duff: 2013, 'Monitoring information security risks within health care'. *Computers & Security* **37**, 31–45.

Veiga, A. D. and J. H. Eloff: 2007, 'An information security governance framework'. *Information Systems Management* **24**(4), 361–372.

Veiga, A. D. and J. H. Eloff: 2010, 'A framework and assessment instrument for information security culture'. *Computers & Security* **29**(2), 196–207.

Vermeulen, C. and R. Von Solms: 2002, 'The information security management toolbox–taking the pain out of security management'. *Information Management & Computer Security* **10**(3), 119–125.

Vitale, M. R.: 1986, 'The growing risks of information systems success'. *MIS Quarterly* pp. 327–334.

Von Solms, R. and J. Van Niekerk: 2013, 'From information security to cyber security'. *Computers & Security* **38**, 97–102.

Von Solms, R. and S. B. von Solms: 2006, 'Information security governance: Due care'. *Computers & Security* **25**(7), 494–497.

Vorster, A. and L. Labuschagne: 2005, 'A framework for comparing different information security risk analysis methodologies'. In: *Proceedings of the 2005 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries*. Republic of South Africa, pp. 95–103, South African Institute for Computer Scientists and Information Technologists.

Wade, M. and J. Hulland: 2004, 'Review: The resource-based view and information systems research: Review, extension, and suggestions for future research'. *MIS quarterly* **28**(1), 107–142.

Walsham, G.: 1993, *Interpreting information systems in organizations*. John Wiley & Sons, Inc.

Walsham, G.: 1995a, 'The emergence of interpretivism in IS research'. *Information systems research* **6**(4), 376–394.

Walsham, G.: 1995b, 'Interpretive case studies in IS research: nature and method'. *European Journal of information systems* **4**(2), 74–81.

Walsham, G.: 2006, 'Doing interpretive research'. *European journal of information systems* **15**(3), 320–330.

Wang, T., K. N. Kannan, and J. R. Ulmer: 2013, 'The association between the disclosure and the realization of information security risk factors'. *Information Systems Research* **24**(2), 201–218.

Ward, J. and E. Daniel: 2006, *Benefits management: delivering value from IS and IT investments*. Wiley.

Ward, J. and E. Daniel: 2012, *Benefits management: how to increase the business value of your IT projects*. John Wiley & Sons.

Ward, J., S. De Hertogh, and S. Viaene: 2007, 'Managing benefits from IS/IT investments: An empirical investigation into current practice'. In: *40th Annual Hawaii International Conference on System Sciences, 2007. HICSS 2007*. pp. 206a–206a.

Ward, J. and R. Elvin: 1999, 'A new framework for managing IT-enabled business change'. *Information systems journal* **9**(3), 197–221.

Ward, J. and J. Peppard: 2002, *Strategic Planning for Information Systems*, John Wiley Series in Information Systems. Wiley.

Ward, J., P. Taylor, and P. Bond: 1996, 'Evaluation and realisation of IS/IT benefits: an empirical study of current practice'. *European Journal of Information Systems* **4**(4), 214–225.

Webb, J., A. Ahmad, S. B. Maynard, and G. Shanks: 2014, 'A situation awareness model for information security risk management'. *Computers & security* **44**, 1–15.

Webster, J. and R. T. Watson: 2002, 'Analyzing the past to prepare for the future: writing a literature review'. *MIS quarterly* **26**(2), 13–23.

Wei, G., X. Xhang, X. Zhang, and Z. Huang: 2010, 'Research on E-government Information Security Risk Assessment - Based on Fuzzy AHP and Artificial Neural Network Model'. In: *First International Conference on Networking and Distributed Computing (ICNDC)*. pp. 218–221.

Wernerfelt, B.: 1995, 'The resource-based view of the firm: Ten years after'. *Strategic management journal* **16**(3), 171–174.

Westby, J. R. and J. H. Allen: 2007, 'Governing for enterprise security (ges) implementation guide'. Technical Report CMU/SEI-2007-TN-020, Carnegie Mellon University SEI.

Westerman, G.: 2009, 'IT Risk as a Language for Alignment.'. *MIS Quarterly Executive* **8**(3).

Whitman, M. E.: 2003, 'Enemy at the gate: threats to information security'. *Communications of the ACM* **46**(8), 91–95.

Whitman, M. E., H. J. Mattord, and A. Green: 2013, *Principles of incident response and disaster recovery*. Cengage Learning.

Woodside, A. G.: 2010, *Case Study Research: Theory, Methods, Practice*. Emerald Group Publishing.

Wrapp, H. E.: 1984, *Good managers don't make policy decisions*. Harvard Business Review Case Services.

Wynn Jr, D. and C. K. Williams: 2012, 'Principles for Conducting Critical Realist Case Study Research in Information Systems.'. *MIS Quarterly* **36**(3).

Xinlan, Z., H. Zhifang, W. Guangfu, and Z. Xin: 2010, 'Information security risk assessment methodology research: Group decision making and analytic hierarchy process'. In: *Second World Congress on Software Engineering (WCSE)*, Vol. 2. pp. 157–160.

Yang, Y.-P. O., H.-M. Shieh, and G.-H. Tzeng: 2013, 'A VIKOR technique based on DEMATEL and ANP for information security risk control assessment'. *Information Sciences* **232**, 482–500.

Yates, K., S. Sapountzis, E. Lou, and M. Kagioglou: 2009, 'BeReal: Tools and methods for implementing benefits realisation and management'. *5th Nordic Conference on Construction Economics and Organisation*.

Yazar, Z.: 2002, 'A qualitative risk analysis and management tool CRAMM'. *SANS Reading Room*.

Yeo, M. L., E. Rolland, J. R. Ulmer, and R. A. Patterson: 2014, 'Risk mitigation decisions for IT security'. *ACM Transactions on Management Information Systems (TMIS)* **5**(1), 5.

Yin, R. K.: 2003, *Case study research: design and methods*. Sage Publications, 3rd edition.

Zafar, H., M. S. Ko, and J. G. Clark: 2014, 'Security Risk Management in Healthcare: A Case Study'. *Communications of the Association for Information Systems* **34**(1), 37.

Zetter, K.: 2011, 'DigiNotar files for bankruptcy in wake of devastating hack'. *Wired magazine*.

Zhang, X., N. Wuwong, H. Li, and X. Zhang: 2010, 'Information security risk management framework for the cloud computing environments'. In: *IEEE 10th International Conference on Computer and Information Technology (CIT)*. pp. 1328–1334.

Zhao, X., L. Xue, and A. B. Whinston: 2013, 'Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements'. *Journal of Management Information Systems* **30**(1), 123–152.