Next Generation Human and Organizational Risk Management

Fenghua Wang

Master's Thesis
Master of Science in Information Security
30 ECTS
Department of Computer Science and Media Technology
Gjøvik University College, 2014

Avdeling for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Abstract

On a regular basis compromise of organizations as result of frauds, espionage, and hackers are presented in the news. Still, many organizations tend to underestimate or ignore human related security problems. Human behavior bears diverse risks such as insider fraud, distrustful behavior and mental disorders, which may result in harmful security breaches for the enterprise. With cloud services a new security architecture and awareness is required, especially for human and organizational issues. In addition, the evolution of our society towards the next generation of the network society requires the attention of security officers for a range of different disciplines: society, politics, economy, culture, new forms of collaboration and interaction, etc. Success in countering new security risks in all of these fields is to a large portion based on understanding and managing next generation human factor.

However, existing frameworks and standards are not already covering issues in dealing with human and organizational risks sufficiently.

By analyzing the current situation of human and organizational risk management frameworks, we supplement and suggest updates to existing frameworks for addressing those aspects in a more appropriate and professional way.

The master thesis uses literature review and expert interview methodology for the identification of the new parameters that influence human and organizational risk management. Due to the fast change of technology, society and environment, many new risks have appeared. The given analysis and recommendations enables us to address these new risks professionally and in a more consistent way.

Sammendrag

Stadig vekk dukker det opp nyheter om organisasjoner som blir utsatt for bedrageri, spionasje og hacking. Allikevel pleier mange organisasjoner å undervurdere eller overse menneskerelaterte sikkerhetsproblemer. Menneskelig atferd fører til ulike risikoer som innsidebedrageri, mistroisk atferd og psykiske lidelser, som kan føre til skadelige sikkerhetsbrudd for forretningsvirksomheten. For skytjenester kreves det ny sikkerhetsarkitektur og –bevissthet særlig i området for menneskelige og organisatoriske problemer. I tillegg utvikles samfunnet vårt mot den neste generasjonen av nettsamfunn og krever derfor oppmerksomhet fra sikkerhetspersonell for en rekke disipliner innenfor: samfunn, politikk, økonomi, kultur, nye måter å samarbeide og samhandle, etc. Suksessfull motvirkning av de nye risikoene i alle disse områdene er i hovedsak basert på forståelse og håndtering av neste generasjons menneskelige faktor.

Imidlertid dekker ikke eksisterende rammeverk og standarder håndtering av menneskelige og organisatoriske problemer.

Ved å analysere de nåværende forholdene i menneskelige og organisatoriske rammeverk for håndtering av risiko, supplerer vi og foreslår oppdateringer til eksisterende rammeverk som kan hjelpe oss å takle disse aspektene på en mer hensiktsmessig og profesjonell måte.

Denne masteroppgaven bruker litteraturstudie til å identifisere nye parametere som påvirker menneskelig og organisatorisk risikostyring. Mange risikoer har dukket opp på grunn av rask endring av teknologi, samfunn og miljø. Den gitte analysen og anbefalingene, gjør at vi kan takle de nye risikoene profesjonelt og på en jevnere måte.

Acknowledgments

I owe my deepest gratitude to my supervisor professor Bernhard M. Hämmerli for his guidance, feedback, support and encouragement throughout the master thesis period. I am indebted for his time and guidance whenever I needed it.

I am also thankful to all my lecturers. I would like to thank them for the wonderful time I had during lectures and the interesting discussion between break times. The knowledge and skills that they taught me help a lot during my period of writing this thesis.

I am grateful to the respondents participating in the interviews for my master thesis: Siv Hilde Houmb (Associate professor II of Gjøvik University College), Thomas Schlienger (Consultant of TreeSolution AS), Stewart Kowalski (Professor of Gjøvik University College), and Hans Marius Tessem (Senior Adviser of NorSIS).

Finally, I would like to thank my family and friends, especially my parents for always believing in me, I could not have done it without your encouragement. I am very grateful to my boyfriend, Eirik Bae, for his encouragement and support during my master study.

Contents

List of Figures

List of Tables

1 Introduction

This chapter provides the general information about the master thesis. It presents the topic covered in this thesis, highlights the problems involved and identifies the research questions we are trying to solve. In addition, the justification, motivation and benefits are given. This master thesis's methodology used to accomplish this are presented before we go further into the background. The claimed contribution and outline of the thesis is introduced at the end of this chapter.

1.1 Topic covered by the project

Humans have already become an important resource for the competitive advantage in any organization and it also makes enterprise different from their competitors. Nowadays, with advanced development of economics, all the enterprises have greater demand of human resources, while increasing risks from human and organizational aspects will impact the benefits of the enterprise. However, lots of existing frameworks are not clear about how to deal with the human and organizational risks. Thus, there is a demand for thinking about what we can update in the human and organizational risk management.

Human is very complex, which can be affected by everything, on the contrary, it can affect everything as well. So what the dynamic change of human situation and behavior? By a resource is meant anything which could be thought as a strength or a weakness of a given firm[7]. Any strength or weakness of humans might become a potential risk towards the enterprise. Therefore, we believe that a threat model that shows the dynamic relationships between human situation and behavior with information security concerns is very important.

In all the organizations' human resources part, trust among human beings is the essential elements in their daily work, but trust is a complex progress. Trust is a group phenomenon, however, the decision to trust is individual[8]. Especially, when we deal with human and organizational process, trust need to be seriously considered.

These questions will give a picture of the changes in human and organizational risk management. We expect for the answers that can help organizations have less risks in human and organizational aspects than before.

1.2 Keywords

Human and organizational risk management framework, organizational risk, human risk, human situation and behavior, "crown jewels", collaboration risks, evaluate security spending, the

network society, new risks.

1.3 Problem description

Today, we all know the importance of human resources in organizations, economic institutions, and industrial enterprises[9]. The world is changing rapidly, which greatly affect the lives and activities of the staff of organizations[9]. One of the big challenges is globalization as it brings new politics, culture, technology, governance, security, which lead to a lasting competitive space. In order to be a winner in this competition, employees are needed by the organizations to achieve their business goal. However, the organizations always ignore many problems among their employees, which introduces many risks, e.g. insider threat, distrust, mental issues, even worse, it can increase risks for security branches of the enterprise.

Because of the global total economic situation is not optimistic in these years, so many organizations use the strategy of reorganization by reducing staff, the need to reduce costs, closing a department or enterprise. As a result, it gives rise to more conflicts among humans and organizations, and brings many social problems as well.

Human is the biggest threat in the organization[10][11, p.42-43]. It is a critical issue that we faced today. However, a sufficient framework for dealing with human and organizational risks is none existing. The existing frameworks are not good enough to handle these risks as well.

In this thesis we will investigate how the existing frameworks are not good enough for handling today's human and organizational risks. Based on the results we will suggest supplements and updates to existing frameworks, so that we can be better protected against the human and organizational risks we face today.

1.4 Justification, motivation and benefits

"*People are the weakest link in the chain*"[10], in many cases, humans bring many threats to the organizations. Espionage, discarding significant information, dishonest are very common human threats. By doing this master thesis we will seek solutions to this situation and propose changes that could make fewer risks towards the organizations.

"*People are the great asset*"[10], any organizations can't live without their people. When employees bring benefits to the firm, they should turn to think what they can give to them? It is important to make employees feel happy, stable and satisfied. Many people rely on their company keep them have a good life. Thus in this master thesis we will give a clear understanding of the relationships between the humans and organizations, to find a better way to caring the human behavior and their situation.

By solving these issues in this master thesis, it will benefit both organizations and humans. And

we will provide recommendations for them.

1.5 Research questions

To get a clear understanding of what that has considered for updating the existing human and organizational risk management framework, six research questions have been defined:

1. In terms of information security, how does human situation affect human behavior?
2. What is the business impact and its associated risks when introducing extensive collaboration in and outside the company and with electronic means?
3. What are the conditions to allow someone to deal with "crown jewels"?
4. A review of risk catalogues and organizational revolution, what should be considered when we approach total networked society?
5. How can we assess security over and under spending in the managerial, human and organizational process?
6. Which environmental, technology, societal and some other parameters must be observed and what is the time line to reassign risks?

1.6 Methodology

In order to find the answers to the research questions just presented, a solid understanding disciplines is involved for how to answer them. A survey of the existing frameworks and standards, related work of human and organizational risk management, key human and organizational process issues analysis and evaluation of security spending is conducted. The methodologies that are used for addressing these disciplines are shown as following:

- Literature review
- Expert interviews
- Existing case study

The following content will explain why the method is appropriate and what desired information it can provide.

Literature review

In order to do literature review scientifically, we follow the methods which are described in [12, p. 51-70]. The literature review is used to analyze the current situation within the human and organizational risk management, and to develop new parameters of managing human and organizational risks. In order to have a clear understanding of the existing frameworks' human and organizational risk management aspects, some of the frameworks and standards study is

needed. These frameworks and standards properly documented what they covered within the aspects of human and organizations risk management. Based on them, we can give a hypothesis of new parameters that need to supplement for the human and organizational risks management framework.

Literature study can also offer ideas, perspectives, and approaches related to the human and organizational risk management, which includes: human behavior analysis, human related security problems, the “crown jewel” protection, risks mitigations, etc.

The references, which includes scientific papers, the existing frameworks and standards, information technology journal, the organization’s on-line publications, are listed in the bibliography. Some of them are founded from scientific resource database, on-line databases, the library of Gjøvik University College, others were suggested to consider by the supervisor of this master thesis. We only use Wikipedia for definitions, which include depression, schizophrenia, bullying, anxiety disorder and interpersonal relationship. We do not use Wikipedia in our research.

Expert interviews

The expert’s interviews carried out via Skype video conferencing, the respondents that participated interviews include professors of Gjøvik University College, an information security consultant, and a senior advisor of NorSIS. We prepared 15 questions that are related the research questions and some other content within the scope of this thesis. The expert interviews are used for collecting senior information about human and organizational risk management, and helping us have a fully understanding of how the information security officers perform the human and organizational risk assessment in their organizations, what kind of potential risks related to humans and organizations are usually exposed, what strategies they use for managing these risks and so on. These could help us to provide advices on how to manage human and organizational incidents and risks, how to promote security awareness, and change attitudes and behavior among the human and organizational security issues. This methodology also introduces us new ideas, knowledge, and skills related to human and organizational risk management process. The information gained from the interviews will be cited in the master thesis or will be regarded as suggestions to find more relevant resources.

Existing case study

The existing case study is focus on the study of "the statement of futurist" from the world future society [1]. The world future society is an organization of people dedicated to exploring the future, where we can learn the future of humanity, governance, information security, and technology. From the issues the futurist predicted, we can identify the potential risks, threats or problems that might happen in the future. In order to have a clear understanding of new risks, we believe that the corresponding business impact should be fully understood and the mitigations should be given. As such, we can prepare for the unexpected, and mitigate the impact and likelihood of

[1] The World Future Society: `http://www.wfs.org/futurist`

these new risks.

1.7 Claimed contributions

The contributions of this master thesis are an analysis of the current situation of human and organizational risk management, and suggestions for supplements and updates to the existing frameworks. We already have some standards, e.g. ISO 27001:2013, which was designed to support an enterprise information security management system. Today we require a much greater focus on people, culture, and relationships[10]. Therefore, we will give the discussion of the key human and organizational issues: collaboration and “crown jewels”. In addition the methods of establishing a secure collaboration system and protecting the ”crown jewel” will be provided. The environment, society, technology changes fast today, which also introduce many new risks, therefore, new risks will be identified. In this master thesis, we will uncover the elements that influence on human and organizational risk management as well.

1.8 Thesis outline

The master thesis has been divided into several chapters, the brief introduction of each chapter has been listed as following:

- Chapter 1 presents the introduction of the master thesis. This chapter includes the information regarding topic of master thesis, keywords, research questions, methodologies, justification motivation and benefits, claimed contribution, and the outline of the thesis.
- Chapter 2 presents the scientific background required to understand what does the existing frameworks cover about the human and organizational risk management. In addition, this chapter provides the information of the network society we live in today and the main potential risks in the future.
- Chapter 3 is about the analysis of dynamic change between human situation and human behavior. In this chapter, we describe several examples of different human situations with security concerns to support a threat model of information security, and also provide countermeasures to response these threats.
- Chapter 4 shows the analysis of human and organizational risk management issues: collaboration and “crown jewels”. We provide associated risks of these issues, and also give the methods of establishing secure collaboration system and protecting “crown jewels”.
- Chapter 5 provides the methodology of evaluating security spending in human and organizational processes.
- Chapter 6 is about new risks that we identified. We identified several new risks based on the futurist study, the analysis of the change of technology, society. In addition, we provide the associated mitigations and business impact of these new risks. At the end, this chapter presents the model for reassigning risks.

- Chapter 7 presents the overview of the new elements that we updated for the human and organizational risk management framework. In order to have a clear understanding, we use a mind map to show the new elements.
- Chapter 8 is about the recommendations for dealing with human and organizational risk management.
- Chapter 9 is about the interview discussions, and the direction of future work is also described in this chapter.
- Chapter 10 concludes this master thesis, and provides the achievements of this thesis.
- Appendix A, B, C, D present all the questions and answers of interviews.

2 Scientific Background

This chapter presents the theoretical background of this thesis. The chapter starts with an explanation of the society we live in today, the network society. Then, an overview of the existing risk management frameworks will be presented, which focuses on human and organizational risk management area, and further comparing the frameworks. As the thesis focuses on updating the existing human and organizational risk management frameworks, a hypothesis on the future dynamic situation and new risks is included as well.

2.1 The network society

Introduction of the Network Society
In today's society, our life and work are increasingly organized around network, which leads to the transforming of our society, and introduces a new notion: the network society. A network society combines between information, communication technology, and the human capacity, which brings innovation, creativity, and convenience to our social life. In the network society, connectivity will be the starting point for new ways of innovating, collaborating and socializing, which are about creating freedom, empowerment and opportunity, transforming industries and society[13]. Almost everything is been connected, as such, the network society is basically centered on mass media, and the foundation of the communication system of network society is interactivity[14]. While the interactivity is not just between messages and audiences, it is the key elements of the network society, which lets technology devices and humans work together. As such, we could have cloud services, broadband, 3G and more in our daily life.

Using networks has already become an important part of people's daily life. We create new value through networking by inputting humans' thoughts, intentions, intelligence and attributes. Thus it could mean that it is not technologies which change society but humans do. Today, individuals and communities empowered by connectivity are driving fundamental changes[15]. Due to this, the network does not only promote the level of individual social relationships, but it contributes to the economy, technology, culture as well. The connectivity is also transforming the whole industry and society, establishing new business models, creating job opportunities, and redefining established models for learning and education [15].

Network has become an integral part of our social life. With the internet and communication technology developing, internet population growing, from life to work and entertainment the daily life of people is closely connected with the network. The traditional way of work and life are greatly improved due to the emergence of the network, both in the realistic environment and the network environment[15]. However, the nature of network society is people interact among networks, thus no matter in our life or work, human behavior impacts today's society system.

Against the network society background, we need to think about how the human factor among network society should be managed in the future.

Trust in the Network Society
With the development of information and communication technologies, the globalization market, network economy has already become today's economic pattern. The development of network economy has caused great changes to modern corporations in almost every aspect[16]. In the network economy, businesses are connected with the internet technology, via it information, goods and capital is transferred. It is similar to the translations, the translator need to be loyal to both: their clients and their readers. Hence, trust has an ethical element to it. Same as the translations, trust is also a key issue with regard to network economy: without the support of organizational structures, the network needs to be "glued together" by trust relations[17]. As such, trust is competitive assets for all organizations. The network economy seems to win compared to the industry economy as it brings more space, time, labor and capital. However, it is difficult to build trust among networks. When the trust problems happened in the network economy system, it will cost so much on transactions. The overall use of information and communication technologies within the economy can also lead to the technical workers becomes an important competitiveness issue for the community[18].

The future network society
Towards the future network society, the wireless connectivity is the key[19]. Increasing amounts of digital and communication devices will expand into the society and private life. New forms of communication will emerge and the arising business opportunities are endless, and will span across all societies, organizations and individuals[20]. Under the help of wireless, almost everything can be connected. Therefore, we can transform, share and collaborate information more efficiently. As the pressure from the expanding use of technology and digital devices, organizations need to think how to structure work, and increase creative output[21]. However, the expanding of technology and digital devices has increased the need for security solutions that protect transactions, connectivity, mobility and identity against potential threats[21]. As such, security and network services will be the core issue among the whole network society.

2.2 The existing human and organizational risk management frameworks

This section, first provides an overview of some of the existing risk management frameworks and standards which focus on human and organizational area. Then, we present the comparison between these frameworks and standards.

2.2.1 Introduction to some of the existing frameworks

In order to supplement and update the existing human and organizational risk management frameworks and standards, it is important to have an understanding of what the existing frameworks and standards cover within the human and organizational aspects. There are many risk

management frameworks and standards, but we chose some of the frameworks and standards which are relevant to this thesis. These are the ISO/IEC 27001:2013 [22], ISO/IEC 27002:2013 [23], ISO/IEC 27005:2008 [24], NIST 800-30 [25], NIST 800-39 [26], COBIT 5 [27], Risk IT [28].

The ISO/IEC 27001:2013 was developed by ISO/IEC in 2013, and is used by internal and external parties to assess the organizational ability to meet the organizations' own information security requirements[22]. Compared with ISO/IEC 27001: 2005, the 2013 version standard puts more emphasis on measuring and evaluating how well the organization's ISMS is performing[29]. If we consider the human factor when we use this standard, it is essential to determine the needs and expectations of interest parties, and understand the internal and external issues that are relevant to their business objectives[22]. Leadership is an indispensable role in the whole organization so it is important to have a clear understanding of their responsibility. The standard presents the top management's responsibility within the organization's information security field, which includes that top management shall demonstrate leadership, as given in the following list[22]:

- Directing and supporting employees, promoting continual improvement.
- Top management shall build a corresponding information security policy.
- Top management shall ensure that responsibilities and authorities for roles relevant to information security assigned and communicated.

The standard also covers the section of competence, awareness, and communication, which presents that the organization shall ensure *"the persons are competent on the basis of appropriate education, training, or experience, be aware of the information security policy"* [22], and follow the policy of communication. In addition, the top management shall review *"the changes in internal and external issues and feedback from interested parties"* [22].

The ISO/IEC 27002:2013 is a general security standard, which helps organizations to preserve the confidentiality, integrity, and availability. Any organizations that adopt ISO/IEC 27002 must assess their own information security risks, clarify their control objectives and apply suitable controls[30]. The standard presents different areas of their related security controls. For the human and organizational field, the standard includes six controls which are divided into the "Organization of Information Security" and the "Human Resources Security" groups. In the group of Organization of Information Security, it presents the controls related to the roles and responsibilities for information security in the internal organizations, and mobile devices and teleworking policy. In the group of Human Resources Security, it demonstrates security controls of three different employment phases, namely: prior to employment, during employment, and termination and change of employment.

The ISO/IEC 27005:2008 is a guideline that help organizations how to assess security risks. All the organizations are very concerned about all kinds of potential information security risks.

This standard helps organizations to manage related information security risks, by providing the risk management process and all relevant actions. The standard gives definitions of information security risks as *"potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organizations"* [24]. The Annex C in this standard provides the examples of typical threats, and more than half of them due to human actions which can accidentally damage the information asset. It also provides a "particular attention" on the list of the human threat sources. The standard should be suitable for the organization's environment, hence it is important to evaluate the organization, and take into account the constraints which affect the organization. In the Annex A, the standard lists the constraints that includes different areas of the organizations. In regard to human risks, it presents the *"constraints concerning personnel"*.

The NIST 800-30 is a risk management guide for IT systems. It is publicly available at no charge. The standard starts with a brief introduction of the risk management, and then presents how it can be integrated into System Development Life Cycle (SDLC). Risk management is a management responsibility[25]. Thus the standard describes seven key roles of the personnel who should support and participate in the risk management process. The NIST 800-30 encompasses three processes: risk assessment, risk mitigation, and ongoing risk evaluation. The risk assessment phase covers 9 steps, it starts from system Characterization and ends of documenting the risks. In the second step-threat identification, it presents that *"motivation and the resources for carrying out an attack make humans potentially dangerous threat-sources"*[25]. The "Human Threats" table presents an overview of today's common human threats, their possible motivations, and the threat actions. This information will be useful to organizations studying their human threat environments and customizing their human threat statements[25]. The second process-risk mitigation, which covers several options that can decrease the frequency and magnitude of the risks. In addition, the NIST 800-30 explains how to do cost benefit analysis. The last section deals with evaluation and assessment of risk.

The NIST 800-39 is a risk management framework that focuses on managing information security risks with a view at organizational, business and information system levels, which includes framing, assessing, responding, and monitoring risks. From the perspective of human and organizational risk management, this framework gives how to address risks from an organizational view, trust and trustworthiness concept related to risk management, and the organizational culture. From the organizational view, address risk need to establish and implement governance structures that are consistent with the strategic goals and objectives of organizations[26]. At the same time the requirements need to be defined by federal laws, directives, policies, regulations, standards, and missions or business functions[26]. Among all the organizations, trust is an important concept. In this framework, it includes how to establish trust among organizations, and how trustworthiness can be used in developing trust relationships. No matter in which organization, the organization culture is the significant background for their risk management. There is a direct relationship between organizational culture and how organizations respond to uncertainties and the potential losses[26]. The organizational culture refers to the values, beliefs, and

norms that influence the behaviors and actions of the senior leaders/executives and individual members of organizations, therefore, it influences the risk management decision of the senior leaders/executives within organizations[26].

The COBIT 5 was developed by ISACA in 2012, and is a business framework that provides the governance and management of enterprise IT. COBIT 5 is not-for-profit and useful for all enterprises. Boards and management—both in the business and IT functions—must collaborate and work together, so that IT is included within the governance and management approach[27]. Because of this, the COBIT 5 provides 5 principles as following[27]:

1. Meeting stakeholder needs.
2. Covering the enterprise end-to-end.
3. Applying a single integrated framework.
4. Enabling a holistic approach.
5. Separating governance from management.

In all principles, COBIT 5 regards people, applications, technology, facilities and information, related data as organizations' main IT governance target. It provides managers, auditors, and IT users with a set of general measures, and indicators to help them get maximizing benefits through the use of information technology in a company. Managers, auditors and users benefit from the development of COBIT as it helps them understand their IT systems and decide the level of security and control, which is necessary to protect their companies' assets through the development of an IT governance model[31].

The Risk IT is an IT risk framework developed by ISACA for helping organizations to identify, govern and manage IT risk. It is integrated with COBIT 5. The Risk IT framework is divided into three domains, each includes three processes:

- *Risk governance*: establish and maintain a common risk view, integrate with ERM, make risk-aware business decisions.
- *Risk evaluation*: collect data, analyze risk, and maintain risk profile.
- *Risk response*: articulate risk, manage risk, and react to event.

This framework uses the quantitative method to assess risk through frequency and magnitude of IT risk scenarios. From the perspective of human and organizational risk management, the Risk IT framework divided the actor of risk scenario into internal and external, which means the people who generates the threat can be within or outside the company e.g. outsiders, competitors. In addition, it defines a number of roles for risk management and the responsibilities and accountability within the process. Therefore, when we deal with human and organizational human risk management, the potential risk actor should not take part in the process.

2.2.2 Comparison among these frameworks

In the comparison between some of the above frameworks and standard presented in Subsection 2.2.1, we try to find out what they do not cover for dealing with human and organizational risk management. It is common among some of the frameworks and standards that they provide the generic risk management process, however, these risk management processes are not suitable for human and organizational risk management due to lack of many parameters that need to be considered when we addressing human and organizational risks. Before we start comparing these frameworks and standards, we need to define the hypothesis parameters for dealing with human and organization risk management, which includes:

- Security controls.
- Risk catalogue.
- Human behavior analysis.
- Roles and responsibility.
- Specific consideration (collaborations, “crown jewels” etc.).

In the following Table 1, it shows the comparison of frameworks and standards, especially what parameters that each framework/standard that does not cover for dealing with human and organizational risk management.

Framework/Standard	**The hypothesis parameters of human and organizational risk management framework**				
	Security controls	Risk catalugue	Analysis of human behavior	Roles and responsibility	Specific consideration (collaborations, “crown jewels”, etc.)
ISO/IEC 27001:2013	Awareness, access control, training.	×	×	×	×
ISO/IEC 27002:2013	Security controls of employment.	×	×	The roles or responsibilities for information security.	×
ISO/IEC 27005:2008	×	Emphasis human risks.	×	×	×
NIST 800-30	×	Human threats table.	×	×	×
NIST 800-39	×	×	×	×	Give consideration for address risks form the organization view, trust and trustworthiness concept.
COBIT 5	×	×	×	×	×
Risk IT	×	It divides the actor of risk scenario into internal and external.	×	×	×

Table 1: Comparison of the frameworks and standards for dealing with human and organizational risk management(x, it means that the framework/standard does not cover this parameter.).

2.3 A hypothesis of new risks

Our life changes quickly because of the development of technology, environment and transformation in our economy and society. We cannot deny that it accelerates the development of social and the progress of humanity, however, at the same time it enhances new risks. Therefore, it's important to manage and understand the risks, and long-term thinking to address and mitigate them.

The Global Risks 2014 Report[1] maps 31 global risks. The report considers 31 global risks in five categories (as shown in Figure 1, 2): economic, environmental, geopolitical, technological, and societal. From the list table of global risks in [1], we can conclude that: except the nature environmental risk and food crisis societal risks, most of the global risks are man-made risks. For instance, in the category of economics, the identified risk *"fiscal crises in key economics"*, because of governments spending more than they raise in taxes, then they borrow money from private investors. While the investors doubt the ability of government for repaying the money, the government has to offer higher interest to compensate investors. As the cycle starts, it increase the fiscal crises. In the category of technological risks, the defined risk *"breakdown of critical information infrastructure and networks"*, people try to build the most secure information system, but humans are not machine, there will always be human errors by accident or purpose.

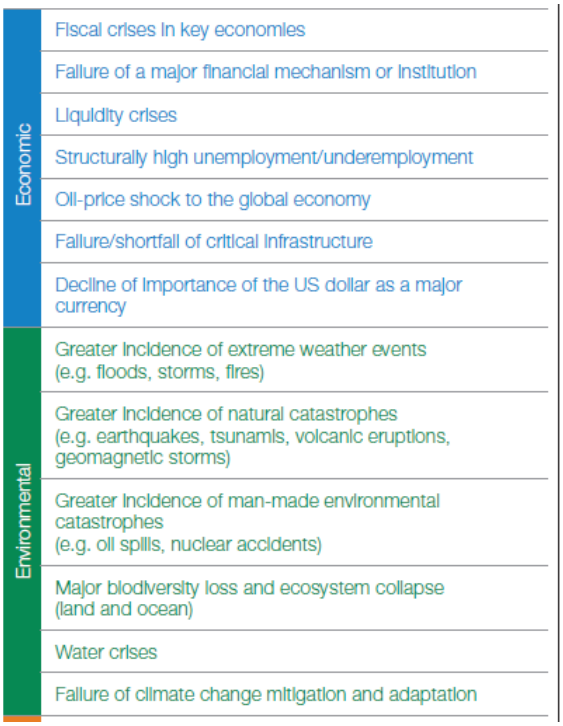


Figure 1: The Global Risk 2014 part 1 (taken from [1]).

Risk trends would be a very good way for organizations to understand the risks in the future. The Global Risks 2014 Report [1] held a survey that identify additional global risks. The following Figure 3 shows the issues that respondents mentioned most frequently. It has been gathered into three broad categories: demographic, societal and technological[1]. From the perspective of demographic, overpopulation, migration, and ageing population will be the critical issues, in which overpopulation should have more consideration. The continuous mining of human beings result in resource scarcity, overpopulations lead to global warming and rising sea levels, and communicable diseases can spread more quickly in densely-populated areas[1], which demonstrates that "growing population, growing risks". When we think about the societal concerns, trust among organizations, underemployment or unemployment for youth, civil wars, and healthcare funding challenge might be frequently highlighted. Technological concerns include data mismanagement, loss of privacy, increase in surveillance, and possible abuse of new and more complex information technology[1]. In the future, these technological risks will become more impactful because of the reason that the growth of "internet things" leads to everything gets connected online, which gives attackers more potential impacts of disruption. In addition, the ever-deepening of connectivity and interactivity among the devices makes it more difficult to predict these impacts.

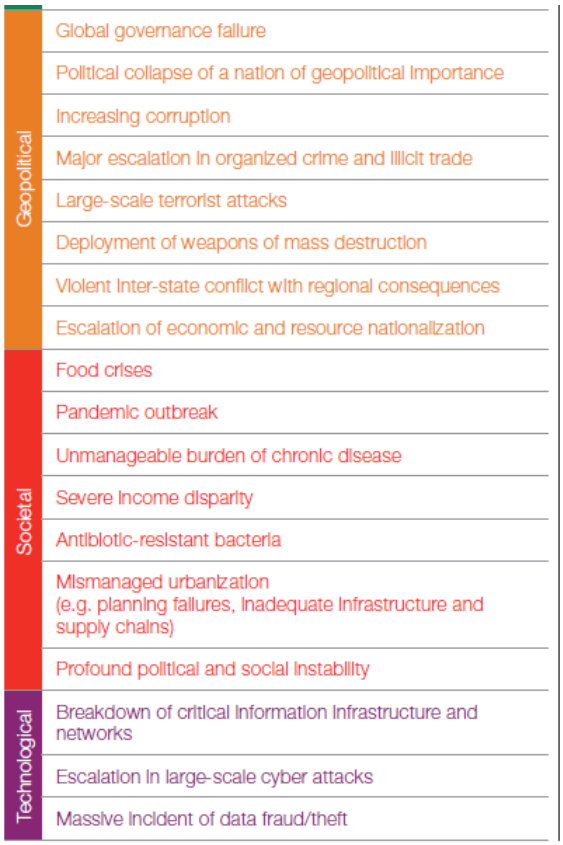


Figure 2: The Global Risk 2014 part 2 (taken from [1]).

Figure 3: Risk Trends (taken from [1]).

3 Dynamic change of human situation and behavior

3.1 Introduction

> *"In April 1997, the core of the internet suffered a disaster. Internet service providers lost connectivity with other ISPs due to an error in a routine internet router-table update process. The resulting outage effectively shut down a major portion of the internet for at least twenty minutes. It has been estimated that about 45 percent of the internet users were affected. In July 1997, the internet went through yet another more critical global shut down for millions of users. An accidental upload of a corrupt database to the internet's root domain servers occurred. Since this provides the ability to address hosts on the net by name (i.e., eds.com), it was impossible to send e-mail or access Web sites within the .com and .net domains for several hours. The .com domain compromises a majority of the commercial enterprise users of internet."*[32]

The opening quote describes a simple keyboarding error can cause worldwide internet outages, which also shows that how humans become the critical threat to information security due to human errors. However, until now a lot of organizations still prefer to focus on the solutions of technical issues instead of humans. Most of them believe that human errors are a kind of careless in information security. But, consider about the conclusion from[33] that *"Human error remains the greatest threat to data security across the health care industry"* and according to [34] at least 78 percentage of respondents indicated that their company had experienced a data security breach as a result of negligent or malicious employees. Therefore, we believe that this kind of careless in information security is unusual. A lot of literature indicates that humans are the weakest link in information security. Thus, we believe that human behavior has a crucial role in many security failures[35]. So what kind of human behavior can lead to the compromise of information security? The author of *The human factor in data protection*[34] identified 10 risky practices in which employees routinely engage, that are directly related to information security:

1. Connecting computers to the Internet through an insecure wireless network.
2. Not deleting information on their computer when no longer necessary.
3. Sharing passwords with others.
4. Reusing the same password and username on different websites.
5. Using generic USB drives not encrypted or safeguarded by other means.
6. Leaving computers unattended when outside the workplace.
7. Losing a USB drive possibly containing confidential data and not immediately notifying their organization.
8. Working on a laptop when traveling and not using a privacy screen.
9. Carrying unnecessary sensitive information on a laptop when traveling.
10. Using personally owned mobile devices that connect to their organization's network.

From the above 10 risks, it seems that employees only make unintentional mistakes and breaches were discovered by accident. Actually, not all human errors just happen unintentionally, most human behaviors are affected by their human situations. For example, the attacker who can gain access to highly confidential information through talking with the CEO who with an addiction for alcohol; or a member of staff experiencing what he considers unfair treatment, receiving a tempting offer from a competitor, he may turn against the organization. As a conclusion we can see that how employees perform themselves largely depends on their situations. The dynamic change between human situation and human behavior we named it as human factor. All the organizations are made of people, so the human factor would influence all the levels in any organizations.

The human factor can represent a considerable threat to information security for any business[10]. Thus, in this chapter we will discuss the dynamic change between human situation and human behavior. The discussion will be based on the different human situations: mental health, physical health, working status, conditions for life, and social relationship. For each situation, some examples of human behavior challenges have been given in order to fully understand the potential threat. A framework to countermeasure these challenges has been given as well.

3.2 Threat model

The area of knowledge for different human situation is vast and complex. Many human situations are not independent, as they in most cases affect each other. For practical purposes, and in order to scope this in this chapter, we will describe a few examples to depict security issues as a result of these different situations. Additionally, some security concerns will be described to support a threat model for information security.

3.2.1 Mental health

The World Health Organization (WHO) defines mental health as *"a state of well-being in which every individual realizes his or her own potential, can cope with the normal stress of life, can work productively and fruitfully, and is able to make a contribution to her or his community"*[36]. It is estimated that one in four people in the world will be affected by mental or neurological disorders at some point in their lives[37]. Around the world, about 900 000 people commit suicide every year, and one of the most prominent and treatable causes of suicide are mental disorders[38]. Therefore, mental health is the emergency issues among the world.

Culture difference, country-specific conditions, social diversity and biological factors all effect how mental health of a person should be. For example, intense social competition leads to employment pressure among humans are recognized risks to mental health for individuals and organizations. In addition, poor mental health is also associated with rapid social change, stressful work conditions, gender discrimination, social exclusion, unhealthy lifestyle, risks of violence and physical illness and human rights violations[39].

According to the WHO statistics, more than 450 million people in the world suffer from mental disorders during their life time. Depression hit more than 350 million people of all ages, around 50 million people worldwide have epilepsy, 47 percent of the adult population have headache at least once within last year in general. In Europe, every year 1 out of 15 people suffer from major depression, and nearly 4 out 15 people are affected. There are more examples, but the point and truth is that mental health challenges are more common and serious than we would like to: it is not only impact our health but information security as well.

The consequences of mental disorder for the individual are often sick leave, irrational behavior, and cannot concentrate enough during work time. What was worse, is that mental disorder could raise to suicide and serious accidents. These will lead to a critical issue for information security as irrational behavior leads to increased risk for compromising security.

As we mentioned before, the reason of mental health are result in different factors, it is complex. In this section we will describe a few examples to depict mental disorders. In addition, the associate security concerns will be described as well.

Depression

The definition of depression is: *"[..] a state of low mood and aversion to activity that can affect a person's thoughts, behavior, feelings and sense of wellbeing"*[40].

The following content describes depression and how common it is: *"Depression is a common illness worldwide, with an estimated 350 million people affected. Depression is different from usual mood fluctuations and short-lived emotional responses to challenges in everyday life. Especially when long-lasting and with moderate or severe intensity, depression may become a serious health condition. It can cause the affected person to suffer greatly and function poorly at work, at school and in the family. At its worst, depression can lead to suicide. Suicide results in an estimated 1 million deaths every year."*[41]

So many things can lead to the depression such as an accidental fire in their own home, loved ones lost their lives, divorce, bad weather, lost something that is important, problems among their own family and so on. These would make people feel sad, anxious, empty, hopeless, worried, helpless, worthless, guilty, irritable, hurt, or restless[42]. They may lose interest in activities that once were pleasurable, experience loss of appetite or overeating, have problems concentrating, remembering details, or making decisions, and may contemplate, attempt[43]. Being in such a situation you might not fight as hard as you normally would do, and ignore information security awareness and behavior in a project. For instance, some employees need to keep doing monotonous tasks day by day, such as programmer, which can lead to work fatigued and so much work pressure. As a result, it would have many human errors during the work time and raise to the information security breaches. As such, depression can cause considerable financial losses for a business as well as intellectual property value.

Headache disorders

The definition of headache disorder is: *"[..] a painful and disabling feature of a small number of primary headache disorders namely migraine, tension-type headache, and cluster headache"*[44].

The following content describes headache disorder and how common it is: *"Globally, it has been estimated that prevalence among adults of current headache disorder (symptomatic at least once within the last year) is 47 percentage. Half to three quarters of the adults aged 18–65 years in the world have had headache in the last year and among those individuals. Headache on 15 or more days every month affects 1.7–4 percentage of the world's adult population. Despite regional variations, headache disorders are a worldwide problem."*[44]

Headache can be a result of both biological facts and social facts. Such as substantial personal suffering, impaired quality of life and financial cost[44] all can result in headache disorder for the individual. Headache is not just painful, repeated headache attacks and often the constant fear of the next one can damage family life, social life and employment[44]. Such a situation is very difficult for people who has a headache to concentrate enough on their work, or even cannot do any job at that moment. As a result, it will have negative impact to the working project, e.g. deny the deadline or have many human errors, and it may lead to the compromise of information security.

Schizophrenia

The definition of schizophrenia is: *"[..] a mental disorder characterized by a breakdown in thinking and poor emotional responses"*[45].

The following content describes schizophrenia and how common it is: *"Schizophrenia is a chronic brain disorder that affects more than one percent of the population. When schizophrenia is active, symptoms can include delusions, hallucinations, trouble with thinking and concentration, and lack of motivation. However, when these symptoms are treated properly, a large portion of those diagnosed will greatly improve over time."* [46]

As a result of schizophrenia people would meet significant social and work problems. The disorder is thought to mainly affect the ability to think, but it also usually contributes to chronic problems with behavior and emotion[47]. As such, people who has the schizophrenia sometimes does not know what they do at the moment, and after it happened they have no memory of that time period, which can lead to irrational actions because of hallucination. Hence, the judgment abilities can be impaired when schizophrenia occurs, which will have negative influence or harmful impact when people taking decision or operating critical tasks. For instance, the database administrator deletes key records due to hallucination, which brings the compromise of the integrity or availability of information security.

Addiction

The definition of addiction is: *"[..] the continued repetition of a behavior despite adverse consequences, or a neurological impairment leading to such behaviors"*[48][49].

The following content describes addiction and how common it is: *"Addiction is a chronic brain disease that causes compulsive substance use despite harmful consequences. Health, finances, relationships, and careers can be ruined. The abuse of drugs and alcohol is by far the leading cause of preventable illnesses and premature death in our society. Addictions can include, but are not limited to, Alcohol, drug abuse, exercise addiction, food addiction, computer addiction and gambling."*[50]

It is common that people suffering addiction due to alcohol and drugs. Addiction is characterized by impairment in behavioral control, craving, diminished recognition of significant problems, and a dysfunctional emotional response[49]. The harmful use of alcohol is a global problem which compromises both individual and social development[51]. In the information security field, some of the employees need to have security clearance before they get employed. In order to get a security clearance, it is necessary to check peoples' background and history. Any drug abuse and alcohol abuse will raise a security concern, e.g. alcohol-related incidents at work: reporting for work or duty in an intoxicated or impaired condition. Therefore, if they find out that you are using any drugs or you are an alcohol abuser or dependent, you will usually lose the security clearance. In addition, you cannot trust a person who has an addiction. Depending on the type of addiction, it is very difficult for the addict's body or mind to stop it. If an addict is put into a position to choose between protecting information security and drugs, the person will most likely choose the latter one, as they cannot withdrawal it.

Bullying

The definition of bullying is: *"[..] the activity of repeated, aggressive behavior intended to hurt another person, physically or mentally, which is characterized by an individual behaving in a certain way to gain power over another person"*[52].

The following content describes bullying and how common it is: *"Victims of bullying are also at increased risk for problems with anxiety and depression. Some victims of bullying even attempt suicide in an effort to escape the ongoing harassment...Children who bully are at risk for future problems at work and in personal relationships. They also have an increased risk of substance abuse and legal difficulties."*[53]

It is very common that to be victimized by bullying at school among children. Actually, bullying has many different contexts, such as cyber-bullying and workplace bullying, which mostly happens among adults. As an adult, bullying might impact their self-esteem and work performance. Cyber-bullying is defined as any bullying done through the use of information or communication technology, e.g. posting or sharing fictitious or damaging information about an individual or organization. Workplace bullying often takes place within the established rules and policies of the

organization and society[54]. A culture of bullying in information technology is common. It leads to high sickness rates, low morale, poor productivity, high staff-turnover, deadline-driven project work and stressed-out managers taking their toll on IT workers[55]. In addition, being victimized by bullying can be result of financial problems. For instance, due to emergency financial need people would borrow money from usury, which leads to an exorbitant interest repayment. While some attackers would through this opportunity ask the debtor get some critical information instead of paying money back, which will lead to the compromise of information security of the organization.

Anxiety disorder

The definition of anxiety disorder is: *"[..] an unpleasant state of inner turmoil, often accompanied by nervous behavior, such as pacing back and forth, somatic complaints and rumination"*[56].

The following content describes anxiety disorder and how common it is: *"Anxiety is a normal reaction to stress and can actually be beneficial in some situations. For some people, however, anxiety can become excessive. While the person suffering may realize their anxiety is too much, they may also have difficulty controlling it and it may negatively affect their day-to-day living."*[57]

It is clear from above description that anxiety disorder combines anxiety and fear. Being victimized by anxiety disorder, people are often over worrying about everyday things and fear about the current situation. Anxiety disorder can be caused by, e.g. drug abuse or stress. Therefore, anxiety disorder often happens in conjunction with other mental disorders, such as, addiction, bullying, depression. Anxiety disorder includes different contexts: social anxiety disorder, separation anxiety, situational anxiety and more. Because of anxiety, people might be feel it is difficult to have social interaction, trust, and also want to avoid public. Being in such a situation, they might think it is difficult to protecting information security in an organization. The person would be too worried about information security and feel that everybody are watching at him/her, then it would be very hard for him/her protect information security very well. Another problem is the people who has anxiety disorder because of fear, will only focus of meeting the goal. If he does not meet the goal, he would be fired. As such, he could neglect the security policy and strategy, which could harm the organization.

3.2.2 Physical health

The World Health Organization defined health as *"a state of complete physical, mental, and social well-being and not merely the absence of disease or infirmity"* [58]. Therefore, physical health is one important element of good health. In our life, lots of people defined physical health as the physical condition of our body, and it can be impacted by many factors, such as: lifestyle, biologic factors, and environment. The poor physical health not just impact the physical condition of your body, it might cause mental disorder as well.

We mentioned the factors that affect physical health, but, how do these factors affect physi-

cal health? Lifestyle, which can defined as how you perform your life every day, it includes diet, emotional health, physical activity, and behaviors. The total sleeping time is a problem for so many people, especially the employees who have to have additional work or the stress from the deadline of their project. Humans' physical health is a cycle system, therefore, the less sleeping time the worse physical health. In addition, it would lead to the inefficient work or have many errors during working time. Another factor is the human biology, which here relates to the diseases we might have. Diseases have two aspects: incurable and curable. Curable diseases can be treated by different ways, while incurable diseases will not only affect the health condition of their body, but also could cause mental disorder. An example is given: the disabled people, a lot of social elements lead to them cannot have job, cannot have a normal life. Under this situation they become self-abasement, as a result, they are more likely to suffer from depression. The third factor is environment, which includes the place we live, weather, culture, the people around us. The environment factor is changing over time. There still exists some risks factors which can increases the likelihood of poor physical health, such as, underweight, high blood pressure, tobacco and alcohol consumption, unsafe water, sanitation and hygiene[59]. The risk factors requires us to pay attention to these problems related to physical health.

Because of poor physical health, people cannot have enough concentration on their work, which affects their judgment and also they might need to bypass security mechanisms to get their job done. Even though most of job mistakes happened unintentionally due physical health problems, it still can compromise the information security of the organization. The following content will include several examples of poor physical health situations and together with their security concerns.

Parkinsonism

The definition of parkinsonism is: *"[..]a progressive disease of the nervous system marked by tremor, muscular rigidity, and slow, imprecise movement, chiefly affecting middle-aged and elderly people"*[60].

The following content describes parkinsonism and how common it is: *"Globally, it is estimated that 7 to 10 million people worldwide are living with Parkinson's disease. Incidence of Parkinson's increases with age, but an estimated four percent of people with PD are diagnosed before the age of 50, 15 percentage before the age of 40 years. Men are one and a half times more likely to have Parkinson's than women."* [61]

Based on the above description, being victimized by parkinsonism, people has trouble with controlling muscle movement throughout the body. Like, it is hard to control muscle around their arm, hence, they can't control their actions when their hands tremor. Even worse is that parkinsonism cannot yet be cured and sufferers get worse over time as the normal bodily functions, including breathing, balance, movement, and heart function worsen[62]. As a result, it is difficult for people who suffers parkinsonism stay at the public area for eating and working, because they will feel embarrassed and nervous when other people notice their hands tremor. Due to

the effects of parkinsonism, some accidental errors could be happen during work time. Such as people deleting critical information unintentionally due to their hands tremor, which may lead to the compromise of the integrity of information security.

Insomnia

The definition of insomnia is: *"[..] a sleep disorder in which there is an inability to fall asleep or to stay asleep as long as desired"*[63].

The following content describes insomnia and how common it is: *"Insomnia affects approximately 30 percent of the general population. The most strongly associated factor underlying poor sleep quality was perceived stress, followed by job dissatisfaction, being unmarried, poor bedroom environment, lower academic attainment, younger age, and hypertension."* [64]

Insomnia is a highly prevalent phenomenon among adults. Today, due to so many social factors, e.g., work pressure, financial problems, have problems at home, the population of suffering insomnia has a gradually growing trend. Insomnia impairs cognitive and physical functioning and is associated with a wide range of impaired daytime functions across a number of emotional, social, and physical domains[63]. Compared with good sleepers, people with persistent sleep disturbances are more prone to accidents, have higher rates of work absenteeism, diminished job performance, decreased quality of life, and increased health care utilization[63]. The consequence of these is that it could lead to the neglecting of an information security project, human errors when you deal with information security issues etc. As such, poor sleep quality are not only the individual problems, considering the productivity and safety it also is the organizational and societal problems.

3.2.3 Working status

Working status is a topic that we need to face every day, which includes workload, working time, working environment, and co-workers. Today, with the advanced development of technology and the demand in all aspects of life, many jobs need people working 24/7. Long time working is not only physically demanding but is also mental requirements. In such situations, many employees become unsatisfied with their job, which could lead to employees avoid meetings, tasks, or showing up to work. As a result, it might bring security breaches to the company, for instance, core people leave company and take the critical information with them. In addition, due to the not optimistically global total economic situation, so many organizations use the strategy of reorganization, which is an important information security problem as well. As explained in A, when we restructuring a company, every time the new structure of a company and a new strategy will lead to the company consistently changing and you will lose control, which results in compromise security of the company easily.

Many information security risks happened due to the irrational working behavior, while most of the working behavior is depending on or related to their working status. Therefore, in the

following paragraphs, we will give several examples with information security concerns in order to introduce how the working status bring the breaches of information security.

Anytime, anywhere working

With the development of information technology and internet, our society has been totally networked. It is very common that smart devices which are enabled by wireless data networks are around our life anywhere anytime. It is not just used for entertainment, mostly it is used for the business. Anytime anywhere working is a new option of usage, under this situation working place become very flexible. Today, instead of being shown to a department or desk, employees can choose to work remotely, like working at home and access to their business email, documents, processes and solutions. We cannot deny that the anytime anywhere working brings many and varied benefits, such as: increased productivity, reduced costs, location flexibility, improved customer relationship etc. However, everything is a double-edged sword, anytime anywhere working is no exception as well. Examples will be given in the following paragraphs.

For the business people, there is too much working time is spent "in flight". They are moving from building to building, and traveling by plane to visit global locations to see their clients. Every morning there are thousands and hundreds of business people at the airport waiting for their flight to travel to another location because of the business need. Some people choose to work on their laptops during waiting time, what was worse some of them used to deal with their business during flight time, as shown in Figure 4. It is very easy to disclose important business information as others can monitor the work for a long time. As a result, it could compromise the information security of the organization, or the competitive organization could get your critical information, which means you might lose a competency area.

In addition, every week more than thousands laptops are lost in airports, and most of lost laptops are never reclaimed. Many of the lost laptops store the individual information of their owner and the sensitive corporate information that is carried by business traveler. As a consequence, it can compromise the confidentiality of information security in their organizations. Next time you travel, we advise that you do not share your business secrets with your neighbor passenger, and do not forget your laptop while traveling.

No peer control

Peer control is defined as *"It occurs when employees pressure others within their team or work group to perform up to or in excess of the expectations of the organization"*[65]. As the definition said, peer control exists when co-workers seek to monitor and influence each other, therefore, no peer control means employees work independently, without any influence and monitor from co-workers. Under the situation of no peer control, people could make errors more easily by accident for no restricted co-workers give advice or monitor their performance, or intentionally delete or copy the critical information of the organization. As a result, no peer control leads to higher possibility of compromising information security in the company. Such threat also existed

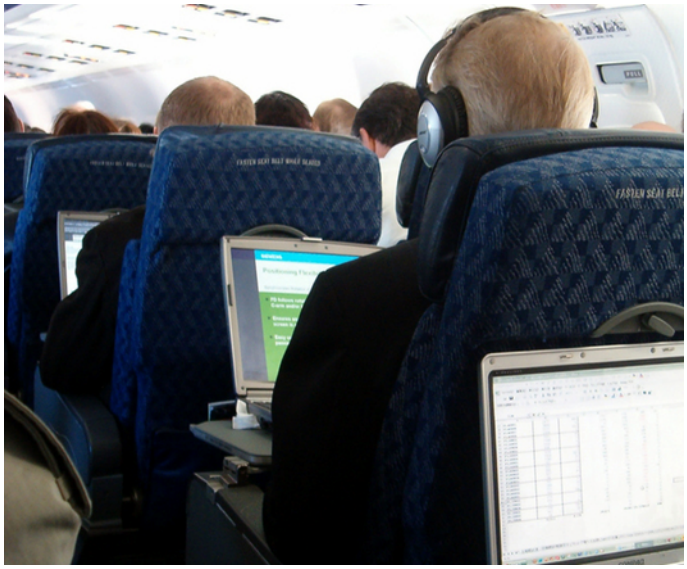


Figure 4: Dealing with business during flight time (taken from Google).

when people choosing to work remotely working that employees are not mandatory ask working around a desk inside the organization, they could just be working at home if they meet the requirement of the position. Working at home by themselves is no peer control, and could raise to some potential information security risks to the organization, e.g. copy classified information to some mobile devices.

Burnout

Burnout is defined as *"a prolonged response to chronic emotional and interpersonal stressors on the job, and is defined by the three dimensions of exhaustion, cynicism, and inefficacy"*[66]. Simply stated that burnout is resulted in long-term exhaustion and diminished interest in work. As such, burnout can be a significant problem in an organization. Burnout relates to both physical health and mental well-being. The job performance of burnout workers declines and they become less effective with co-workers, in addition, their negative attitudes also could spill over into relationships with their family and friends, making their entire world less bright[67]. Burnout has already become a high-profile issue in the information security community, and it continues to be a problem[2].

The online slide [68] gives a survey result of burnout in the information security, it shows that 94 percent of workers think it is stressed work in the information security field, and 10 percent of them believe it is extremely stressed, and one of the biggest stressors is job satisfaction, which is 55 percentage. Some people said that burnout is a result of work demands rather than other situational factors. In the online slide [68], there is another survey result proved it. Namely, the least people like in information security field is that employees have to tolerate bad business

decisions, endure the bad attitude from management, snobbery etc. Therefore, the personality that excels at information security is also highly susceptible to burnout[2]. The Figure 5, shows that compared to the general population, information security workers are more affected by exhaustion and cynicism. The reason for this is that the information security culture and employers have extremely high expectations from employees.

Generally, there are several reasons that result in burnout. When working too much, people feel constantly overwhelmed, stressed and exhausted, and they cannot recover from burnout for by taking time off. Secondly, it is due to the unjust environment. Another reason is that information security employees believe that no matter how hard they work it is unable to affect the change, so it is hard for people to keep motivated. The fourth reason is insufficient reward, whether the currency is money, prestige, or positive feedback[2]. The consequence of burnout can be that employees suffering depression, financial losses to the organization, and it also could end in suicide.

No corresponding security policy

In an organization, the security policy means how an organization plans to protect the organization's physical and information technology (IT) assets[69]. Today, a lot of organizations do not have their corresponding security policy, which means there is no statement that can address the behavior of the employees. As a result, it could result in information security risks in the organization. For instance, lack of proper policy for classifying information, the employees do not classify all information, or when they classify it is common that the information is classi-

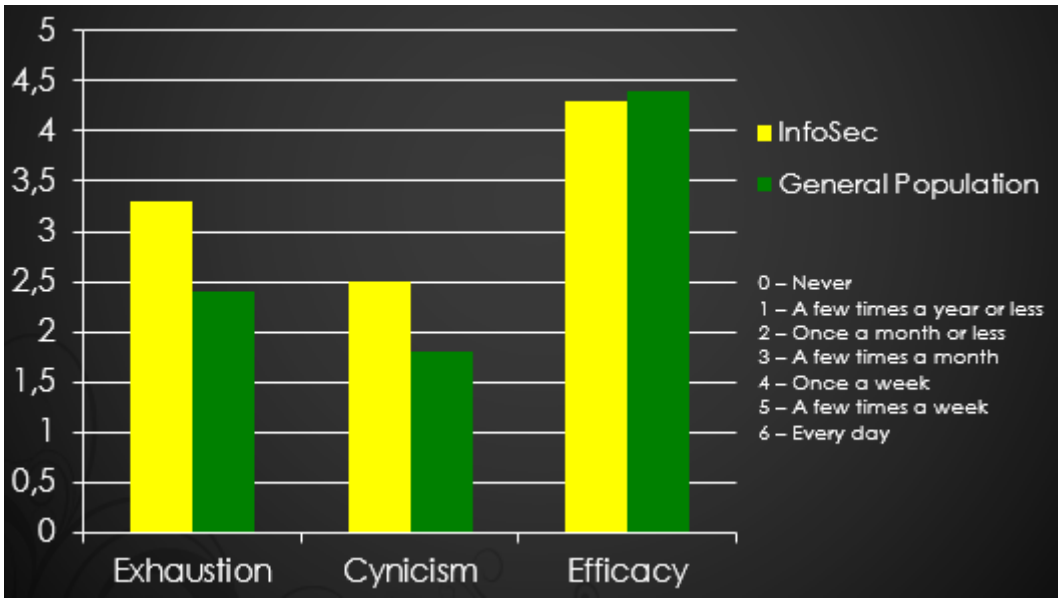


Figure 5: Information security Burnout survey results (taken from [2]).

fied incorrectly, which lead to too many people may get access to very confidential information. Another common example is employees do not encrypt with disks, consequently it might bring some potential threat to the information security of the organization.

3.2.4 Conditions for life

Conditions for life means circumstances needed for physical or biological life to exist, which includes living conditions such as food, safety, quality of house, and other factors, e.g. income, quality and availability of employment, incidence of disease, cost of goods and services, economic and political and stability[70]. People work not only to achieve their career objectives, mostly, they want to work to support their life and family goals. As such a situation, people's working performance or behavior could be impacted by their life situations. Hence, bad conditions for their life might affect the productivity level of the employees, or lead to irrational behavior, which result in the company could lose confidential information, e.g. clients list, and some important projects turned aside due to low working efficiency. Here is an example: because of the accidental fire, the employee's house has totally been destroyed, so it is very difficult for him focuses enough on his work. In such a case, it is very easy for him makes some errors during working time, e.g. leave his working desk without locking his laptop, or send an important e-mail to a wrong person. These errors all will bring hazards to the company's information security. Another example is, due to the emergency need of lot of money for personal reasons, the employee might sell some confidential information, such as important customer information or new product information to the competitive company for exchanging of a lot of money.

3.2.5 Social relationship

We defined social relationship as any relationship between two or more individuals. Today, due to fast development of information technology, the interactivity among humans is not just limited to people's face to face communication, the new information technology, e.g. Internet and many applications, brings so much convenience for people when interacting with each other. However, in most cases, people ignore the hidden hazards to the information security. We divide social relationships into two types: one is the relationships among social networks, like general friends, business partners and outlander. Another one is interpersonal relationship, it is not only based on communicating with each other through social networks, normally, it includes family members, good friends, and co-workers. The following consists of two examples that shows that how individual social relationship affect their behavior and impact the information security.

Social Network

Humans have been social networking for a very long time, dating back to when we started talking to each other. In the past, the main forms of social networking were only talking, writing and sending letters. With the advanced development of information technology, we start using e-mail, Facebook, Twitter and some other forms to social network with the help of computers. What does the term social network really mean? Wasserman defined social network as following:

> *"A social network is a social structure made up of individuals (or organizations) called 'nodes', which are tied (connected) by one or more specific types of interdependency, such as friendship, kinship, common interest, financial exchange, dislike, sexual relationships, or relationships of beliefs, knowledge or prestige."*[71]

With the popularity of the network, social networking also attracts mass popularity. Increasing amounts of employees have their personal networks. Normal supervisors and more administer numbers are not really willing to support content wise the employee. Today, social network already became an Internet-based application that allow users to create profiles and share content easily with other users. Therefore, modern employees discuss their job with their personal networks members and other experts to get solutions. In addition, as all the companies need to communicate quickly, there is no doubt that social networking can bring the speed of communication, as well as the power of people.

Use of social networks can also have unexpected consequences. Social networks are becoming an integral part of people's personal and business worlds. It is a collaboration between colleagues, but it also put risks into corporate information assets and reputation of business, e.g. share the critical information with others. In respect to security, especially the sensitive information, this behavior should be questioned. Today, more and more risks of using social networks have been exposed. As such, security professionals get nervous about this new communication technology - social networks. Therefore, we believe that it is necessary to define several current information security risks due to the use of social networks.

1. **Loss of reputation**
   An organization's reputation is its intangible asset. Any negative impact may lead to that the organization is less trusted by the customer, which will no longer wish to conduct business with them. An organization should be aware of who is talking behind their back and talking about them, whether the discussion is positive or negative[72].

2. **Piracy and Copyright Infringement**
   The piracy and copyright infringement always has been included by the digital form work product. If a published book is scanned and posted to the Internet as an e-book, the publisher will lose book sales because of traded or downloaded for free[72]. It also includes any type of software, digital copies of music, and movies. This phenomena are very general in China. The people living in China can download so many pirated software, movies, music from the Internet and can also by some counterfeit CD from the video store. These all resulted by people who through using social networks like Facebook, blog, Weibo to advertise the pirated content and provide the access links, which is illegal. And in an organization, it can be put at legal risk if an employee posts or reposts content without permission[72].

3. **Identity theft**
   Identity theft is common that if people want to participate in an Internet society, they have to provide their personal information for the registration. In another situation, attackers can get more individual information because people usually posted their personal data on

the social network. This information might be used for identity verification, e.g. birthday. This data can be used by criminals to impersonate an individual, usually in order to gain access to resources such as a bank account, or to obtain credit or other benefits in their name[73].

4. **Physical safety**
   As we mentioned in the last risk scenarios that social network user may post their own information on their own web page, which may include their address or location. In some organization's website, we also can find their specific address easily. Such online activity can lead to actual physical attacks, which are particularly relevant for individuals who have sensitive roles or positions within society[73].

5. **Recruitment**
   Social network websites are increasingly used during recruitment processes[73]. It is very common in Norway as well. 1/3 of the Norwegian population use social networks to find their dream job. In order to get the job there are many steps we should follow, like register, build on-line CV, chose position etc. Such behavior may give the possibility of identity theft, and people may be wrongly excluded from a position as a result of content linked to their identity, on social network sites[73].

6. **Malware**
   Malware can spread through social networks in different ways. Such as malware will utilize popular communication tools, like worms through emails and instant messages, and Trojan horses from websites and virus-infected downloaded files shared from peer to peer connections[74].

Interpersonal relationship

Interpersonal relationship are social associations, connections, or affiliations between two or more people, which is based on love, solidarity, regular business interactions, or some other type of social commitment [75]. Normally, interpersonal relationship is established because of individuals who share common interests or goals. Therefore, any period of interpersonal relationship mostly depends on individual factors, such as: personal development, interpersonal needs, working requirements, living environment, individual needs that include emotional and material needs etc. However, due to the change of individual elements and environment, interpersonal relationships cannot keep unchanging forever. For this reason, it could bring negative or harmful impacts.

"From a socio-technical perspective, a digital divide in information security can be viewed as consisting of the existing differences with regard to information security skills and knowledge, perceptions of information security, social norms, and interpersonal relationships, any or all of which can result in differences in information security performance between individuals"[76]. Therefore, the change of interpersonal relationship could lead to hazards to information security. We will discuss this problem from two aspects: change of individual elements, change of environment.

Mostly, people believe that family is very important among their life. While, lots of employees think that it is difficult to keep balance between work and family. Especially for women, work-family conflict always existed among them. As such, asking for leave and work incapacitation for long enduring periods is a common phenomenon for many organizations. In addition, loss of family members or divorce can affect individual working performance as well. These situations could result in depression, or addiction due to too many negative emotions, which results in many errors and lack of focus during working time. Consequently, it will represent a serious threat to information security, such as data leakage due to recklessness and intoxication, which is a serious information security concern.

The change of environment includes both living environment and working environment. Here we will give a simple example of change of working environment with security concerns. Many organizations face the challenge of fast change of personnelB. Thus, for the employers and employees, they lack of long term relationships. As a result, trust and loyalty would be a critical issue among them, especially for the information security management system of organizations. They could question all the working mistakes because of distrust, even though it is an unintentional errors.

3.3 Countermeasures

Understanding and managing the human factor in information security is vital. Human factors are not like technologies that you can calculate how much the organizations invested, gain or even lost. It is difficult to use numbers to measure how much you have gained or lost due to human factors. Therefore, it is significant to have the proper countermeasures to deal with human risks in the organization. It is important to have leader and management support information security. Managing human factor is no different. Without leader and management support it is hard to get the resources needed to implement countermeasures, security policies and security controls. In previous Section 3.2, we discussed the dynamic change between human situation and human behavior with security concerns, in this section we will suggest several countermeasures for how to response these problems.

3.3.1 Managing relationships

Security manager should be good at managing relationships[10]. In order to survive in the security world, security managers have always needed to network with other security managers to gain privileged knowledge about recent incidents and emerging security threats[10]. In addition, for achieving the business objectives, security managers also need to communicate with business managers, customers and colleagues to ensure they fully understand the importance of information security for their business.

Relationship management is, in fact, a well-understood, long-practiced art[10]. As a security

manager it is not only important to tell employees about our achievement, working objectives, but also asking them about their own, such as their interests, life situations, previous working experience, and understanding as well as supporting their culture. Background research can work very well for building a good relationship between managers and employees. For instance, you could know their personal achievements, family details, personal details, which makes them feel important. It is recommend to listen to others and help others, which also help security managers to better understand their motivations, priorities.

The better relationship between security manager and employees, the more trust and understanding could exist between each other, at the same time, the less human threats due to the dynamic change of the human situation.

3.3.2 Caring

It is essential that manager care about his employees' work, life, health, interests, family etc. As employees usually feel better if they are happy at work, it is up to managers to create happiness atmosphere. Caring can help employees to feel motivated and happy, and it can also increase the quality and productivity of information security tasks. On the contrary, if a manager does not have the skill for caring, the business would be in an unoptimistic situation due to the manager has a poor insight to his employees, so we can say that this manager cannot manage human factor very well. Argenti and Forman [77] provided several methods of how to care for employees.

- *"Create an atmosphere of respect."* In so many cases, managers always focus on employees who can create the most business value, but ignore the employees who just have an ordinary working performance. It is important to establish the organization culture that respect for all staffs, which could bring more active affects to the organization.
- *"Treat employees as insider."* Treat employees as your family members or close friends. Make them feel a sense of belonging. Think about the employees first, not the working partner or programs.
- *"Build up corporate loyalty."* By treating employees with respect and including them in important decisions, you are more than likely to get loyalty from them in return[77].
- *"Increase two-way communications."* Managers should be willing to listen to employees' feedback, advice, be willing to help them solve problems, and give proper suggestions. In addition, a manager could through communication get a deep insight of his employees various situations.

3.3.3 The help of professionalism

Due to many reasons, some organizations need to restructure. Many security managers regard restructuring as an irritating distraction[10], e.g. loss of control. In order to decrease the negative impact of restructuring, we need the help of professionalism.

Professional development should not just focus on security managers, as all the staffs should be included. If the organizations do not train and develop their staff, they will face a major crisis. Professional development of staff should, in fact, be a major, long-term goal and consideration[10]. Education and practice is the critical requirements of staff improvement. However, as David Lacey [10] said: *"we have nowhere near enough professional information security training available, and many information security stands are not entirely clear"*. Thus, development of a comprehensive information security training program is fully required. Nonetheless, we still have some ways to develop and train our staff. Such as, put more people on the course of information security, during recruited time the organization should prefer the candidate who has information security professional study background, or the organization can arrange staff with part-time or full-time information security training. We cannot deny that this kind of training program is expensive, but after training and development they could deliver high qualification of information security services or information security functions, and at the same time it can decrease the level of security incidents[10].

3.3.4 An effective awareness program

An effective awareness program needs to have a fully understanding of the organization's business areas, key problems areas, and the root cause of the incidents. Every company should have their own awareness program, and the awareness program should adapt to the company as well. Therefore, a proper effective awareness program could help the company manage the threat which due to the dynamic change of human situation, especially the human threats caused by the change of working status.

It is difficult to establish an effective awareness program which is suitable for the company. The first step of establishing an awareness program is to find out what people know and think about security awareness, as well as how they behave. David Lacey suggested to regard questionnaires as a survey method, which could help to better understand user requirements, and at the same time they could provide valuable information to help shape policies and controls[10]. In addition, we could get help from other professional supports, such as copywriters, behavioral psychologists and other experts, which might rarely relate to information security, but could serve as an useful indicator to identify the behavior that within the company[10].

Training and education are two important components of establishing an effective awareness program. The NIST defined training as:*"The 'Training' level of the learning continuum strives to produce relevant and needed security skills and competencies by practitioners of functional specialties other than IT security"*[78]. As such, training could help staff perform the proper and professional information security function. An example of training is some companies provide e-learning of information security to their employees. Education is different from training, which strives to produce IT security specialist[78]. People who have such education need to learn great amount of knowledge and skills, it includes theory, standards, principles, concepts. For example, in order to become more professional and master more knowledge and skills in information security

field, there are lots of experienced information security officers return to school and study for their information security master degree.

3.3.5 Changing behavior

Irrational human behavior can lead to the compromise of information security. We believe that change behavior would be an effective measure. However, it is difficult to change behavior. Changing behavior is not just a simple communication progress as human behavior depends on human motivation, human attitudes, environment and other social, technical, physical factors. Rules, commands, orders, instructions and policies are rarely effective for changing behavior. For this reason, David Lacey[10] suggested several methods that can help to change behavior:

- *"Reward beats punishment."* A lot of managers regard both reward and punishment as approaches to courage, restrict, and manage employees. However, they did not notice that punishments definitely lead to people become de-motivated, people who was being punished would hold a long-term grudge[10]. On the other hand, reward can inspire and motivate people. Managers should reward employees more than they punish them, and of course it is very important to give a fair, reasonable and consistent judgment.
- *"Environments shape behavior."* There is no doubt that people will behave very differently in different environments. The size and shape of a working place will have a significant influence on people behavior. A good design and state of physical environment can encourage people to behave in a consistent, disciplined way[10]. Therefore, it is important that organizations should take greater care when they design physical environment.
- *"Enforcing the rules of the network."* It is important that the organization enforces all staff to comply with the rules of the network in order to qualify the behavior. It is even more important to set down the rules when it comes to surfing the internet, or engaging in social networks[10]. The rules could include: not share any confidential information on public websites, not download any inappropriate documents, and obey the disciplines of using network.

3.3.6 Work smarter, not harder

In the information security field is not based on working harder, but to work smarter. Working smarter needs valuable thinking, which can bring creative improvements, and high qualification of the information security service. An example is given by Gonzalez[3] where he describes an improvement process towards a cyber security reporting system (CSIRT). The Figure 6 shows how "work smarter, not harder" improve the security level in a cyber security reporting system.

In the Figure 6, a plus sign indicates a causal influence in the same direction and a minus sign indicates an influence in the opposite direction[3]. This figure demonstrates how the CSIRT react for two different options: B2-Learning from incidents (Work smarter) and B1-Coping with incidents (Work harder). From loop B2 and B1 we know that both options could help CSIRT decrease the performance gap between "Actual CSIRT performance" and "Desired CSIRT incident

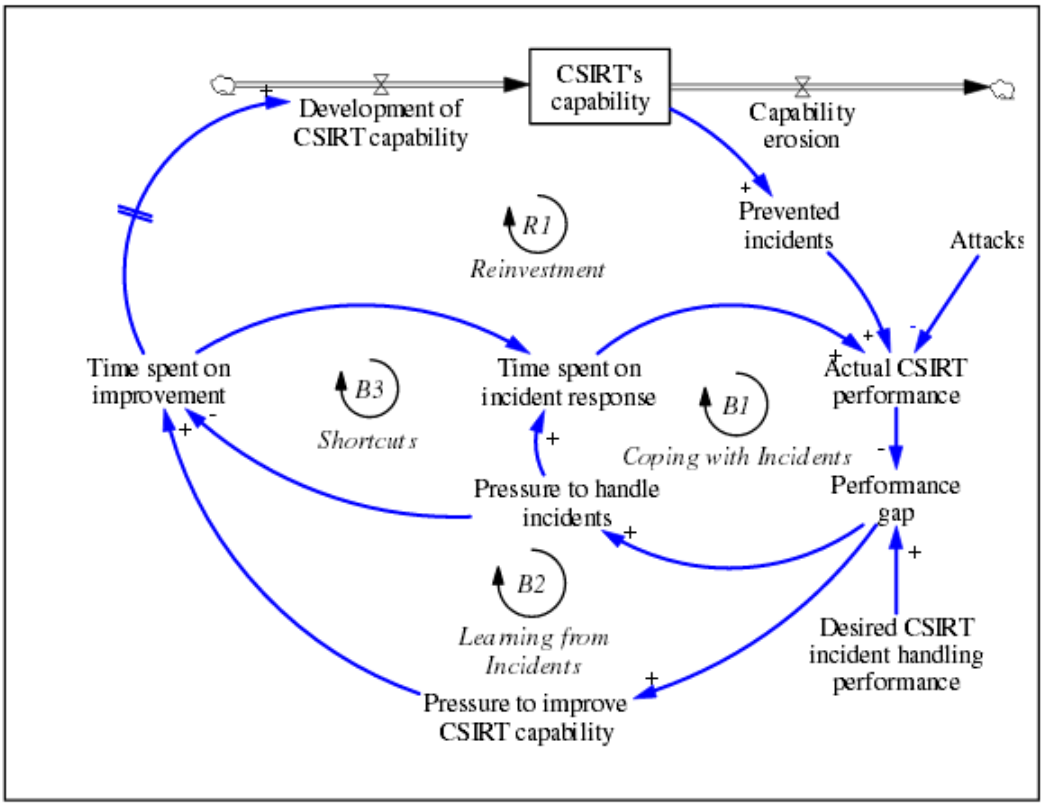


Figure 6: Basic system dynamics model of CSIRT performance[3]. (taken from [3])

handling performance". However, from simulation result of CSIRT, shown in Figure 7, we can see that choosing to working harder (more coping with incidents) gives a "better-before-worse" response; opting for working smarter (more capability development through learning from incidents) yields a "worse-before-better" situation[3]. Therefore, it is important to choose work smarter, not work harder.

Because of the culture habits, "work smarter, not harder" cannot always be applied very well. For example, China is a big country with lots of human labor. In China, the human labor is largely needed by agriculture and processing industry due to lot of production need to be produced by their hands. Under such a situation, working harder works better than working smarter. Therefore, there are some limitations for applying the countermeasure of "work smarter, not harder", not everything can be changed due to it.

3.3.7 Long-term management

As we discussed in Section 3.2, a lot of reasons could lead to the irrational human behavior. No matter if they are physical reasons, mental disorder, social relationship, or working situations.

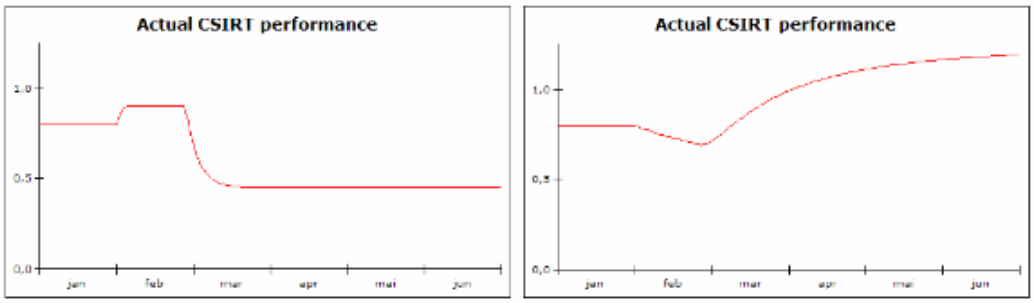


Figure 7: Simulations of CSIRT. The right side is the simulation of "Learning from incidents" (Work smarter). The left is the simulation of "Copying with incidents" (Work harder). (taken from [3])

Ultimately, they can all lead to the breach of information security or huge economic losses. So managing, avoiding and mitigation these human risks is an emergency issue for the information security community. Due to the variable dynamic change between human situation and human behavior, we suggest that long-term management could be an effectively countermeasure.

Long-term management, which needs periods of time and the support from the leader in order to manage, examine and help the staffs. The long-term management starts from the time of recruiting. HR department needs to know and check the background of the candidates, which includes study background, family background, hobby, physical health situation, previous working experience. Social network platforms can be used to know more about their personality as well, e.g. Facebook and Twitter. Once they start working in the company, the manager could use the employees' performance to decide if they are some potential threat. This judgment could depend on the following methods:

1. Examine the person's things that outside of the work, such as relationships, mental health, family situations, interest, which could lead to working stress.
2. Try to find out that if the job role and the career fit the employee's personality and natural talents [2].
3. Examine if the employees share common values with the organization.
4. Care the employees, not only their daily work, but also their life.

In addition, the employees to be implemented in the long-term management as well. If the employee discover areas of stress and conflict, start building longer-term plans to resolve them, or once the employee creates a more compatible work life, perform self-checks to make sure they don't recreate the problems that drove you to unhappiness[2]. After the recruitment, the manager should make sure that the people who leave cannot bring any important information away from the company. The company should make sure that the employee has no hostile feelings toward them.

4 Human and organizational risk management issues

4.1 Collaborations

Collaboration is the key to successful information security [79]. For example, the organization's threat intelligence improved when it collaborate with other organizations. Collaboration brings so much benefit to the development and improvement within the information security field. However, how secure the collaboration can be is still a critical issue that we need to think about it. How do we build a secure network communication? How can we improve trust of security among participants that take a part in cloud platforms that store common information? There are a lot of questions need to be questioned and many human issues need to be managed when we deal with collaborations within information security.

4.1.1 Introduction

Originally, people defined collaboration as working together to do a task and to achieve the common goals. Today, collaboration is not just limited to "working together", it involves the culture, strategy, communication, people, etc. There are many collaborations that fail to deliver on promise, and there are many reasons for this. Additional problems are related to that trust is not build among collaboration partners, strategies are unreasonable, no secure collaboration tools, etc. Due to the fast development of technology, Internet, and environment, our society has been totally networked-almost everything is connected. When we are collaborating, we are instead of person to person, using cell-phones, Skype, cloud services, video conferencing, etc. to achieve our business goals. The quick change of technology and networks bring us so much convenience, but brings us also threats on information security. In the following, we will give a typical issue to explain our viewpoint.

- **Video conferencing** It is very common to use video conferencing as a collaboration tool for organizations during their shared business time, especially for the organizations that are located in different cities or countries. It is important to address security concerns when we use video conference for business tasks. The security concern includes: security of the end-points, eavesdropping on the video or audio portions of a connection (meeting security), denial of service attacks, administrative security[80]. For example, millions of Yahoo web-cam users were targeted by an UK agency (GCHQ), and millions of Yahoo webcam images were intercepted by GCHQ, GCHQ state that a surveillance program code named Optic Nerve collected steal images from Yahoo webcam chats in bulk and saved them to agency databases, regardless of whether individual users were an intelligence target or not[81]. This attack can be performed because the web camera streams were not encrypted as they were sent between the Yahoo users.

Ultimately, the final reason of the collaboration's failure is that the collaboration system is insecure. So how secure can a collaboration system can be? We believe that it needs secure technology and success in managing human behavior.

Secure technology

As we mentioned above, most of the organizations achieve their business collaboration through various information technologies, such as Internet, cloud, mobility, etc. Secure technology is therefore an essential condition for the secure and successful collaboration.

Success in managing human behavior

Managing the human factor in information security is essential, there is no different when we deal with collaborations. For instance, how do we build trust with your collaboration partners? When an employee working independently without peer control, how will he regulate his behavior? Human behavior can be changed due to various reasons, such as personal gain, society, physical surroundings, etc., and any bad human factors could lead to the failure of collaboration, or financial losses.

4.1.2 Collaboration associated risks and the business impact

The Risk IT [28] defined the business impact as *"An IT person should understand how IT-related failures or events can impact enterprise objectives and cause direct or indirect loss to the enterprise. A business person should understand how IT-related failure or events can affect key services and processes."* As such, risks have a great impact on their associated business. Hence, in order to make sure the collaboration is successful and secure, it is important to have a clear understanding of its associated risks and find out their corresponding business impact.

- **Risk 1** Trust problems. It is the major collaboration risk that acknowledged by many peoples (see appendix A B). Lack of trust is harmful to organizations, businesses, and collaborations. Low trust or distrust can lead to financial losses, business failure, and unhappy customers. When we specialize in collaboration, trust is an issue that need to keep balance between business and loyalty. Here, we defined loyalty as secure behavior for the company. The motivation of an employee to be loyal includes two aspects: loyalty to the company and to be responsible for projects. As such, the employee needs to think about business benefits of the company and well-being at the same time. However, there exists a conflict between business and loyalty. For instance, if managers give employees little time and much pressure to finish the projects, many employees would ignore secure policy, strategy and behavior in order to finish the projects quickly. As a result, it could bring information security threats to the company because employees are used to focus on business tasks instead of focusing on secure behavior, etc. Therefore, the more pressure from managers, the less loyalty (secure behavior) the employees will have.

  Business impact : Security is the cornerstone for the business and collaborations, e.g.

IT company. Due to distrust, it can very easy lead to the failure of business, and organizations might be in the situation of losing control.

Countermeasures :

- Information security training, and awareness campaign.
- Organizations should build their own security policy or strategy.
- In some specific information security business, employees need to get security clearance.
- Establish a secure collaboration system.

- **Risk 2** Leakage of information. People usually get or publish some information via websites, blogs, or social networks. From the perspective of information security, the activities of people sharing information with others and publishing information on the websites should be questioned, especially when it includes sensitive information. The situation can also happen due to having insufficient protection measures so that some unintended persons join the collaboration meeting. This can lead to that the person steals information and sells it to the competitors. Information belongs to the enterprise entity, as it is the asset of the organization. If the information is impacted in a negative way, usually referred to as a breach, it may lead to financial losses, and also the reputation may be depreciated due to loss of customers[72].

  Business impact: We have discussed this question with Siv H. Houmb in the interview A, we all agree that due to information leakage it can lead to that IPs are compromised, loss of customers, and competitors can gain advantage by using the compromised IPs.

  Countermeasures : Information leakage can lead to the loss of confidentiality of the enterprise. So in order to avoid disclosure of information to an imposter, users and employees should follow a privacy policy. The content of the policy may include:

  - Informing employees of permitted use of information when transacting business on social networks.
  - Training employees about what should and what should not be shared when utilizing social networks.
  - Providing employees with useful information on how to avoid threats of social networks.

- **Risk 3** Cloud security. More than 80 percent of business and IT managers worldwide are transferring, or plan to transfer, sensitive or confidential data into the cloud without understanding all the security implications [82, 83]. As such, a central component of managing risks in cloud computing is to understand the nature of cloud security threats. There are numbers of security concerns or threats associated with cloud computing, but these cloud security threats fall into two dimensions [84]:

1. Security issues faced by cloud providers, e.g. cloud data may be mishandled by the cloud provider because of technology gaps.
2. Security issues faced by their customers, e.g. cloud resident data may be stolen by a hacker because of the shared resource nature of cloud computing.

"The Notorious Nine: Cloud Computing Top Threats in 2013" report also reflects the most significant threats to cloud security[85]:

- Data breaches
- Data loss
- Account Hijacking
- Insecure API (Application programming interface: specifies how some software components should interact with each other)
- Denial of Service
- Malicious Insiders
- Abuse of Cloud Services
- Insufficient Due Diligence
- Shared Technology Issues

The above cloud security threats are specifically related to the shared, on-demand nature of cloud computing.

Business impact : Due to the organizations store amount of critical data into the cloud, any information security threats could bring hazards to the organizations, such as: loss good business reputation, loss of customer, financial loss, etc.

Countermeasures : When we use cloud services it is important to make sure the organization understands the security implicates of cloud computing. Understanding who have accessed to their equipment and networks. Based on their service level they can use different security controls (e.g. the following controls) to mitigate the cloud security threats:

- Data encryption.
- Keep offline back-ups of data.
- Intrusion detection.
- User access policy.
- Use incident response system.

- **Risk 4** Mobility security. Due to collaborations spanning across different locations, some employers and employees might use mobile devices to connect with their partners. As such, their personal smart phones and tablets need to connect to networks and have company information on them.

Business impact : The loss of a mobile device could compromise of information security, e.g. disclosure of cooperation information. As a result, the companies might lose their partners and have financial losses.

Countermeasures : All the mobile devices require a good password for access. If the business find it necessary, they can ensure that mobile devices contain GPS for tracking so that they can locate it if the device is lost or stolen. Implement encryption of e-mail and company data.

4.1.3 A secure collaboration system

When introducing extensive collaborations, we need to connect and share information with business partners. Therefore, it is important that a secure collaboration system should have different security levels based on the confidentiality levels of information. We divide information into three confidentiality levels:

1. "Crown jewel"
2. Confidential
3. Internal use only

Based on the different confidentiality level of information, the collaboration system will have different prioritization of security, shown as following (in each collaboration system, "..." means some other goals need to be achieved):

- "Crown jewel"
    1. **Security**
    2. Business progress
    3. Personal reputation
       ...
- Confidential
    1. Business progress
    2. **Security**
    3. Personal reputation
       ...
- Internal use only
    1. Business progress
    2. Personal reputation
    3. ...

4. ...
5. **Security**

When we deal with collaborations, keeping balance between loyalty and business is the most important problem that need to be considered. We defined loyalty as security behavior or security awareness during business process. Same as the 'Trust problems' we talked about before, there exists a conflict between loyalty and business, and the conflict is due to the pressure from the manager of the company. The more pressure from the manager, the less time the employee has to finish the projects. At the same time, the employee will ignore more security awareness in order to finish the business project on time. As such, choosing the security level of collaboration system would help employees keep balance between business and loyalty.

When we deal with "crown jewels", security is the most critical problem that needs to remain vigilant all times, no matter if it is humans, tools or environment. When we deal with "confidential" information, employees should comply with the security policies, information security standards and laws. For the information that covers "internal use only", the security can be ignored during business processing time.

4.2 "Crown jewel"

The "crown jewel" is the most important information asset of the organization, e.g. intellectual property, customer ID information, financial records and confidential data. Any harm and loss of "crown jewels" will lead to compromise of information security, and huge financial losses. As such, it is essential that organizations protect their "crown jewels" very well, but it is difficult for the organizations to decide who that deals with "crown jewels".

Generally, we need to protect "crown jewels" from two aspects: web-based attacks and insider threats. Protecting "crown jewels" from web-based attacking cannot fully depend on firewalls, IPsec, Web app shields[86]. The best strategy against these attacks is to harden their target, e.g. properly configured databases will stand strong against most attacks[86]. However, protecting "crown jewels" from insider threats is difficult, as it is not easy to find defense solutions. It is a significant problem related to human factors. Therefore, in this section we will focus on discussing how to protect "crown jewels" from insider threats.

4.2.1 Insider threat

In most cases we largely believe that *"people are our greatest asset"*. However, the employee-related crimes are constantly emerging. According to a recent survey, 58 percent of data breaches are caused by insiders, and 71 percent of insider threats use appropriate access[87]. As such, we can conclude that *"people are also our greatest liability"*. There is so much difference between the term of "insider" and "insider threat". The definition of "insider" has one or more of the following attributes[88]:

- Access to the system.

- Ability to represent the organizations to outsiders.
- Knowledge. Such as, the person who design the system.
- Trust by the organization, empowering an individual.

Therefore, we can conclude that "insider threat" depends on what the "insider" is. The GovInfoSecurity gives the definition of insider threat:

> *"Insider threat is the risk that current, former or contract employees might abuse system access to compromise data, operations or security."(alternative definitions can be found, e.g.in [88], [89])*

The term "misuse" demonstrate several problems. Misuse, which means human performance or behavior against the organization's rules or policies. The motivation of misuse also need to be questioned. For example, an insider may steal information for their personal gain, or a "spy" will steal critical information from the company for the benefit of another company. The FBI [90] presents variety of factors that may increase the likelihood of insider threat.

- **Personal factors** Persons change quickly due to environment, society, and their own situations. Such changes may raise the motivations for insiders to commit crimes or breach information security in their organizations. The reasons for the insiders to do so includes:
  - Emergency financial need or greed. Persons who believe that money means everything in their life. It can also be people who are addicted to gambling and need to pay for the debt within a limited time.
  - Problems at work. E.g.: conflict with co-workers, dissatisfaction with their work, lack of recognition from top management.
  - "Divided loyalty, insiders allegiance to another person or company[90]."
  - Family problems: divorce, loss of family members.
  - Vulnerability to blackmail: extra-marital affairs, fraud[90].
  - Compulsive and destructive behavior: drug or alcohol abuse[90].
  - Other personal reasons: revenge, adventure, ingratiation, etc.
- **Organizational factors** In many organizations, some organizational situations could lead to insider threat. Examples are given in the following content:
  - Improper classification of information or no classification of information, which lead to access privileges for those who do not need it.
  - "Undefined policies regarding working from home on projects of a sensitive or proprietary nature[90]."
  - Time pressure. The employees are focusing on finishing their project on time, and do not consider any information security aspects in their work.
  - Reorganizations. It can lead to that the organization loses control, and in that situation it could increase the amount of insider threats.

  - Employees lack of information security training.
  - "The perception that security is lax and the consequences for theft are minimal or non-existent[90]."

- **Behavior indicators** Some behavior may indicate that an employee is stealing information from the organization[90], the behaviors include:
  - People bring business materials home via PC, disks, or e-mail without permission. Alternatively, they are trying to gain some other classified information and documents which is not related to his work duties.
  - People cancel their holiday, and keep working during weekends as well.
  - Unnecessarily copy confidential information.
  - Remotely accessing the business process or system during vacation or sick leave.
  - "Disregard company computer policies on installing personal software or hardware, accessing restricted websites, conducting unauthorized searches, or downloading confidential information[90]."
  - "Engages in suspicious personal contacts, such as with competitors, business partners or other unauthorized individuals[90]."

We believe that there are many other factors that could influence human behavior and lead to insider threats. As such, it is essential to remind employees to be aware of security concerns, in order to protect the organizations' classified information. Dealing with insider threats is a big project which needs to be successful in the discipline of human factor. Hence, it is vital to know humans, and be careful during before, during and after recruitment time.

4.2.2 People are different

David Lacey[10] quotes Bob Courtney, the former Director of Security at IBM:

> "There are three categories of insider who commit crime. Single woman under 35, ladies over 50 who want to give money to charity, and older men who feel their careers have left them neglected."

Is this absolutely right? We think it should be questioned because people are different, and it is very difficult to conjecture what people will do next. To assume that all of the company staff will be loyal, ambitious and upwardly mobile is very normal for the managers[10]. However, this is not the fact in the real life. David Lacey also said that: people look and act the same on the outside, but it can be very different on the inside. Therefore, it gives espionage and frauds a higher chance to access the company to commit crimes. Ideally, the company should be able to identify the potential spies and frauds before they cause any business damage, unfortunately, many facts have proved that it is very difficult to detect criminal activities by insiders[10]. In such situations, it is also hard to let the top management decide which people can deal with the protected secrets of the organization. Therefore, we need to find the proper methods or solutions to protect the organization's documents, especially the classified information.

4.2.3 "Crown jewel" protection

One of the greatest threat and vulnerability of a company is the human factor [11, p. 42]. On a daily basis, many companies are being attacked by internal attackers looking to steal data for personal financial gain. A company must be prepared to respond to the inevitable incident, restore normal operations, and ensure that the company's assets and reputation are protected [91], especially, the "crown jewel" - critical asset. In this section, we will discuss how to protect "crown jewels".

Background

It is important to increase the ability to protect the organization's "crown jewels". There are different solutions for protecting "crown jewels" in the organization, which includes improvement of hire and pre-employment policies, cyber security risk management, "crown jewel" analysis, etc.

- **Protecting "crown jewels" through new hire and pre-employment policies and practices.** This method provides some steps that the companies take before or when they hire employees. It will increase the ability to protect company's trade secrets and other property while reducing your risk of liability[92]. These steps conclude observe the physical worksite, implement security measures and policies, educate employees, sign the Confidentiality Agreement and so on. The detailed steps of "Protecting Your Company's Assets Now and In The Future"[92]is shown as following:

    1. Require that new hires and consultants execute a confidentiality and inventions agreement.
    2. Reiterate confidentiality obligations in the employee handbook.
    3. Consider (carefully) using surveillance tools.
    4. Implement reasonable physical security measures.
    5. Educate your workplace on what is confidential.
    6. Create a document treatment policy.
    7. Describe appropriate and inappropriate use of company systems.
    8. Establish procedures now for future terminations.
    9. Evaluate the effectiveness of your policies and procedures.

- **Confidentiality Agreement.** Law is a useful tool to protect an employer's right when he engaged in the collaborations, no matter collaborate with business partners or employees. Contract is a legitimate mean for behavioral constraints. As such, you could restrain the employee's ability to use the company's confidential information to do so, and at the same time, you may protect yourself from claims that your company wrongfully is using someone else's information[93]. As such, 12 steps of "How to Protect Your Proprietary Information and Reduce Potential Liability Through a Confidentiality Agreement" [93] are needed, which is shown as following:

    1. Define your particular confidential and trade secret information.

2. Prohibit dissemination of confidential or trade secret information both during and after the employment relationship.
3. Prohibit competition during employment.
4. Prohibit the solicitation of employees after termination.
5. Exercise caution in other restraints of trade.
6. Confirm that the employee has no conflicting contractual obligation.
7. Confirm that the employee is prohibited from using confidential or trade secret information from a prior employer.
8. Define your company's policy on inventions.
9. Reserve the right to share this agreement with future employers.
10. Make sure you include an integration clause.
11. Require the return of confidential information at termination.
12. Reaffirm your at-will policy.

- **"Crown Jewels" Analysis (CJA).** It is a process for identifying the cyber assets that are most critical to the accomplishment of an organization's mission[4]. In many organizations CJA is often the first step in a Mission Assurance Engineering (MAE) process (see Figure 8),which includes the following analysis approaches:

  1. Understand what information need to be protected and identify the most critical assets of the company - the "crown jewel".
  2. Through "Cyber Threat Susceptibility Assessment" process to identify the threats and risks to "crown jewels".
  3. Through "Cyber Risk Remediation Analysis" process to select countermeasures to mitigating the risks.

The above three methodologies of the "crown jewels" protection focus on different aspects. The first method suggests us to use different polices and strategies during people's employment time. The second method demonstrates that "confidentiality agreement" is a useful way for protecting secret information in the organization. While the last method focus on how to protect "crown jewels" from an overall perspective of an industry. Each methodology has provide a good solution of protecting "crown jewels", but they all lack of human related problems or issues that need to be considered. Especially the third method, it did not consider any human factors. As such, we will develop a more completed solution with human factor consideration for handling "crown jewels".

How to protect "Crown Jewels"?

There is no easy route to establish trust among people and secure environments. Human factor is always remains the soft underbelly of the organizations' business operations. When we let somebody deal with "crown jewels", there are a lot of human-related problems need to be considered, e.g. who we should choose, who can we trust, how to detect insider threat, how to respond to

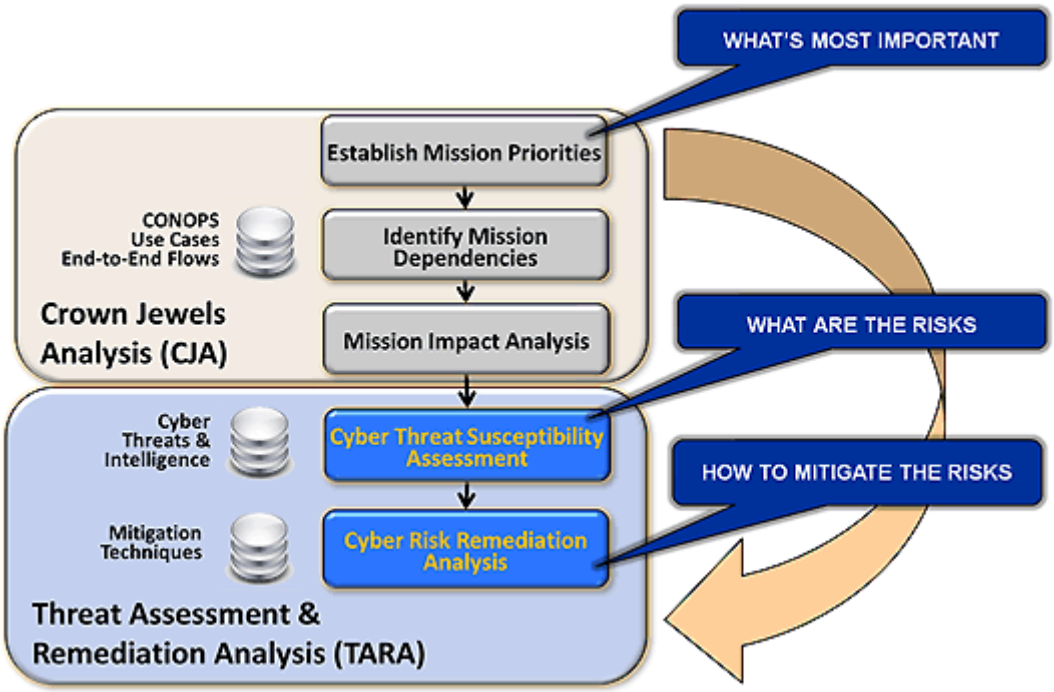


Figure 8: The Mission Assurance Engineering (MAE) Process[4]. (taken from [4])

insider threats, etc. Therefore, human factor is the most significant parameter for dealing with and protecting "crown jewels". Based on the previous three methodologies study, we provide a ten-step program for demonstrating our thoughts of protecting "crown jewels". It includes three main aspects: understanding what is the "crown jewel" for an organization, identifying who can deal with "crown jewels", mitigations of threats to "crown jewels".

1. Classify assets of the company, which could be divided in to different types: fixed asset, current asset, tangible asset and intangible asset.

2. Understand which company assets you are trying to protect and why: identify the "crown jewel".

3. Require Security clearance. The Norwegian National Security Authority defined security clearance as *"a vote of confidence, indicating that it has been cleared, is considered sufficiently reliable, loyal and with enough sanity to handle classified information in a good way. The classified means information not be made public, and that can be a danger to the security of society if it spread."*[94]. In some organizations, people need security clearance in order to access the classified critical corporate information. Based on the different classified critical information, it needs the different level of security clearance. For example, the Norwegian National Security Authority defined three different trust levels compare with North Atlantic Treaty Organization definitions: Cosmic top secret (STRENGT HEMMELIG), secret (HEMMELIG), confidential (KONFIDENSIELT)[94].

4. Employment requirement that the employee needs to sign a confidentiality agreement.

5. Get to know the person as much as possible. There is an essential condition of choosing the person who can deal with the corporate “crown jewels” is a long-term relationship B, which means you fully know and trust this person. It includes: know person’s personality, make sure they are loyal to the company, check their references, and it is require that they are part of the internal staff A.

6. Understand your enemies C. Understanding your enemies should be an integral part of any professional security risk management[10]. It is essential to take motivations in to account and forecast the capabilities of potential enemies. In order to better confront a range of external and internal security threats, we need to form a good understanding of what kind of people they might be, why they do it, what they are after, how they go about it, and how we might best deter them[10].

7. Separation. Separation of information or knowledge about “crown jewels” and distribute partial information to many persons. For instance, in your organization you separate the whole information about the “crown jewel” into ten parts and you give these ten parts to different persons to work with. You are the only one to know the connection to each groups. In this way, the “crown jewel” is not that much exposed. You will never have the whole “crown jewel” at risk, even though two or three people talk together, they will still not be able to combine the whole picture out of it.

8. Identify warning signs in people’s character, attitude, and behavior, which are closely correlated with espionage or fraud[10].

9. Build systems and office environments that deter theft and fraud[10]. Such as, implementing an employee monitoring program.

10. Security skills assessment and appropriate training[95]. This step is to make sure that the organization understand the security skills within its workforce. Improve the security level of the organization could via awareness training, secure behavior training, and policies.

5 Evaluation of security spending in the human and organizational process

Generic risk management process contains three phases: identification, evaluation and response of risks. Human and organizational risk management process is no different. When we evaluate security spending in the human and organizational risk management process, it largely depends on which countermeasure the manager will decide to implement. There is a golden rule that the decision maker needs to follow: *"NOT spend more money on the decision than the actual VALUE of the decision."* As such, the decision maker has some dilemmas[96]:

- Meet the correct level of security. We need to maintain the balance between the cost and security.
- Need quantitative assessments of cost and losses.
- Need an easy and resource effective way of evaluating alternative security strategies.

Evaluate security spending in the human and organizational risk management process has so many differences to the information technical risk management process. However, they all have the same situation that it is hard to make a security investment decision. In this chapter, we will provide the reason that why it is hard to make security investment decisions, introduction of security trade-off analysis, and evaluation of security spending in human and organizational risk management process.

5.1 Making security investment decisions is hard

Information security attracts a great deal of attention today, and at the same time information security expenditures are increasingly coming under greater and greater scrutiny [97]. However, risk assessment approaches focus only on security risks and not on the economics involved with security decisions[96]. Information security officers are struggling between managing risks and their budget's needs. Here is an example which shows the different countries how to respond to the bank frauds and their economic costs:

> "In the USA, if a customer disputed a transaction, the onus was on the bank to prove that the customer was mistaken or lying; this gave US banks a motive to protect their systems properly. But in Britain, Norway and the Netherlands, the burden of proof lay on the customer: the bank was right unless the customer could prove it wrong. Since this was almost impossible, the banks in these countries became careless. Eventually, epidemics of fraud demolished their complacency. US banks, meanwhile, suffered much less fraud; although they actually spent less money on security than their European counterparts, they spent it more effectively."[98]

No matter what kind of countermeasures they chose to invest for responding to bank fraud, it is still difficult for managers to make such a difficult decision. The information security economics

lecture [96] which taught by Siv H. Houmb conclude the following reasons of why making security investment decision is hard.

- Any security decisions require a holistic view on security, but it is hard for the decision maker to get overview of dependencies among systems, controls and decisions.
- In order to make a security decision, we need to evaluate the investment alternatives, but it is almost impossible to get the same comparable amount of information for each alternative.
- When we make security decisions, we should consider the associated risks. However, it is hard to estimate uncertainties about future potential events.
- It is hard to estimate costs and benefits of alternatives and to balance these with risk when we consider trade-off.
- Security decisions involve reflection on previous and others experiences, it is hard to obtain historical data related to security and to reuse it.

5.2 Security trade-off analysis

"There's no such thing as absolute security, and any gain in security always involves some sort of trade-off "[99]. Security costs money, time, capability, resources, etc. We do security trade-offs every day: we use security belt when we drive a car, we brush our teeth before we go to sleep, and we cook food by following the receipt. All security is trade-off [99].

"A tradeoff is a situation that involves losing one quality or aspect of something in return for gaining another quality or aspect"[100]. When we talk about security trade-off, it is the trade-off between security and performance. Security is not the only objectives, it may compete with other objectives such as availability, maintainability, time to market, etc. For example, accountability requires a strong audit trail and end-user authentication, which conflicts with privacy needs for user anonymity[101, 102]. When we design a security system, different views will have different system quality attributes as described by Siv H. Houmb[96]:

- End User's view. The end user needs to consider the products' performance, availability, usability, security, etc.
- Developer's view. In order to make sure all the products are qualified, the developer needs to take maintainability, portability, reusability, etc. into consideration
- Business Community view. From the overview aspect of the business community, it is important to consider the attributes that include time to market, cost and benefit, project life time, targeted market, etc.

When we doing security trade-off, we usually ask "Is it a good trade-off?" There are two types of security trade-off analysis, which were taught by Siv H. Houmb in the information security economics lecture[96].

- Technical: Evaluation against system quality attributes. E.g. Architecture Trade-off Analysis Method (ATAM)[1].
- Economic: In large complex systems, trade-offs have to do with economics, cost and benefits associated with architectural design decisions, E.g. Cost Benefit Analysis Method(CBAM)[2].

Any type of security trade-off analysis needs the risk assessment approach. The trade-off analysis depends on the result of risk management. As such, there are several specific aspects of the security trade-off that can go wrong [99]:

1. The magnitude of the risk.
2. The probability of the risk.
3. The cost if the risks happened.
4. The effectiveness of the countermeasure at mitigating risk.
5. The method of comparing risks and costs.

If we cannot accurately assess the risks, we will not have the correctly security trade-off analysis, then there is no chance to keep balance between the benefits and costs. Consequently, we cannot arrive the correct or proper security level, and it will create new potential hazards.

5.3 Evaluation methodology

The generic method to evaluate security spending in the human and organizational process is to measure how much is the investment is and what the according result is. However, in the human and organizational process, the most important discipline is to manage human factor. Due to the human factors, e.g. the company's personnel changes quickly and personal situation, evaluating security spending in human and organizational risk management process is very difficult. This is because it is very hard to measure and observe humans.

5.3.1 Background

In order to develop a new evaluation method, we believe that the background study of the existing evolution methods is essential. In this subsection, the brief instruction of two existing evaluation methods are provided.

Financial models

In her information security economics lecture, Siv H. Houmb have introduced four financial models, which are used to calculate, forecast or estimate financial numbers. Following is a brief introduction of each financial model.

[1] ATAM: To assess the consequences of architectural decisions in light of quality attribute.
[2] CBAM: it is different from ATAM in that it adds costs as quality attributes.

- **ROA - REAL OPTIONS ANALYSIS**
  It calculates values at a specific point in time or over a period. ROA has two options: financial option and non-financial option. Financial option refers to a financial asset and the owner of the asset has the right to exercise an option. Non-financial option refers to more tangible and not financial assets. It need to be adapted set of options and compound options and it is for non-capital investments.

- **ROSI - RETURN ON SECURITY INVESTMENT**
  ROSI = ("what-I-gained" – "what-I-invested") / "what-I-invested"
  Worthy investment when ROSI > 0

- **ALE - ANNUAL LOSS EXPECTANCY**
  ALE = "impact of future events in one year" * "likelihood of these events"
  ALE calculates the untreated losses and compare those to the security investment needed to mitigate losses.
  Worthy investment reduces risk: ("ALE without-investment" – "ALE with-investment") > 0

- **NPV - NET PRESENT VALUE**
  Its calculation based on "discounted cash flow" (uses estimations of cost, cost savings and revenues). And it based on principle of discounting: projected cash flows of the investment at a point in time in the future back to present time.
  Worthy investment when NPV > 0

Where do the numbers come from when we use the above four financial models? In order to get the numbers we need to do risk assessment before we use financial model. Risk assessments often result in qualitative subjective information, such as: likelihood, severity, consequence, and risk level [3]. We need to transfer these qualitative judgments to quantitative estimates, and the types of estimates needed depend on the requirements of the financial model. Then use the related data and financial model to assess if the security is over or under spending.

These four financial models are suited for evaluating security spending within technical problems, however, for human and organizational processes we do not know if they are suitable or not.

Valuesec project

The Valuesec Project [4], is a measure for cost-benefit analysis of current and future security in Europe, which aims *"providing public authorities with a decision support tool-set to analyze different aspects decision process and make decisions based on sound economic analysis"*. The Valuesec project indicates that effective and efficient cost-benefit-analysis must integrate features that are unique to the following security domains [103]:

- Cost structure analysis of consequences of security incidents.

[3] The risk level usually show on a scale: low, medium, high.
[4] The Vauesec Project website: `http://www.valuesec.eu/`.

- Direct cost and returns of security related measures.
- Multi-criteria decision making.
- Effectiveness and cost-efficiency analysis of security improvement measures and options.
- Social costs of the impact of and public reaction to, security measures.
- Legal and ethical costs of implementing or not implementing particular security measures.
- Political value assessments related to security governance.

Based on the above research information, we can via Valuesec's methods to analyze cost, benefits and drawbacks of security measures; to evaluate the results from the different perspectives of decision makers in security, etc.[103]. It will lead to more appropriate and effective decisions.

5.3.2 Triangle evaluation methodology

The new methodology we developed for evaluating security spending in human and organizational process named as "Triangle evaluation methodology". The mechanism of triangle evaluation methodology is shown in Figure 9. This methodology aims to help managers make the most proper security decision for investing human and organizational process. As shown in the figure, we need to keep two triangle relationships: "Risk, Measures, Policies" and "Options, Cost, Coverage". The definition of each term in the figure is shown as following:

- Risk - human and organizational risks.
- Measures - human and organizational risks responses.
- Security policy - how a company plans to protect the company's physical and information technology (IT) assets (an explanation of how security measurements will be carried out and enforced) [69].
- Target - it includes three types of assets in the companies: "crown jewels", confidential, internal use only.
- Options - solutions for the specific target.
- Cost - spending of the solution or security investment.
- Coverage - how much risks can be mitigated by using this option.
- Compliance - any action needs to meet the laws, standards and rules or terms of contracts for maintaining confidentiality, integrity and availability.

In order to mitigate human and organizational risks, we need to find out the corresponding measures to risk response based on the security policy that covers how to protect the company's assets. Due to that different assets need to meet different security levels, we divided the assets into three types: "crown jewels", confidential, internal use only. Once the type of asset is determined, the organization can provide various options for protecting it. Different options have

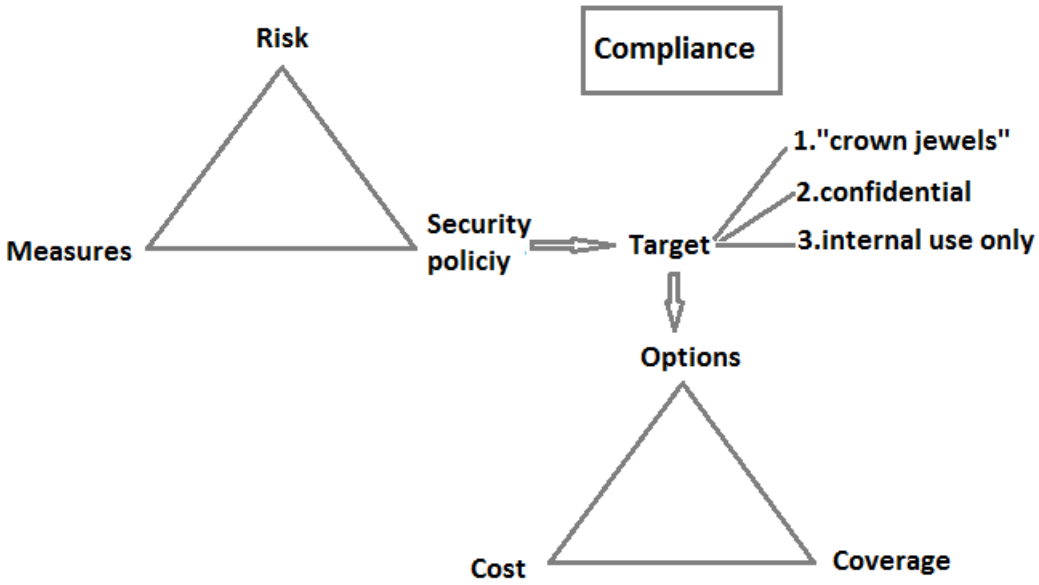


Figure 9: Triangle evaluation methodology - make the most proper security decision for investing in the human and organizational processes.

different costs, and the coverage of how many risks that can be mitigated or how much assets that can be protected is different. Based on this, the organization can choose the option that cover as much as possible, while paying as little as possible. To evaluate whether it is over or under security spending, we can compare the value of the asset and the cost of the protecting option.

5.3.3 Other evaluation methodology

Bench marking

Based on how much your enemies spend on attacking your system, you will spend the same or more for protecting it C.

Comparison

To assess and measure security spending we can compare the results before security spending and after security spending. We can measure it by using a triangulation, which means that you combine several methods to measure the same thing. As such, we could combine several outputs to better see the result B.

6 Completing with upcoming risks existing 2013 risk catalogue

Our society has already been totally changed by networks, which gives a new name of our society: the network society. The network society makes our lives become more advanced, quick, convenient, while it also introduces various risks that could compromise information security, lead to financial losses and negative technical impacts, etc. The newest ISO standards was published in 2013 together with the risk catalogue, which is included in the standard. Due to a long cycle of commending and quality assurance, we assume that this risk catalogue was made in 2011. Our society changes quickly and new society leads to new security as well as new risks. How will it change tomorrow? What will happen in the future? We need to explore the future, to find out what the future will be like. Therefore, there is a demand that need us to investigate the upcoming risks. As such, in the chapter we will try to define new risks based on the futurist study [1], give their mitigation methods, and an analysis their business impacts as well.

6.1 The effect of network society

The network society, a society made of individuals, businesses and state operating from the local, national and into the international arena[104]. The nature of the network society is that everything has been connected because of the network. Due to it, everything around us is totally changed: work style, lifestyle, business tools, human activities, the value of human beings, etc. For example, in the corporate environment the network society brings convenient and benefits to the enterprise, e.g. increased marketing opportunities, appeal more customers. In our life, instead of shopping in the supermarket or shopping mall, we can choose to buy many things from the Internet. However, the network society is still full of uncertainty, as when we deal with social networks it can introduce many risks to the organizations or individuals. The risk assessment report of social media[72] gives a list or risks for assessing social networks. Mark A. Gregory and David Glance[105] also presented a collection of security risks in the network society, which covers hacking, cyber security, internet, smart phones, and applications. Despite all this, networks are still the central element of our life and the network society will not stop, but keep developing. In Section 2.1, we have talked about the future network society. In the future network society, more and more digital and community devices will be used among the whole society and individual lives. As such, more and more technologies need to be introduced, and more security implications need to be considered as well.

[1] The statement of futurist: `http://www.wfs.org/futurist`.

6.2 Risk catalogue of the network society

The new risks that we identified are divided into four categories: human, organizational, legal, and technology risks. Most of these risks are based on the futurist study.

6.2.1 Human risk

No peer control

In the following years, personnel changes in the company will become more frequent. People constantly come and go, which leads to difficulties in building teamwork. Due to the disappearing of job[6], instead of having one task needed to be finished by many employees, we will have the situation that many business tasks to be done by one person. As such, most of the work needs to be finished by the employees themselves and there is no peer control any more.

Living in permanent transition

With the development of the society, the flow of time, the surroundings are in constant change. The world is changing, technology is changing, environment is changing, and people are changing. The same situation can also happen in your organization: you get new bosses and colleagues. In such a way, it is difficult to ask employees to be loyalty. In addition, the futurists predicted that more than two billion jobs will disappear by 2030 due to technologies disrupt economies[6]. In the future, all the organizations will highly rely on the knowledgeable persons who can implement and control technology. But due to the conflict between less loyalty and strong dependence of knowledgeable persons, it could bring serious damage to the organization.

6.2.2 Organizational risk

The new habit is nomadic society

Many traditional control elements of working have passed away. Today, there is no more need for people work at the specific workplace. People can work anywhere anytime, no matter if it is in the airport or a restaurant. Some of the job positions accept that people work at home. In such a situation, organizations' demand of loyalty is much higher.

Inadequate protection of data within an organization

As we mentioned in the previous risk – "living in permanent transition" that there is the trend of decreasing amounts of jobs in the future. At that time, in many organizations will have the situation where one person has a lot of tasks about handing the security or business. One person will control all the data, and if this person fails, the organization will face serious hazards as well. For instance, a company has its "crown jewel" and only has one person to deal with it. Because it is a single responsible person, this person has all the information about the company's most important information and this situation could more easily expose them to a third party. Once it has been exposed, the organization might have to face huge losses.

Fast changing of technologies

With fast development of technology, lots of companies need to adapt to these technologies. But many companies do not have sufficient preparation for new technologies, and they are therefore not ready to that advance. Hence, most of the companies start using new technology without having a clear understanding of the technology's security implications.

Big exposure of public data

There are amounts of information on the website such as LinkedIn, Facebook, etc. These websites are very good open resources for the enterprises. For instance, if you want to find the management person of one company, you cannot find any management position on the company's official website, but if you search the company name on LinkedIn you can find its CEO, CIO, CISO, etc., as well as their education and working history, and other personal information. Such a big exposure of their information could give an advantage to attackers which may lead to harmful damage to the company.

Use of company resources for private purposes

Many organizations are introduced to many new technologies for their business use. Due to the expensive prices for the advanced technology products, individuals may not afford them, and therefore the technology products might be only owned by the organization. The potential threat can be that employees make something that is not related the business by using these advanced technologies. For instance, an employee uses the organization's 3D-printer and material to make something for himself during work time. If this improper behavior was not stated in the organization's policy, this employee cannot be punished by his manager.

6.2.3 Legal risk

Human privacy is impacted by smarter software

The futurist says: *"At present, there is no computer program that can perfectly interpret human speech"*[106]. The futurists have however provided several methods that can let it come true. At that time, a smarter algorithm can scan your e-mails and get all you data, and it is not only the communication's metadata, but the literal content as well. Then we would like to ask *"what happens to privacy when an algorithm can understand us as well as humans"*[106]?It is intrusive and seriously impacts human privacy. If attackers get a hold of the data collected by algorithms, they can do whatever they want with these data, in this case, *"the danger clearly gets worse as the software gets smarter"*[106].

6.2.4 Technology risk

Threats from 3D-printing

The futurists present that worldwide demand for 3D printers and software will grow by 21 percent a year through 2017. The printing technology has improved in the last few years, and

the range of materials that printers can work with has expanded[107]. More metal products can be printed, e.g. in aerospace industries, which are using more and more 3D-printing systems to manufacture aircraft parts[107]. With such fast development of 3D-printing, people can print various kinds of things if they need. However, it will also raise to some threats:

- People can make whatever they want. People can make something which is illegal. People can make guns which are untraceable because they have lack serial number or they can more easily be destructed. If somebody is hurt by these guns, the police could therefore have difficulties to determine the culprit.
- Copyright infringement. If somebody wants to have something which is very expensive, they can get that thing via 3D-printing with lower spending. However, it breaks the copyright for producing that thing without authorization.

Organization in transition

The security concepts in your house include locking the door, having a fire alarm, closing windows, etc. When you move from one place to another, these security concerns will transfer from the house to the car. Changing a company to another location have similar behavior as when changing residence. Company in transition is not only the change of location, but also the change of network, IT, environment and people. A lot of companies are not aware of attacks during the transition time, and therefore the transition is much less protected. For example, if there is an access problem with a bank's service system, in order to make sure the availability of the bank system, all employees will have the access right at that time. It might not last so long and the likelihood of somebody knowing is very low, but it still give a very high possibility for attackers to access the bank system.

Bad robots

Unmanned systems are poised to revolutionize all aspects of daily life, such as vacuum cleaners, lawnmowers, and window washers[5]. However, the robots still have the dark side. The evil robots are not just a story in the film or novel, it is real life. Example of evil robots activities are shown in the following Figures 10 and 11.

These examples are not novels, numerous study groups have indicated that this threat is growing due to terrorist usage. As the usage of robots or unmanned vehicles grows, their misuse is more viable. Hence, it can have new dangers in the future. For example: flying parcel-delivery drones, driverless vehicles and trucks, and other mobile robotic systems can be stolen, hacked into, and hijacked to deliver explosives and other agents of destruction [5].

Loss of control in the digital world

The future of our world will be a digital world. At that time your screen make your digital world local, you enjoy digital boundaries for privacy, everything is there[108]. Everything will be digital services, no matter if it is business, food, entertainment or social life. From the futurist [108] we

- The Irish Republican Army was able to take control of a British Army EOD (explosive ordnance disposal) robot carrying explosives and turn it against its operators.
- Iranian Revolutionary Guards rehearsed attacks using bomb-laden remote-controlled boats.
- The Basque separatist group ETA tried to blow up a Spanish patrol boat with four-foot-long remote-controlled boats packed with explosives.
- Drug smugglers started using homebuilt unmanned submarines to hide contraband from the U.S. Coast Guard.
- The FBI found catalogs and operator manuals for EOD robots within an Aryan Nations leader's cabin.
- Branch Davidians experimented with an enhanced bomb-laden remote-controlled plane.
- Japanese cult Aum Shinrikyo examined using crop-dusting radio-controlled helicopters for sarin payloads.

Figure 10: Examples of evil robots activities since the 1970s. (taken from[5])

- In 2004, Canadians of Arab descent were charged with working on a GPS-navigated model airplane that could be fitted with explosives. They were being directed by a senior al-Qaeda figure in Pakistan who wanted the men to unleash a wave of simultaneous bombings in the UK.
- In 2007, Iraqi terrorists drove bomb-laden remote-controlled cars toward American convoys in Al-Durah and Al-Taji.
- In 2008, Columbus, Ohio, resident Christopher Paul, an accused al-Qaeda member, pleaded guilty to planning attacks in the United States and Europe using remote-controlled boats and five-foot-long helicopters.

Figure 11: Examples of unmanned and hobby remote-controlled vehicles. (taken from[5])

know that in the future we will have a digital world centered around ourselves, which recognizes and follows us from screen to screen. For instance, instead of worrying your retired parents, you can put your family's life space on the nearest screen to check how your parents are adjusting to retirement[108]. In order to achieve the digital world, we need to input numerous of data, build many digital communication channels, but we also need to establish encryption to make sure it is secure. However, how do we respond when we lose control of this digital world? We would lose everything, we cannot have a normal life every day, our privacy world might be explored in the public, companies and factories cannot stay in business or produce products. We need to think about how we can protect our world from future potential threats.

6.3 Mitigation

The impact of these new risks are high, which could result in harmful damage to the organization. Therefore, it is very important that organizations identify new risks and respond to them by implementing their associated countermeasures. The following content provides some suggested countermeasures that might be useful for mitigating the magnitude and possibility of the new risks:

- **Driverless cars** will be on the verge of eliminating millions of driver positions. Buses, taxis, trucks, limos, UPS, FedEx, and more will be transitioning into driverless forms of themselves. At the same time, we'll see a dwindling of parking lots, gas stations, traffic cops, and traffic courts, and fewer doctors and nurses will be needed to treat injuries.
- **Education** will see a mass transition from teaching to coaching, as 90% of all traditional classes will take place online by 2030, even in K-12.
- **3-D printers** will disrupt everything from manufacturing, to health care, to retail, to art, to construction and building materials. Printed clothing and shoes produced at the store you're shopping in will replace garment districts around the world. Printed buildings and houses will eliminate the need for contractors and building materials. Pill printers will replace entire pharmacies.
- **Automated manufacturing** is already eliminating tons of jobs. Bots and drones will begin disrupting many other industries along with their base of employment.

Figure 12: Examples of learning new skills will keep people in business. (taken from[6])

- Learn new skills. As the advanced technologies replace many job titles, keep learning new skills can keep people in business. Example is given in the Figure 12.
- When we use advanced system or technology, association members should monitor potentially abusive applications[5].
- Establishing a list of "early warning" indicators to monitor and track the development and use of mobile[5].
- Separation of duty. Separating knowledge or information to many people will have much less harm to the organization.
- In order to use new technology securely, CISO needs to understand the nature of the technology's security implications and identify its associated risks.

6.4 Business impact

Summarizing the new risks we identified that every new risk can impact enterprise objectives and cause direct or indirect loss to the enterprise. These risks can affect the enterprise's key services and processes from both business capability aspects and secure business aspects. In order to have a more clear understanding of each new risks' business impact, we will provide more information in the following Table 2:

6.5 Reassign new risks

From the No.13 question we asked in the interviews (see appendix A B CD), we can have a common conclusion that when we do changes we need to reassign risks. As such, we defined reassign risk as reassess risk, evaluating the magnitude and possibility of the risk again. The world changes quickly, as well as the technology, environment, society, people, etc. New changes lead

Risk catolugue	New risks	Business impact
Human risk	No peer control	Human errors or irrational behavior leads to business fail.
	Living in permanent transition	Exposure critical information of the organization. Lose customers.
Organizational risk	The new habit is nomadic society	Exposure critical information of the organization.
	Inadequate protection of data within an organization	Exposure confidential data of the organization. Financial loss. Lose good reputation.
	Fast changing of technologies	Much less effectiveness and efficiency of the business.
	Big exposure of public data	Break business regularly compliance.
	Use of company resources for private purpose	Financial loss. Break the compliance of the organization.
Legal risk	Human privacy is impacted by smarter software	Customers are not satisfied.
Technology risk	Threats from 3D-printing	Financial lose. Break business regularly compliance.
	Organization in transition	The failure of business aspects to the use of IT.
	Bad robots	Due the business process is not secure, the company could lose their business.
	Loss of control in the digital world	Financial loss.

Table 2: Business impact of new risks.

to new security and risks, similar to the new risks we identified above. What kind of changes will lead us to reassign the new risks? It may include many parameters: environment, technology, society, time, etc. Example is given: recognized organizations, introduced new technologies, relocated the company, etc. There are two purposes for reassigning risks: measure the impact of the risk after implementing countermeasures, and to find out what is the potential impact of this risk in the future. Improperly reassessed and coordinated risks can result in a significant business impact or harmful hazard to information security. Therefore, it is important to reassign risks.

The model we developed for reassigning risks is based on the study of change management process[109], and it includes steps that ensure that changes are formally described, adequately reviewed for their impact on business, risks are reassessed, and that they are coordinated with ongoing business activities. The last three steps can be processed by following the normal risk management procedure. It is difficult to understand and measure changes, therefore, we will focus on the step of describing changes sufficiently. The change often affects risk itself in four

ways:

- The magnitude of the risk.
- The occurrence possibility of the risk.
- The time when the risk occurs.
- The reason that the risk occurs.
- The time line to reassign the risk.

In order to address these five issues that reassign risks properly, seven questioned must be answered about every change. The questions are based on the study of the change management process[109] and are as following:

- Who raised the change that affect risks?
- What is the reason for the change?
- Who is related to the change?
- What are the risks involved in this change?
- What resources are required to deliver the change?
- Who is responsible for the build, test, implement the change?
- What is relationship between this change and other changes?

How does these questions affect reassignment of risks? In the following content, we will answer these seven questions for every change. Organizations should reduce or reassign risks that associate with these changes.

For example, let us consider a change that organizations might face - organization transition. Using the above seven questions, we could get the following answers:

- **Who raised the change that affect risks?** Top manager (both business and IT managers).
- **What is the reason for the change?** Business need or the top management decides organization transition due to financial problems or other reasons.
- **Who is related to the change?** This question identifies the people who might affect the change. In this example, it is the employees of the organization, and the organization's competitors.
- **What are the risks involved in this change?** During the transition time, the whole organization (IT, network, physical environment etc.) is much less protected. The organization is not aware of attacks during the change.

- **What resources are required to deliver the change?** This identifies the specific tools and equipment used to deploy the change, as well as the target configuration items for the change[109].
- **Who is responsible for the build, test, implement the change?** This question identifies the people responsible for ensuring the change is correctly built, tested, and implemented as intended[109]. In this example, the people who responsible for the organization transition is the top manager.
- **What is relationship between this change and other changes?** This identifies any other changes occurring at or near the same period time of this change, and the interactions between this change and other changes[109]. Such as personnel come and go.

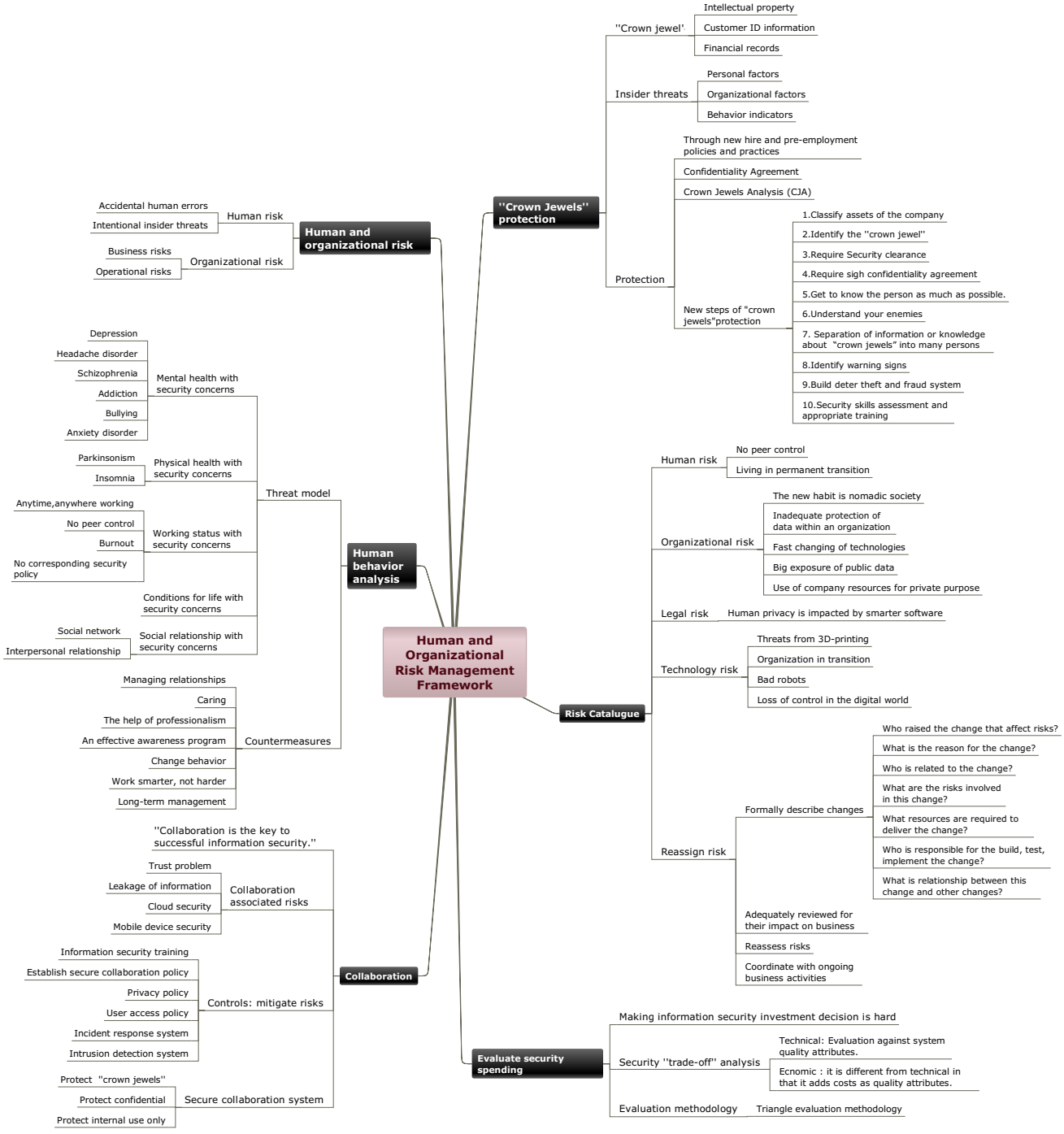
As shown in the example, any organization that needs to change can use these seven questions to generate enough information to sufficiently understand the critical aspects of the change. Once the organization understand the change, they can process the reassessment of risks accurately.

7 New elements of the framework

In this chapter, we provide a mind map to show all the new elements that we updated for the human and organizational risk management framework. The mind map is shown in the next following page 64. The mind map it includes six new parameters for dealing with human and organizational risk management: Human and organizational risk, Human behavior analysis, Collaboration, “Crown jewels” protection, Risk catalogue, and Evaluate security spending.

More detailed information for each parameters are described in the previous chapters. Through these chapters, we have managed to answer the research questions(RQ) that we described in Section 1.5. We answered RQ1 in the Chapter 3. In terms of RQ2 and RQ3, the answer is provided in Chapter 4. Our answer to RQ4 is reflected throughout this thesis. We answered RQ5 in the Chapter 5. In terms of RQ6, the answer is given in Section 6.5. The information that we got by answering our research questions are combined and provided in the mind map on page 64.

Ontology of a Human and Organizational Risk Management Framework.



8 Recommendations

Recommendation 1: Address human risks - the crucial challenge today.
Based on the background study, we get to know that there is no framework or standard that can deal with risks within the specialization of human and organizational aspects. The existing frameworks and standards focus too much on technical problems. The situation is similar to when the organization faces risks which at the first point in their mind is not human risk but technology risk. As the saying that *"Computer do not commit crime, but human do"*, which means that the humans are the reason for many technical risks. When people use information systems, mistakes happen[11, p. 42]. Even a harmless human mistake can produce extensive damage. As such, one of the greatest threats to the organization are its employees. We recommend that organizations address human risks, especially insider threats.

Recommendation 2: Develop and apply a human and organizational risk management framework
The objective of this master thesis is to update the existing frameworks as they did not conclude any parameters for dealing with human and organizational risks management. We found out that there is no framework for specifically handling human and organizational risks. Most of the frameworks and standards, e.g. ISO 27001, ISO 27002, Risk IT, they all focus on technical problems in the information security field. Therefore, we feel that there is a strong need for developing a human and organizational risk management framework. We also suggest that in order to develop such a framework, it would be smart to cooperate with an organization that has experience in dealing with human and organizational risks, e.g. Gjøvik University College or NorSIS. Once the human and organizational risk management framework is developed, it is important to apply it for addressing human and organizational risks.

Recommendation 3: Identify and protect "crown jewels".
The "crown jewel" is the most critical information of the organization, any compromise of "crown jewels" will lead to the harmful damage. As such, the need for the organizations identify and protect their "crown jewels" is very high. In the first interview A, Siv H. Houmb mentioned that 90 percent of security breaches are caused by insiders. Therefore, we recommend that the protection methods should focus on protecting "crown jewels" from the insider threats.

Recommendation 4: Prepare for the new risks.
It is very important to prepare for the unexpected. We believe that take the potential new risks seriously is essential for the organizations. The new risks we identified in the Chapter 6 are all in the category of high level, and might lead to the unexpected damage to the organization. Therefore, we recommend the organizations to find out the risk responses based on their business needs and to implement the corresponding mitigations. Implementing the risks mitigations will

reduce the likelihood and decrease the impact of these risks. Highly recommended preparations for new risks are:

1. Information security training,
2. Awareness campaign
3. Implementing security policy

Recommendation 5: Implement on all managerial level human and organizational risk management framework.
It is imperative that organizations should understand the serious situation of human factor in the network society and the organization's cooperate environment, and how to manage the human and organizational risks. Thus, we suggest to implement on all managerial level human and organizational risk management framework. A communication plan is provided on how to communicate and implement the new parameters that we supplemented for dealing with human and organizational risks.

- Board meeting for presenting the importance of human related security problems. The top manager should have the high-level understanding of information security concerns related to human and organizational processes.
- The line manager that responsible for dealing with human issues should get support from the information security manager C. In addition, the line manager should keep communicating with both information security managers and HR department about the human related problems. We recommend that line managers should not have more than 10 employees to responsible C.
- All the managers in each department should have a workshop meeting with their own staffs for introducing the importance of security behaviors, and can though e-learning as well as awareness campaign improve the security level of the organization.
- The IT department should take human risks seriously, and develop an information security policy anchored the use of IT equipment, software and applications.
- Once the human and organizational risk assessment report is produced, the employees should produce an articulated interpretation of the human and organizational risk assessment report and business objectives that affect their daily work, and understand their accountability for risks.
- Prepare for human and organizational risks, no matter if it has already happened, can, or will happen.
- Employees report systematically to senior management about any new risks or failures of existing controls.
- Based on the human and organizational risk assessment report build a recovery process for the risks.

9 Discussion and Future Work

In order to know how people performs human and organizational risk management processes in the real life, we decided to carry out the expert interview methodology to get the information from four interviewers. In this chapter, we will first recap and discuss the interview result. Then we will give the direction of future work which is related to this master thesis.

9.1 Interview discussion

The first interview
This interview was held by Skype video conferencing. The interview answers were given by Siv H. Houmb, the associate professor II of Gjøvik University College. From the interview we got to known that most of the major critical cyber-attacks and security attacks are caused in some of way by insiders. In this situation, some organizations use ad-hoc to perform human and organizational risks, and some organizations do not identify these risks. It is important and essential to identify and manage human and organizational risks as the hazards from these risks can raise serious damage to the organizations. We believe that organizations should take human related security problems seriously and identify mitigations for pushing down the impact and likelihood of these risks.

The framework Siv H. Houmb mentioned for dealing with human and organizational risk management is only ISO 27001, which includes access to systems, security awareness, and training people. However, to manage human and organizational risks is a tough task, and the existing security controls are far away to be good enough to address human and organizational risk.

For the issue of dealing with “crown jewels” in the organization, she provided the following elements:

- Security clearance.
- Loyalty.
- Know the people’s personality.
- Check the people’s reference.
- People who can deal with “crown jewels” should be an internal person.

These can be the important elements that are contained in the “crown jewel” protection, but for the personal-related conditions, we need to keep a high awareness as it is very difficult to be able to recognize crooks by their appearance.

For the ideal situation for an organization considering human issues, she said it should be a separate professional group that works with human and organizational risk management, and has ability to monitor risks and decide how to address issues. We agreed that to have a separate group, but that it was needed to define what kind of capability that should be considered when they address human risks, and to define how they will perform human and organizational risk management processes. This separate group should be integrated into the information security management system.

The second interview
The interview was a Skype video conferencing with Thomas Schlienger, a consultant at TreeSolution AS. The method that he provided for dealing with human and organization risk management is to analyze and improve the information security culture, which can help the organizations to measure how big their human risks are, and how they can lower them. But, many organizations almost do not identify human and organizational risks. The only framework that can be used for performing human and organizational risks management is ISO 27001, but it is far from enough. We believe that analyzing and improving information security culture is a very good way to handle human and organizational risks. The culture impacts and restricts human behavior, and is therefore an important element for the organization. The better information security culture, the less human errors and insider threats, and will result in better business.

For the issue of dealing with "crown jewels" in the organization, Thomas believe that it is very important to know the people very well and have long-term relationship with the persons dealing with "crown jewels". These factors are certainly important, but we think that the solutions for detecting or avoiding insider threats also should be contained, and more restricted conditions are needed to allow someone to deal with "crown jewels" in the organization.

The third interview
It was a Skype video conferencing with Stewart Kowalski, the Professor of Gjøvik University College. The framework he provided for dealing with human and organization risk management is ISO 27001 and capability maturity model. Kowalski mentioned that in order to perform human and organizational risk assessment, the information security officer talks to the line manager to get more information due to the line manager is given the responsibility for dealing with human issues. We believe that it could be a very good solution for managing human and organizational risks, as line managers interact with employees much more often than information security officers, and line managers are not as centralized as HR department officers.

The conditions Kowalski provided to allow someone to deal with "crown jewels" are:

- Be able to suave the attackers.
- Know your enemies.
- Know the person's financial statement.

In order to suave the attackers, we believe that communication could be a good way. However, how to approach this process, and what human related problem should be considered are need to be defined.

To have an ideal situation for an organization addressing human issues, he said the line manager plays a significant role, and the line manager should get support from the information security manager. This could be a good recommendation for the organization managing human issues.

The fourth interview
The interview answers were provided by Hans Marius Tessem, the Senior Adviser of NorSIS, and this interview was conducted by using Skype video conferencing. The organization Tessem works with is NorSIS, which deals with human risks on a national basis but do not use any frameworks. Based on his experience, Tessem said most of the companies take human risks seriously, but they do not know how to handle it. There are no frameworks for performing human and organizational risk management, and a lot of companies do not have strategies for handling human and organizational risks, however, they might have a strategy stating that managing human and organizational risk is important for them. For these situations, we would like to suggest to develop a framework which is specific for human and organizational risk management. Addressing human and organizational risks by putting the finger in the air to feel the wind is not a scientific method, as a result you will not evaluate the risks accurately and cannot provide the proper countermeasures, which could raise to new risks.

To assess and measure security over and under spending in human and organizational process, he specifically said that instead of talking about measuring all the time, we need to talk about having open channels for getting information which can help us prevent something bad to happen. It is very important to have good communication, as this is the way to control or change something. We believe that it is a very good guideline to follow. People are very difficult to measure, instead of measuring them we need to consider more about how to protect our organizations by avoiding or preventing human and organizational risks to happen.

The ideal situation Tessem described for an organization considering human issues is a position between IT and HR position. They should have a triangle relations, where the people who works on this position should communicate with both IT and HR department, and tell them what they should do. It might be a good situation, but the responsibility for this person and how he handles the human and organizational risks should be defined. This position has the similar responsibility with the line manager that Kowalski talked about in the third interview.

During the interview, the four interviewers provided different human and organizational risks due to various human issues. The following Table 3 is a collection of human and organizational risks that the interviewers mentioned during the interviews.

Risk catalogue	*Risks*
Human risks	Insider threat
	People leave the company
	People intentionally bring confidential information out
	Lack of proper classification of documentation
	People does not encrypt their disks
	Leakage of information
	Trust problems
	Loss of mobile devices which store lots of business information
	Human error
	People making delivery mistake
	Improper back-up
	People have bad passwords
	People does not follow their responsibility
Organizational risks	Missing use of the policy
	Through organization's structure to get access into the system
	Lose control due to the company restructuring
	Fast personnel change in the organization
	The more and more complex of work
	Loss of business
	The loss of control over the finances
	Competitors

Table 3: Collections of human and organizational risks from interviews.

9.2 Future work

This thesis has shown that by updating the human and organizational risk management framework, we could have more solutions to address and handle human and organizational risks. Managing human issues is a complex task, but the good results can protect the organization from the extensive damage caused by human error or failure. As such, it motivates us to develop a good framework within human and organizational risk management aspects. Despite the new elements we updated for this framework, we believe there is a lot of work needed to help the organizations to better handle human issues. Due to this reason, we provide several possible directions for the future work which are related to this project.

Establish a professional information security training program.
Regarding the content we mentioned in Section 3.3.3, there is nowhere an enough professional information security training available. Considering how important the information security training it is in an organization, establishing a comprehensive information security training program is fully required. This training program should consider the different human situations, the information security culture of the organizations, and the organization's policies.

Development of human and organizational aspects in the information security system.
This work would increase the knowledge and skills of managing human and organizational risks. In that way, the managers who are responsible for the human related security problems could get enough resources for dealing with human and organizational risks.

Development of practical implementations or theoretical methods for measuring human behavior.
Insiders are the biggest threat to our organization, especially today as almost 90 percent of major critical cyber-attacks and security attacks are caused by insiders. However, it is very difficult to detect insider threats as human behavior changes quickly and human is very complex. Therefore, we believe that if we can have proper measurement of human behaviors, we could contribute so much to protect the organization's security, in particular protecting the organization from the hazards of insider threats.

More methodologies for reassigning risks should be defined.
The method that we used for reassigning risks that we only consider the measurement of the risk-related change. Other mechanisms and technical parameters for reassign risks would be worth looking into.

The evaluation for the new parameters of the human and organizational risk management frameworks should be performed.
The master thesis lack of evaluation of the new parameters that we updated for the human and organizational risk management frameworks, thus we think that the future work could include the evaluation of the new parameters' performance. This would improve the knowledge of the human and organizational processes' success and the value of these parameters.

Supplement and update other parameters for the human and organizational risk management framework.
In addition to the parameters that we updated in this thesis, other parameters could be supplemented, e.g., a more sufficient new risk catalogue, and defining the proportion of accepting human and organizational risks. The world changes quickly, and gives raise to the new societies, new security, and new risks, thus new parameters are fully needed for handling new human and organizational risks. Therefore, updating and supplementing parameters for the human and organizational risk management framework should be a continuous work in the future.

10 Conclusion

We contribute to existing management frameworks with updates and supplements in respect to human and organizational risk.

In our analysis of exiting frameworks and standards, a very limited coverage of human and organizational aspects was found, and the number of security controls were dramatically low or non-existent, except the ISO 27001. However, most literature references deny that the ISO 27001 is qualified to deal with human and organizational risks.

The development of the network society asks humans to input thoughts, intentions, intelligence and attributes. As such, humans become the greatest assets for the organization as well as the biggest potential for threats due to lazy, irrational or even intentional human actions. In order to provide the parameters that can help organizations with managing human and organizational risks, we decided to start with the analysis of human behavior.

Challenges related to human behavior are much more serious than we would like it to be. The analysis of human behavior that we carried out were based on the different human situations, which include: mental health, physical health, working status, conditions for life and social relationship. Through this analysis, we found that the human behavior is largely depending on specific situations human beings are confronted with. Different human situations can interrelate with each other resulting in a variety of combinations which may result in actions not really predictable. The analysis of human behavior is a quite complex, but we believe it is a well-justified research area for the future as even little advancement could make a real difference in protecting corporate information assets.

For the human and organizational risk management issues, we chose to discuss about collaboration and the “crown jewel”. Collaboration is the key to successful information security, but to make a secure collaboration system is a difficult task that all the organizations face. In order to make collaboration more secure and effective, we suggested three different security levels for collaboration systems. The organization can choose their collaboration system based on the confidentiality level of concerned information. Handling the “crown jewel” is an essential and important task that all the organizations need to deal with. As such, we recommend a ten-step program for protecting “crown jewels”.

When dealing with human and organizational risks there is one thing we need to think about: it is how to evaluate security spending in the human and organizational process. People are difficult to measure. Due to this reason, we transferred the measure target from humans to assets and provided the new triangle evaluation methodology for evaluating potential security over

and under-spending. We can compare the value of the asset and the cost of the protecting option. However, instead of thinking how to respond to these risks and evaluate the corresponding security spending, we believe it is more important to think about how to mitigate human and organizational risks. One solution we suggested is to secure human actions by information security training and the use of open communication channels.

At the end we identified 12 new risks categories based on futurist study in respect to newly upcoming human, organizational, legal, and technological risks. Our world is changing quickly, so our society, technology, environment, and people do as well, and many unforeseen things can happen in the future. However, through the scientific methodology applied in this study we are confident to have a reasonable good coverage and precision for the next few years.

Bibliography

[1] World Economic Forum. 2014. Global risks 2014 ninth edition. http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf [Accessed 15-February-2014].

[2] Press, W. August 2013. Infosec burnout survey results and bsideslv talk. http://p0lr.org/?p=69 [Accessed 14-April-2014].

[3] Gonzalez, J. 2005. Towards a cyber security reporting system – a quality improvement process. In *Computer Safety, Reliability, and Security*, Winther, R., Gran, B., & Dahll, G., eds, volume 3688 of *Lecture Notes in Computer Science*, 368–380. Springer Berlin Heidelberg. http://dx.doi.org/10.1007/11563228_28.

[4] Hastings, G., Montella, L., & Watters, J. May 2009. Mitre crown jewels analysis process. http://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/crown-jewels-analysis [Accessed 01-May-2014].

[5] Shaker, S. M. June 2014. World future society: Good robots gone bad. http://www.wfs.org/futurist/2014-issues-futurist/may-june-2014-vol-48-no-3/good-robots-gone-bad [Accessed 09-May-2014].

[6] Frey, T. October 2013. World future society: Disappearing future 4. jobs and workplace processes. http://www.wfs.org/futurist/2013-issues-futurist/september-october-2013-vol-47-no-5/top-10-disappearing-futures/disap-2 [Accessed 11-May-2014].

[7] Fossas Olalla, M. 1999. The resource-based theory and human resources. *International Advances in Economic Research*, 5(1), 84–92. http://dx.doi.org/10.1007/BF02295034.

[8] Bernhard Hämmerli, Margrete Raaum, G. F. June 2013. Trust networks among human beings: Anaysis, modeling, and recommendations. *Effective Surveillance for Homeland Security*, 22–49.

[9] Esmaeili, A. 2012. Strategic human-resource management in a dynamic environment. *Scientific and Technical Information Processing*, 39(2), 85–89. http://dx.doi.org/10.3103/S0147688212020037.

[10] Lacey, D. 2011. *Managing the Human Factor in Information Security: How to win over staff and influence business managers*. Wiley. com, ISBN: 978-0-470-72199-5.

[11] Whitman, M. E. & Mattord, H. J. 2009. *Principles of Information Security*. Course Technology, 3rd edition, ISBN: 1423901770.

[12] Leedy, P. & Ormrod, J. 2012. *Practical Research: Planning and Design*. Pearson Education, Limited, ISBN: 9780132899505.

[13] ERICSSON. March 2013. Networked society: A connected world is just the beginning. http://www.ericsson.com/thinkingahead/networked_society [Accessed 07-March-2014].

[14] El Gamal, H. 2010. Network society: A social evolution powered by youth. *Network*, 1, 16–26. http://www.gmj-me.com/gmj_custom_files/volume1_issue1/articles_in_english/volume1-issue1-article-16-26.pdf [Accessed 20-May-2014].

[15] ERICSSON. July 2013. Networked society essentials. http://www.ericsson.com/thinkingahead/networked_society/networked_society_essentials [Accessed 07-March-2014].

[16] Lu, L. & Wang, G. 2008. A study on multi-agent supply chain framework based on network economy. *Computers & Industrial Engineering*, 54(2), 288 – 300. http://dx.doi.org/10.1016/j.cie.2007.07.010.

[17] Abdallah, K. & Koskinen, K. 2007. Managing trust: Translating and the network economy. *Meta: Journal des traducteursMeta:/Translators' Journal*, 52(4), 673–687. http://dx.doi.org/10.7202/017692ar.

[18] Information Technologies Group Center for International Development at Harvard University. Readiness for the networked: A guide for developing countries world. http://cyber.law.harvard.edu/readinessguide/index.html [Accessed 25-February-2014].

[19] Ayala, J. L. July 2013. Toward the networked society 2020. http://www.slideshare.net/EricssonLatinAmerica/hacia-la-sociedad-conectada-2020 [Accessed 07-March-2014].

[20] ERICSSON. November 2013. Next generation working life : From workplace to exchange space. http://www.ericsson.com/working-life/wp-content/uploads/sites/2/2013/12/next-generation-working-life.pdf [Accessed 07-March-2014].

[21] Giesecke & Devrient. February 2014. Mwc 2014: Encompassing security solutions for networked society by giesecke & devrient. http://m.gi-de.com/can/en/about_g_d/press/press_releases/MWC-2014%3A-Encompassing-Security-Solutions-for-Networked-Society-by-G%26D-g30208.jsp [Accessed 07-March-2014].

[22] International Organization for Standardization. September 2013. ISO/IEC 27001:2013 information technology – security techniques – information security management systems – requirements.

[23] International Organization for Standardization. September 2013. ISO/IEC 27002:2013 : Information technology – security techniques – code of practice for information security controls.

[24] International Organization for Standardization. June 2008. ISO/IEC 27005:2008 : Information technology – security techniques – information security risk management.

[25] Stoneburner, G., Goguen, A., & Feringa, A. July 2002. NIST 800-30: Risk management guide for information technology systems.

[26] NIST. March 2011. NIST 800-39: Managing information security risk - organization, mission, and information system view.

[27] ISACA. 2012. COBIT 5 - a business framework for the governance and management of enterprise it.

[28] ISACA. 2009. The Risk IT Framework.

[29] Manasdeep. January 2014. ISO/IEC 27001: 2013 How it is different? http://www.slideshare.net/null0x00/iso-27001-2013-changes [Accessed 11-March-2014].

[30] International Organization for Standardization & International Electrotechnical Commission. 2014. ISO/IEC 27002:2013 information technology — security techniques — code of practice for information security controls. http://www.iso27001security.com/html/27002.html [Accessed 11-March-2014].

[31] Sahibudin, S., Sharifi, M., & Ayat, M. May 2008. Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations. In *Modeling Simulation, 2008. AICMS 08. Second Asia International Conference on*, 749–753. http://dx.doi.org/10.1109/AMS.2008.145.

[32] Kennedy, J. T. Internet intricacies: Don't get caught in the net. *Contingency Planning & Management*, 3, page 12.

[33] Kroll Cyber Security. 2012. The 2012 HIMSS analytics report and exclusive webinar. http://www.krollcybersecurity.com/white-papers/himss-2012-report.aspx [Accessed 28-March-2014].

[34] Ponemon Institute LLC. January 2012. The human factor in data protection. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_trend-micro_ponemon-survey-2012.pdf [Accessed 25-March-2014].

[35] Ahmed, M., Sharif, L., Kabir, M., & Al-Maimani, M. 2012. Human errors in information security. *International Journal*, 1(3). http://warse.org/pdfs/ijatcse01132012.pdf [Accessed 27-March-2014].

[36] World Health Organization. September 2007. What is mental health? http://www.who.int/features/qa/62/en/ [Accessed 30-March-2014].

[37] World Health Organization. 2001. Mental disorders affect one in four people. http://www.who.int/whr/2001/media_centre/press_release/en/ [Accessed 30-March-2014].

[38] World Health Organization. December 2013. 10 facts on mental health. http://www.who.int/features/factfiles/mental_health/mental_health_facts/en/index2.html [Accessed 30-March-2014].

[39] World Health Organization. September 2010. Mental health: strengthening our response. http://www.who.int/mediacentre/factsheets/fs220/en/ [Accessed 30-March-2014].

[40] Salmans, S. 1995. *Depression: questions you have-answers you need*. People's Medical Society Allentown, PA, ISBN:978-1882606146.

[41] World Health Organization. October 2012. Depression. http://www.who.int/mediacentre/factsheets/fs369/en/ [Accessed 30-March-2014].

[42] N/A. March 2014. Depression. https://en.wikipedia.org/wiki/Depression_%28mood%29#cite_note-Salmans1995-1 [Accessed 30-March-2014].

[43] National Institute of Mental Health. 2011. What is depression? http://www.nimh.nih.gov/health/publications/depression/index.shtml [Accessed 30-March-2014].

[44] World Health Organization. October 2012. Headache disorders. http://www.who.int/mediacentre/factsheets/fs277/en/ [Accessed 30-March-2014].

[45] Oxford University Press. 2010. "Schizophrenia", Concise Medical Dictionary (8 ed.). http://www.oxfordreference.com/view/10.1093/acref/9780199557141.001.0001/acref-9780199557141-e-9060[Accessed 31-March-2014].

[46] American Psychiatric Association. 2013. Schizophrenia. http://www.psychiatry.org/Schizophrenia [Accessed 31-March-2014].

[47] N/A. March 2014. Schizophrenia. https://en.wikipedia.org/wiki/Schizophrenia#cite_note-1 [Accessed 31-March-2014].

[48] Angres, D. H. & Bettinardi-Angres, K. 2008. The disease of addiction: Origins, treatment, and recovery. *Disease-a-Month*, 54(10), 696–721. http://dx.doi.org/10.1016/j.disamonth.2008.07.002.

[49] American Society of Addiction Medicine. April 2011. Definition of addiction. http://www.asam.org/for-the-public/definition-of-addiction [Accessed 31-March-2014].

[50] American Psychiatric Association. 2014. Addiction. http://www.psychiatry.org/Addiction [Accessed 31-March-2014].

[51] World Health Organization. February 2011. Alcohol. http://www.who.int/mediacentre/factsheets/fs349/en/ [Accessed 31-March-2014].

[52] Besag, V. E. 1989. *Bullies and victims in schools: A guide to understanding and management*. Open University Press Milton Keynes.

[53] American Psychiatric Association. 2014. Bullying. http://www.psychiatry.org/mental-health/bullying [Accessed 31-March-2014].

[54] N/A. March 2014. Bullying. https://en.wikipedia.org/wiki/Bullying#In_different_contexts [Accessed 31-March-2014].

[55] Thomson, R. April 2008. IT profession blighted by bullying. TechTarget. http://www.computerweekly.com/feature/IT-profession-blighted-by-bullying [Accessed 31-March-2014].

[56] N/A. March 2014. Anxiety. https://en.wikipedia.org/wiki/Anxiety#cite_note-Seligman-2 [Accessed 31-March-2014].

[57] American Psychiatric Association. 2014. What is anxiety disorder? http://www.nimh.nih.gov/health/topics/anxiety-disorders/index.shtml [Accessed 31-March-2014].

[58] Grad, F. P. 2002. The preamble of the constitution of the world health organization. http://www.who.int/bulletin/archives/80%2812%29981.pdf [Accessed 05-April-2014].

[59] World Health Organization. 2014. Risk factors. http://www.who.int/topics/risk_factors/en/ [Accessed 05-April-2014].

[60] Oxford University Press. 2014. Parkinson's disease. http://www.oxforddictionaries.com/definition/english/Parkinson%27s-disease?q=Parkinson%27s+disease [Accessed 05-April-2014].

[61] Parkinson's Disease Foundation. 2014. Statistics on parkinson's. http://www.pdf.org/en/parkinson_statistics [Accessed 05-April-2014].

[62] The Michael Stern Parkinson's Research Foundation. 2013. About parkinson's disease. http://www.parkinsoninfo.org/about-parkinsons-disease/ [Accessed 05-April-2014].

[63] Roth, T. 2007. Insomnia: Definition, prevalence, etiology, and consequences. *Journal of clinical sleep medicine: JCSM: official publication of the American Academy of Sleep Medicine*, 3(5 Suppl), S7. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1978319/ [Accessed 01-Apri-2014l].

[64] Minowa, M., Tango, T., et al. 2003. Impact and correlates of poor sleep quality in japanese white-collar employees. *Sleep*, 26(4), 467–471.

[65] Charles W.L. Hill, S. M. 2008. Principles of management: Peer control. http://highered.mcgraw-hill.com/sites/0073530123/student_view0/chapter9/chapter_glossary.html [Accessed 10-April-2014].

[66] Schaufeli, W. B., Leiter, M. P., & Maslach, C. 2009. Burnout: 35 years of research and practice. *Career Development International*, 14(3), 204–220. http://dx.doi.org/10.1108/13620430910966406.

[67] Leiter, M. P. & Maslach, C. July 2013. The areas of worklife and maslach burnout inventory(general survey) group report.

[68] McKeay, M., Corman, J., Thayer, S., Yerric, K., Shpantzer, G., & Daniel, J. August 2011. Burnout in information security. http://www.slideshare.net/secburnout/burnout-in-information-security [Accessed 14-April-2014].

[69] Rouse, M. May 2007. Definition: security policy. http://searchsecurity.techtarget.com/definition/security-policy [Accessed 08-May-2014].

[70] Investopedia US. Definition of 'standard of living'. http://www.investopedia.com/terms/s/standard-of-living.asp#ixzz1VUli2yEI [Accessed 14-April-2014].

[71] Wasserman, S. 1994. *Social network analysis: Methods and applications*, volume 8. Cambridge university press.

[72] Shullich, R. December 2011. Risk assessment of social media. http://www.sans.org/reading-room/whitepapers/privacy/risk-assessment-social-media-33940 [Accessed 17-March-2014].

[73] Scottish Information Assurance Forum. April 2011. Social networking – general risk assessment. http://www.siaf.co.uk/resources/SIAF_snrisks.pdf [Accessed 14-April-2014].

[74] BITS. June 2011. Social media risks and mitigation. http://www.bits.org/publications/security/BITSSocialMediaJun2011.pdf [Accessed 14-April-2014].

[75] N/A. May 2014. Interpersonal relationship. https://en.wikipedia.org/wiki/Interpersonal_relationship [Accessed 25-May-2014].

[76] Albrechtsen, E. & Hovden, J. 2009. The information security digital divide between information security managers and users. *Computers & Security*, 28(6), 476–490. http://dx.doi.org/10.1016/j.cose.2009.01.003.

[77] Argenti, P. A. & Forman, J. 2004. The employee care revolution. *Leader to leader*, 2004(33), 45–52. http://dx.doi.org/10.1002/ltl.88.

[78] Wilson, M. & Hash, J. 2003. Building an information technology security awareness and training program. *NIST Special publication*, 800, p. 50.

[79] Ashford, W. Collaboration is key in enterprise security puzzle. http://www.computerweekly.com/feature/Collaboration-is-key-in-enterprise-security-puzzle [Accessed 21-April-2014].

[80] Christianson, J. 2003. Polycom videoconferencing endpoint security and configuration. http://www.sans.org/reading-room/whitepapers/commerical/polycom-videoconferencing-endpoint-security-configuration_21 [Accessed 28-April-2014].

[81] Ackerman, S. & Ball, J. February 2014. Optic nerve: millions of yahoo webcam images intercepted by gchq. http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo [Accessed 21-April-2014].

[82] Adhikari, R. August 2012. How secure is the cloud, really? http://www.technewsworld.com/story/76019.html [Accessed 12-May-2014].

[83] Babock, C. March 2014. 9 worst cloud security threats. http://www.informationweek.com/cloud/infrastructure-as-a-service/9-worst-cloud-security-threats/d/d-id/1114085 [Accessed 12-May-2014].

[84] Yunus, M. December 2009. "Swamp Computing" a.k.a. Cloud Computing. *Web Security Journal*. http://security.sys-con.com/node/1231725 [Accessed 12-May-2014].

[85] Cloud Security Alliance. February 2013. The notorious nine: Cloud computing top threats in 2013. http://www.cloudsecurityalliance.org/topthreats/ [Accessed 12-May-2014].

[86] Search Security. 2014. Guardians of the crown jewels. http://searchsecurity.techtarget.com/magazineContent/Guardians-of-the-Crown-Jewels [Accessed 01-May-2014].

[87] GovInfoSecurity. 2014. The three Ds of incident response - protecting your company from insider threats. http://www.govinfosecurity.com/webinars/three-ds-incident-response-protecting-your-company-from-insider-threats-w-403 [Accessed 01-May-2014].

[88] Hunker, J. & Probst, C. W. 2011. Insiders and insider threats—an overview of definitions and mitigation techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 2(1), 4–27.

[89] Bishop, M. & Gates, C. 2008. Defining the insider threat. In *Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead*, 15. ACM. http://doi.acm.org/10.1145/1413140.1413158.

[90] Federal Bureau of Investigation. 2014. The insider threat: An introduction to detecting and deterring an insider spy. http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat [Accessed 03-May-2014].

[91] National Cyber Security Alliance. 2014. Cyber risk assessment and management. http://www.staysafeonline.org/re-cyber/cyber-risk-assessment-management/ [Accessed 01-May-2014].

[92] Schor & Freeland LLP. 2014. 9 steps to take today to protect your company's assets now and in the future. http://www.schorfreeland.com/newsletter06.htm#creating%20a%20weapon [Accessed 01-May-2014].

[93] Schor & Freeland LLP. 2014. How to protect your proprietary information and reduce potential liability through a confidentiality agreement. http://www.schorfreeland.com/newsletter06.htm#creating%20a%20weapon [Accessed 01-May-2014].

[94] Nasjonal Sikkerhetsmyndighet. 2014. Sikkerhetsklarering. https://www.nsm.stat.no/Arbeidsomrader/Personellsikkerhet/sikkerhetsklarering/ [Accessed 01-May-2014].

[95] SANS. 2014. Critical security controls for effective cyber defense. https://www.sans.org/critical-security-controls/ [Accessed 01-May-2014].

[96] Houmb, S. H. 2013. Høgskolen i Gjøvik: Information Security Economics lecture 1.

[97] Su, X. 2006. An overview of economic approaches to information security management. Centre for Telematics and Information Technology University of Twente.

[98] Anderson, R. 2001. Why information security is hard - an economic perspective. In *Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual*, 358–365. IEEE. http://dx.doi.org/10.1109/ACSAC.2001.991552.

[99] Schneier, B. January 2008. The psychology of security. https://www.schneier.com/essay-155.html [Accessed 05-June-2014].

[100] Wolter, K. & Reinecke, P. 2010. Performance and security tradeoff. In *Formal methods for quantitative aspects of programming languages*, 135–167. Springer. http://dx.doi.org/10.1007/978-3-642-13678-8_4.

[101] Sandhu, R. 2003. Good-enough security: Toward a pragmatic business-driven discipline. *IEEE Internet Computing*, 7(1), 66–68. http://dx.doi.org/10.1109/MIC.2003.1167341.

[102] Elahi, G. & Yu, E. 2009. Modeling and analysis of security trade-offs - a goal oriented approach. *Data & Knowledge Engineering*, 68(7), 579–598. http://dx.doi.org/10.1016/j.datak.2009.02.004.

[103] European Community's Seventh Framework Programme. 2010. Valuesec project. http://www.valuesec.eu/content/valuesec-project [Accessed 05-June-2014].

[104] Castells, M. & Cardoso, G. 2005. The network society: From knowledge to policy. *The Network Society From Knowledge to Policy*, 1. http://www.ebooksmagz.com/pdf/the-network-society-university-of-massachusetts-amherst-181985.pdf [Accessed 04-April-2014].

[105] Gregory, M. A. & Glance, D. 2013. Security and the networked society. ISBN: 978-3-319-02390-8.

[106] Hetrick, K. December 2013. World future society: Smarter software's impacts on human privacy. http://www.wfs.org/futurist/2013-issues-futurist/november-december-2013-vol-47-no-6/smarter-softwares-impacts-human-pri [Accessed 09-May-2014].

[107] World Future Society. June 2014. 3-d printing keeps growing. http://www.wfs.org/futurist/2014-issues-futurist/may-june-2014-vol-48-no-3/3-d-printing-keeps-growing [Accessed 11-May-2014].

[108] Abelow, D. April 2014. World future society: Your devices will have no limits. neither will you. http://www.wfs.org/blogs/dan-abelow/your-devices-will-have-no-limits-neither-will-you-0 [Accessed 11-May-2014].

[109] Scarborough, M. S. February 2011. Global knowledge: Understanding and managing the risk. http://www.brandchannel.com/images/papers/528_global_knowledge_paper_change-mgmt_0811.pdf [Accessed 14-May-2014].

A First Appendix: Interview 1

Siv Hilde Houmb, Assosciate professor II of Gjøvik University College

The interview was conducted by using Skype Video Conferencing

1. What does "human and organizational risk" mean in your organization? And what do you think it means in general?
   Answer:
   The human and organizational risks normally categorize into two groups:

   - Accidental human errors, which include organizational miss communication, organizational structure does not support human actions.
   - Intentional insider threats, almost 90 percent of major really critical cyber-attacks and security attacks are caused in some kind of way by insiders. It is usually very difficult to detect insider threats, so in a lot of ways you monitor it through technical system. The technical means can monitor people where they get access to and what they do, but it might not give what you want.

   In general, human risk means a person uses his/her relationship or association to an organization to gain access to inside. The organizational risk is usually the consequence of human risk, which interns the way of social works, e.g. the organization's employees miss use of the rules, employees use organization's structure to get access into the system.

2. What are the major human and organizational risks and uncertainties which your organization faced in the last 5-10 years?
   Answer:
   The major human and organizational risks are:

   - People leave the company, previous employees might take information with them.
   - People intentionally bring information out, which could be technical drawings, architecture drawings, Intellectual Property related staffs.
   - Insider threats. People moving around your organization to get access to the company.
   - Lack of proper classification of documentation, which may lead to too many people get access to very confidential information.
   - People do not encrypt with their disks, bring information on the flights, leave them on the airport

   The uncertainties that you might face in next 5-10 years:

- Core people leave company and take the knowledge with them, which means you lose a competency area.
- Company restructure. Every time the new structure of a company and a new strategy will lead to the company consistently changing, and will face the risk that loss of control.

3. How does the organization identify the human and organizational risks that it faced?
   Answer:
   That is usually none existing.

4. Were the human characteristics behavior and associated risks sufficiently covered in information security management system? If yes, tell me how. If no, tell me what was missing. How it is change over time?
   Answer:
   The information security management system deals with access control, security awareness, training. E.g., the ISO27001, it includes access to systems, security awareness, making people trained and been conscious about information security. It changes from no security awareness to having security awareness.

5. What are the anticipated new human and organizational risks due to centralization in data center, cloud service, and mobility in the next 5-10 years?
   Answer:
   These will give access ability to data. Therefore, educating people on classifying information, placing information where it should be, and being awareness about the information should be distributed would be very important. There are two main risk:

   - Lose control of information.
   - Risk of information leakage.

6. How does the information officers perform the human and organizational risk assessment?
   Answer:
   Ad-hoc, which means there is not structured approach, it might be a problem that will be discussed. People use ad-hoc to doubt with potential risks, e.g. if there is an issue with a person, the information security officer might start paying attention to this person.

7. Which framework do you use for dealing with human and organizational risk management?
   Answer:
   There is no any structure we can use. The only thing we can use is the control in ISO 27001, actually it does not applicable, but it is the only framework addresses human and organizational risks.

8. What does human situation and human behavior mean in information security, how do they affect each other?
   Answer:
   There are several risks:

- People become stress about work, which affects their judgment, they cannot concentrate enough on their job and also they might need to bypass security mechanism to get their job done.
- Having an issue at home, people's barrier of doing something will be reduced, which could be they give their passwords.

9. What is the business impact and its associated risks when introducing extensive collaboration, for instance: tools, outside partners, client and so on?
   Answer:
   The main risk is leakage of information. The business impact of it might be get your IP compromised, which can lead to you lose your customers, you competitor can gain advantages from you by using your IP.

10. What are the conditions to allow someone to deal with "crown jewels"?
    Answer:

    - Security clearance.
    - Loyalty.
    - Know the people's personality.
    - Check their reference.
    - People who can deal with "crown jewels" should be an internal people.

11. What risks should be considered when we approach total networked society?
    Answer:
    The main issue is information leakage. It will be hard to control information, and it will be hard to control how people move information, what people discuss with the information.

12. How to assess and measure security over and under spending in managerial, human and organizational process?
    Answer:
    You have to be able to measure how much is the investment and what is the result. But, it is difficult to measure and observe humans.

13. Which environmental, technology, societal and some other parameters must be observed and what is the time line to reassign risks?
    Answer:

    - Environmental parameter: it can be spills or anything.
    - Technical parameter: People.
    - It depends on national and international, the organizational level.

    For reassigning risks, you need to know what the risk changed compared the last time you assess it. If there is no change, there is no need to reassign the risk. The time line to reassign risks might be every 10th year.

14. What should be an ideal situation for an organization considering human issues for overall information security management system?
    Answer:
    A separate professional group that works with human and organizational risk management, which has the monitoring capability and the ability to decide how to address issues.

15. What strategies does the organization use to manage human and organizational risks?
    Answer:
    Ad-hoc. It based on perception, observation of strange behaviors, anything related to documents.

B Second Appendix: Interview 2

Thomas Schlienger, Consultant of TreeSolution AS

The interview was conducted by using Skype Video Conferencing

1. What does "human and organizational risk" mean in your organization? And what do you think it means in general?
   Answer:
   For addressing the human and organizational risk, it is very important to analyze and improve the information security culture in the organizations, which can help the organizations to measure how big their human risks are and how they can lower the risks.

   In general, human and organizational risk means a people applied risks in a company, it can be a human error, e.g. people share information they should not share.

2. What are the major human and organizational risks and uncertainties which your organization faced in the last 5-10 years?
   Answer:
   The major organizational risks are:

   - Today, the business is getting more and more complex. Due to the complexity of business, people working on it but do not understand it very well.
   - The commitment in the company is going down, personnel change in the company is very quickly, so it is difficult to build trust among employers and employees.

3. How does the organization identify the human and organizational risks that it faced?
   Answer:
   They almost not do it. Many information security standards are not good enough to manage human and organizational risks. Therefore, I have developed a new approach for measuring information security culture and identifying the risks of this culture.

4. Were the human characteristics behavior and associated risks sufficiently covered in information security management system? If yes, tell me how. If no, tell me what was missing. How it is change over time?
   Answer:
   The ISO27001, it includes security awareness, training employees. But every company should have their own strategy, which includes how they would like to influence people's behaviors. If the company only concentrate on training, it is far than enough.

5. What are the anticipated new human and organizational risks due to centralization in data center, cloud service, and mobility in the next 5-10 years? 30
   Answer:
   For the cloud service, we have problems of trust.
   Due to everything is centralized, if several companies stored all the data into one data center, one side we might have technical failure, another problem is people who working at these data center may access to it.
   For the mobility, we have problem that data get transferred frequently, as such, you may do not know where it is, and it is difficult to control them.

6. How does the information officers perform the human and organizational risk assessment?
   Answer:
   They use the ISO 27001 standard. And some companies perform trainings, they take e-learning of the information security, at the end of e-learning they will have a test, the test result can help them start a new measure to improve human behavior.

7. Which framework do you use for dealing with human and organizational risk management?
   Answer:
   We can use the control in ISO 27001 and the approach of analyzing information security culture of the company.

8. What does human situation and human behavior mean in information security, how do they affect each other?
   Answer:
   There are several risks:

   - People addicted to drugs, alcohol, gambling.
   - Problems from the family.
   - Health problems.

9. What is the business impact and its associated risks when introducing extensive collaboration, for instance: tools, outside partners, client and so on?
   Answer:
   The most critical problem is the trust problem.

10. What are the conditions to allow someone to deal with “crown jewels”?
    Answer:

    - Know the people very well.
    - Long-term relationship.

11. What risks should be considered when we approach total networked society?
    Answer:
    Among a lot of traditional risks we face in IT in general, I see mainly three big picture risks:

- Industrial espionage (everything is at the fingertips of everyone).
- Ultimate dependencies from critical infrastructures like electricity and internet access/bandwidth.
- Changes in society which require new ways of living together and also new laws and law enforcement agencies

12. How to assess and measure security over and under spending in managerial, human and organizational process?
    Answer:
    To assess and measure security spending we can compare the result between before security spending and after security spending. We can through a triangulation to measure it, which means you combine several methods to measure the same thing. Then we should combine several output to get a better result.

13. Which environmental, technology, societal and some other parameters must be observed and what is the time line to reassign risks?
    Answer:
    You should observed as much as you can. You have to done something to improve the situation, it will take a time, and after that time you can measure it again. For instance, when are doing security awareness campaign, do not measure it at the moment when this campaign finished, wait three months then measure it.

14. What should be an ideal situation for an organization considering human issues for overall information security management system?
    Answer:
    The ideal situation would be the human issues are integrated into the information security management system.

15. What strategies does the organization use to manage human and organizational risks?
    Answer:
    ISO 27001 and the information security culture method.

C Third Appendix: Interview 3

Stewart Kowalski, Professor of Gjøvik University College

The interview was conducted by using Skype Video Conferencing

1. What does "human and organizational risk" mean in your organization? And what do you think it means in general?
   Answer:
   I worked both in public and private organizations before. The human risks are often considered the area of safety. The organizational risk, we divided it into business risk (e.g. market risk) and operational risk.

   In general, risk is defined as probability of either positive or negative advantage to affect organization. Risk can be both good and bad.

2. What are the major human and organizational risks and uncertainties which your organization faced in the last 5-10 years?
   Answer:
   The major organizational risk is losing business. The biggest organizational problems are competitors and the loss of control over the finances.

   The major human risk is people stealing and trying to hurt the company. The biggest human risk is human error, which means people make mistakes but they are not trying to be malicious.

   In the last 5-10 years, the organizational risk was competitors, and the human risk was people making delivery mistake or accidental mistakes.

3. How does the organization identify the human and organizational risks that it faced?
   Answer:
   In the organization I worked before, we do risk analysis once a year. The other method we use is scenario excises.

4. Were the human characteristics behavior and associated risks sufficiently covered in information security management system? If yes, tell me how. If no, tell me what was missing. How it is change over time?
   Answer:
   In the information security system, they put the responsibility of human risks on the managers, but the information security system did not give enough resources to managers for

dealing with human risks. So the change should be the managers get more resources to deal with human risks. And the Whistleblower function is becoming bigger now, which can report human risks.

5. What are the anticipated new human and organizational risks due to centralization in data center, cloud service, and mobility in the next 5-10 years?
   Answer:
   The biggest challenge is we do not know who is responsible for the security.

6. How does the information officers perform the human and organizational risk assessment?
   Answer:
   Information security officer will talk to the line manager to get more information, some cases they will use internal investigation, some cases they will go to external.

   The line manager is given the responsibility for dealing with human issues, because they interact employees more often. A line manager should not have more than 10 employees to responsible. To deal with human issues, it need to have an often contact. If we put the responsibity to HR department, due to they are too centralized, it is very difficult for them to understand the whole organization.

7. Which framework do you use for dealing with human and organizational risk management?
   Answer:
   ISO 27001 and capability maturity model.

8. What does human situation and human behavior mean in information security, how do they affect each other?
   Answer:

   - Stress: time pressure
   - People are not happy for their work.
   - Be sense of distribution, fairness.
   - Different countries have different income equality.

9. What is the business impact and its associated risks when introducing extensive collaboration, for instance: tools, outside partners, client and so on?
   Answer:
   The winwin situation. The less winwin situation, the higher risks.

10. What are the conditions to allow someone to deal with “crown jewels”?
    Answer:

    - Be able to suave the damagers
    - Know your enemies.
    - Know the person’s financial statement.

11. What risks should be considered when we approach total networked society?
    Answer:
    Small mistake can create very large problems.

12. How to assess and measure security over and under spending in managerial, human and organizational process?
    Answer:
    Bench marking. How much you enemies spend for attacking you system, and then you should spend more for defensing your system.

13. Which environmental, technology, societal and some other parameters must be observed and what is the time line to reassign risks?
    Answer:
    Any time you have a major change, then you should have a new risk done. Both the organizational changes or the technical changes.

14. What should be an ideal situation for an organization considering human issues for overall information security management system?
    Answer:
    Line manager should get support from the information security manager.

15. What strategies does the organization use to manage human and organizational risks?
    Answer:
    Awareness campaign and dialogs, and create a culture with escalation process. People willing to face their mistakes and problems, and they will not be punished by the information security problems.

D Fourth Appendix: Interview 4

Hans Marius Tessem, Senior Adviser of NorSIS

The interview was conducted by using Skype Video Conferencing

1. What does "human and organizational risk" mean in your organization? And what do you think it means in general?
   Answer:
   My organization is dealing with human risks on a national basis, one big part of our work is teach public about awareness. In the internal organization, there is no program for handling human factor risks in NorSIS. One reason is we are a small organization, another reason is since we are working on human risks, the leader assumes that we do not need to deal with that problem internally. The human risks are most of the companies take seriously, but they do not know how to handle it.

   In the NorSIS, we also have a lot of human risks, but the individual employee is aware. In everything the employee does is aware that what he/she doing now can be a risk.

2. What are the major human and organizational risks and uncertainties which your organization faced in the last 5-10 years?
   Answer:
   The major risk is we do not update webservers, the person responsible for that but do not do it. Problem for small organizations is one person has a lot of tasks for handing the security, if one person fails the organization will face a big problem. The other risks can be lose equipment, improper back-up.

3. How does the organization identify the human and organizational risks that it faced?
   Answer:
   In NorSIS, we do not identify the human risks on a day to day basis, because we understand the problems. If in some other small organizations in Norway, I think they do not identify human risks, they may understand that it can be a risk, but how they identify them is very random. A lot of small companies identify human and organizational risk when it occurs or when it is a problem. The medium and large size of companies, some of them use ISO standards but that is not a good tool to identify human risks. Identifying human risk in these companies is largely based on the competency of the person who handles information security.

4. Were the human characteristics behavior and associated risks sufficiently covered in information security management system? If yes, tell me how. If no, tell me what was missing.

How it is change over time?
Answer:
No. There is no standard on how to handle it, as such, a lot of companies they make their own standard to handle it.

5. What are the anticipated new human and organizational risks due to centralization in data center, cloud service, and mobility in the next 5-10 years?
   Answer:
   The obvious problem is people have bad passwords. When it comes to mobility the problem is people lose equipment and they do not have passwords on that equipment as well. Another risk is when you put things into a cloud, you need several levels of encryption, if someone break the cloud, they will only get the encrypt data. How to handle the encryption locally, is it easy to encrypt or it is hard? If it is made hard, it will be difficult for the user to encrypt it, then it will be a problem.

6. How does the information officers perform the human and organizational risk assessment?
   Answer:
   It is different from one organization to another organization. I think the usual way they do it is: they just recognized it is a risks, then put it them into a normal risk assessment process.

7. Which framework do you use for dealing with human and organizational risk management?
   Answer:
   In NorSIS we do not use any frameworks. The ISO is normal for dealing with human and organizational risks.

8. What does human situation and human behavior mean in information security, how do they affect each other?
   Answer:
   It depends on the value of that human.

9. What is the business impact and its associated risks when introducing extensive collaboration, for instance: tools, outside partners, client and so on?
   Answer:
   It depends on how your organization is organized. For example, in NorSIS, where the security is based on individual, if we do not have a specific knowledge in information security it could be problems, e.g. we could give away information that we should not. If the organization restricts it on a technical level, it is a smaller risk, but it still has human related problems.

10. What are the conditions to allow someone to deal with “crown jewels”?
    Answer:
    It depends on the business, it is not just conditions.

11. What risks should be considered when we approach total networked society?
    Answer:
    Firstly, we need to ask where my data are and how it is protected. That is perhaps the most important thing. And if something shucks down, will I still have my data? Can I keep my business as usual if something goes down? When data is traveling how to make it secure? These problems do really need us to think about when we are in the network society.

12. How to assess and measure security over and under spending in managerial, human and organizational process?
    Answer:
    How to measure a human is very difficult, as such I would say it is impossible. So I think instead of talking about measuring all the time, we need to talk about having open channels for getting information that you can prevent something bad to happen. It is very importance to have good communications, this is the way to control or change something.

13. Which environmental, technology, societal and some other parameters must be observed and what is the time line to reassign risks?
    Answer:
    When you recognized organizations, when you change technology you need to reassign risks. Actually, when we do changes we need to reassign risks.

14. What should be an ideal situation for an organization considering human issues for overall information security management system?
    Answer:
    There should have a position that handle this problem in the organization. A position between IT and HR positions. They should have a triangle relations, the position of handling human risks should communicate with both IT and HR department, and tell them what they should do.

15. What strategies does the organization use to manage human and organizational risks?
    Answer:
    Actually a lot of companies they do not have strategies for handling human and organizational risks, they might have a strategy states that manage human and organizational risk is important for us. They might have e-learning, which teaches employees do not have a bad password, do not open the attachment of e-mail, etc. However, they also should teach them about the way that you might be fooled, because the attacks change all the time.