jamk.fi

Implementing Information Security Management System as a part of business processes

Where to gain competitive advantage for ISMS?

Jari Flyktman

Master's thesis
June 2016
Technology, ICT
Master´s Degree Programme in Information Technology

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Description

Author(s) Last name, First name Flyktman, Jari	Type of publication Master's thesis	Date June, 2016
		Language of publication: English
	Number of pages 91	Permission for web publication: x

Title of publication

Implementing Information Security Management System as a part of business processes

Where to gain competitive advantage for ISMS?

Degree programme

Master´s Degree Programme in Information Technology

Supervisor(s)

Kotikoski, Sampo

Assigned by

Inmics Oy

Abstract

The Idea and background to the study subject lies in the interest in security, leadership and organizational development. The research question was how to provide best practices to fit these all together in harmony.

The objective was to help small and medium sized organizations to understand the multifaceted nature of cybersecurity and requirements for successful implementation of information security management system (ISMS). ISMS help companies to form the needed security structures in practice.

The thesis was implemented using qualitative action research methodologies. The research data was collected during several years' timeframe from literature, mainly in fields of management, military sciences, information security and behavioural science.

As a result, a practical approach on what should be considered while implementing security management system was formed. The aim for this is to help companies to form strong security structure within their company. The central idea behind this is how the presented frameworks could be used to form better communication and cohesion between individuals and groups in an organization and how this could help the target audience to achieve better organizational performance.

The conclusion made from the research was that an Information Security Management System (ISMS) should be taken into consideration while forming company's processes. Even though OODA loop itself was not found the most suitable solution for longer term planning cycles as such, the adaptation of OODA loop and Cynefin framework are recommended and they have been found appropriate to support leadership in constantly evolving, emerging situations.

Keywords/tags (subjects)

ISMS, PDCA, OODA loop, Cynefin, information security, cybersecurity

Miscellaneous

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Flyktman, Jari	Opinnäytetyö, ylempi AMK	Kesäkuu 2016
	Sivumäärä 91	Julkaisun kieli Englanti
		Verkkojulkaisulupa myönnetty: x

Työn nimi

Implementing Information Security Management System as a part of business processes

Where to gain competitive advantage for ISMS?

Tutkinto-ohjelma

Master´s Degree Programme in Information Technology

Työn ohjaaja(t)

Sampo Kotikoski

Toimeksiantaja(t)

Inmics Oy

Tiivistelmä

Innoitus ja tausta tutkia aihetta ovat tekijän kiinnostuksessa turvallisuuteen, johtajuuteen ja organisaation kehittämiseen. Tutkimuskysymys oli, kuinka sovittaa edellä mainittujen kokonaisuuksien parhaat käytännöt sopusointuisesti yhteen.

Tarkoituksena on auttaa pieniä ja keskisuuria yrityksiä ymmärtämään kyberturvallisuuden monitahoista luonnetta sekä vaatimuksia tietoturvallisuuden hallintajärjestelmän menestykselliselle kehittämiselle. Hallintajärjestelmä mahdollistaa turvallisuusrakenteiden muodostamisen yritykseen onnistuneesti.

Toteutus tehtiin käyttäen kvalitatiivisia toimintatutkimuksen menetelmiä. Tutkimusaineisto kerättiin usean vuoden aikana kirjallisuudesta, pääosin johtamisen, sotilastieteiden, tietoturvallisuuden ja käyttäytymistieteiden aloilta.

Tuloksena muodostui käytännönläheinen näkemys siitä, mitä tulee ottaa huomioon toteutettaessa tietoturvallisuuden hallintajärjestelmää. Keskeinen päämäärä tutkimuksessa on tuoda julki, kuinka esitetyt viitekehitysmallit voivat auttaa yhteisöä ymmärtämään ilmiötä, kommunikoimaan paremmin sekä luomaan viestinnällä yhtenäisyyttä eri organisaatioryhmien ja asiakkaiden välille. Paremmin ymmärretty viestintä mahdollistaa yritystä saavuttamaan paremman suoritustason ja vakuuttaa asiakkaat osaamisesta.

Tutkimuksen päätelmänä on, että tietoturvallisuuden hallintajärjestelmä (ISMS) tulee ottaa huomioon, kun yrityksen prosesseja muodostetaan. Vaikka OODA-silmukan sellaisenaan ei havaittu olevan kaikkein sopivin ratkaisu suunnitteluun, OODA-silmukan ja Cynefin-kehysmallin omaksumista suositellaan ja ne nähtiin sopivina tukemaan johtajuutta jatkuvasti kehittyvissä, orastavissa tilanteissa.

Avainsanat (asiasanat)

ISMS, PDCA, OODA loop, Cynefin, tietoturvallisuus, kyberturvallisuus

Muut tiedot

Contents

Figures

Tables

List of abbreviations

APT	Advanced persistent threat
BSI	The British Standards Institution
BYOD	“Bring Your Own Device”
CISO	Chief Information Security Officer
CMM	Capability Maturity Model
CSIS	Center for Strategic and International Studies
DHS	U.S Department of Homeland Security
EC	European Commission
ENISA	The European Union Agency for Network and Information Security
EU	The European Union
IEC	The International Electrotechnical Commission
$(ISC)^2$	The International Information Systems Security Certification Consortium
ISSEA	The International Systems Security Engineering Association
ISO	The International Organization for Standardization (in English)
IoT	Internet of Things
ISMS	Information Security Management System
ITIL	Information Technology Infrastructure Library
KPI	Key Performance Indicator
LIGO	Laser Interferometer Gravitational-Wave Observatory
MoD	U.K Ministry of Defense
MP	Member of Parliament
NCSP	(U.K) National Cyber Security Programme
NSA	U.S National Security Agency

PDCA	Plan – Do – Check – Act, model used to describe continuous improvement
RC	Reflexive Control
ROI	Return Of Investment, metric to measure return on money invested in an entity in order to decide whether or not to undertake an investment.
SME	Small and mid-sized company
SOP	Standard Operating Procedure
U.K	United Kingdom
U.S	United Stated Of America
USAF	United States Air Force
VTT	VTT Technical Research Centre of Finland Ltd

1 Introduction

In modern world organizations and their business operations are highly dependent on different information systems, no matter if they are public or private. It would not be an overstatement to say that our whole society is somehow reliant on information systems and their security.

As an example, our modern way of life is somehow dependent on technology from the moment an electric alarm clock wakes us up in the morning until the moment we turn off the lights in the evening before going to have a good night sleep. Even during the night there are systems which monitor our sleep, air quality and amount in our bedroom, temperature and so on. We have a constant relationship to technology from our birth to our last breath, 24/7, around the year. These conveniences are provided to us by companies which have built their businesses on those.

Technology serves us in many ways, which is good. Modern technology and its development have made such things possible which were visions of sci-fi writers few decades or only years back. It has created whole new lines of business and good opportunities to capable persons and companies willing to take advantage of this rapid development. Technology helps us many ways and makes our lives comfortable, releasing our time for matters that make life fun and worth of living. For companies technology means new business opportunities or a cost effective way to implement processes to support business, which also means that companies must be capable to take cybersecurity issues into consideration and that is where one of the biggest risks in computerized world lies according the Nokia Group's Chairman Risto Siilasmaa (Dahlgren 2016).

2 Trust, resources and how to gain those with help of processes

We share our information carelessly with our friends and third parties interested in it, which make it possible for them to serve us and our way of living. At the same time, technology has lulled us into good faith that everything is fine and affairs will continue going their smooth, effortless way.

In that sense technology has become a master instead of drudge, which it should and is supposed to be.

2.1 Significance of trust

Current situation is a kind of mirage and tells an observer about the significance of trust. A great majority of people have trust on technology and its purposes. Author – and most probably many others – think that trust is the glue which binds our society together. Trust makes it possible to communicate, trade and carry out other transactions which are the basis of the world as we know it in our time. Without trust technology could not serve society and its functions like it does currently. But should technology be trusted without suspiciousness? Many people, like professor Anu Kantola from Helsinki University Department of Social Research Media and Communication Studies, think that criticism should be kept in mind, unless it actually can be seen which master it serves and what is happening behind closed curtains (Lotila 2016). What happens if trust, which is currently shown, is lost or damaged? How could this trust be shaken and by what means? Can the situation be handled, does the society have resilience if all this good goes due to the lack of confidence? How can these systems affecting the everyday life be made and prepared to be more trustworthy?

Securing information is often seen mainly as a technology related task, however, technology per se does not guarantee success either for the organization or the task. The concept of securing information and information systems is a complex, multifaceted task in which human interactions have a remarkable role. The International Information Systems Security Certification Consortium states *"…that people are the most critical part of effectively securing an organization*" ((ISC)² 2009, 1). Often information security is seen primarily as a cost, but the question could be asked how information security could give a competitive advantage for the organization by supporting organization's business goals.

2.2 The most important assets and tasks for security management

To align mentioned initiatives, company has to have resources to accomplish information security related tasks. Formerly most organizations relied on a few professionals in the IT department dedicated to the security of their infrastructure (Cho 2003, 4), however, as stated earlier, information security is not only technique and does not demand only technical skills. In addition to those, persons involved should have skills for team work, fluent communication in both written and oral form, understanding of company business and processes, and they should be able to provide training, just to mention few. Of course such "super humans" with all necessary skills and needed time to complete them all are rare. Instead, a team responsible for company's information security should have all the mentioned skills.

A team formed from such separate skill sets and personalities naturally demands daily management and guidance. The person managing this skill set is called Chief Information Security Officer, or CISO for short. CISO is a senior-level executive responsible for aligning security initiatives with company policies and business requirements, ensuring that information assets and technologies are adequately protected (Cho 2003, 4-7). Julia Allen et al. have recognized four key functions which cover majority of CISO's responsibilities as follows (Allen, et al. 2015, 1) :

- *"**Protect, Shield, Defend, and Prevent***
  Ensure that the organization's staff, policies, processes, practices, and technologies proactively protect, shield, and defend the enterprise from cyber threats, and prevent the occurrence and recurrence of cybersecurity incidents commensurate with the organization's risk tolerance.
- ***Monitor, Detect, and Hunt***
  Ensure that the organization's staff, policies, processes, practices, and technologies monitor ongoing operations and actively hunt for and detect adversaries, and report instances of suspicious and unauthorized events as expeditiously as possible.
- ***Respond, Recover, and Sustain***

When a cybersecurity incident occurs, minimize its impact and ensure that the organization's staff, policies, processes, practices, and technologies are rapidly deployed to return assets to normal operations as soon as possible. Assets include technologies, information, people, facilities, and supply chains.

- ***Govern, Manage, Comply, Educate, and Manage Risk***
  Ensure that the organization's leadership, staff, policies, processes, practices, and technologies provide ongoing oversight, management, performance measurement, and course correction of all cybersecurity activities. This function includes ensuring compliance with all external and internal requirements and mitigating risk commensurate with the organization's risk tolerance."

The guidance to fulfil the previous needs could be then provided by a properly formed and managed Information Security Management System (ISMS); however, before getting in to ISMS, an overview of the processes is taken for that ISMS is created to protect and serve.

2.3 Division and relations of processes

Thomas Davenport has defined processes as follows: "*…a process is simply a structured, measured set of activities designed to produce a specified output for a particular customer or market. It implies a strong emphasis on **how** work is done within an organization, in contrast to a product focus's emphasis on **what**.*

A process is thus a specific ordering of work activities across time and place, with a beginning, an end, and clearly identified inputs and outputs: a structure for action. " (Davenport 1992, 12). As noticed by Davenport, before process can be accomplished, processes should have clearly identified inputs, meaning resources like time and money, which further produce outputs like services for other processes or security processes for the whole organization.

If looking from business management perspective, each service causing costs should be taken into account in a budget, it should have key point indicators (KPI) based on requirements (by legislation, customer or business requirement) to measure its effectiveness. To find out the previous, process

should be described to know what that particular process does include and does not include.

Describing processes is work which is done last when when company plans adopting some standardization process like ISO9001 (quality management) or in ICT-business more commonly ISO20000 (IT service management). Standards have noticed the meaning of the information security and they have a requirement that also security processes are described along business processes. (ITSMF 2009, 78-81).

ITIL v3 advices that to meet all requirements, service design should include (among many others) "*legal or regulatory compliance requirements, e.g. required security levels*" and "*The technology required to support and deliver the service: the data, applications, infrastructure and environment*". (ITSMF 2009, 49). The first requirement includes security management and the latter technological means to provide the required security level for the covered service. Thus, security services should be no difference and they should be treated from the management's perspective just like any other business service or process needed to deliver those. Important in this is the word "required", in which implicates security to service which has a requirement for that. In practice this means that the provided security control is provided for business needs and business requirements should be considered while security service is implemented. It not stated explicitly in the requirement, implicitly this means that security is part of business service and the appropriate service must uphold its costs. This is essential while considering the effect between security and business services.

2.4 What are the business processes?

The definition of what business processes are, varies a great deal in literature. In this thesis the definitions are based on recommendations used largely in Finland, The Public Administration Recommendations (JHS recommendations). In this thesis, business processes are considered such processes that are critical for an organization's operations and success.

Business processes could be further divided into sub processes. Processes

producing value (service) for external parties (customers), are called core processes and they are not taken into account in this research. To clarify core processes further, they are processes needed to produce billable services directly to customers. In many cases, security processes are not considered core processes, unless they are products themselves.

Supporting processes are a company's internal processes which are a requisite for the company's operations (JUHTA 2012, 7). Importance of supporting processes is often noticed after they do not work as expected. Processes go throughout the organization and they ignore organizational limits and might continue also to customers (if agreed) or partially to (sub) contractor's organization. The processes managed by Information Security Management System (ISMS) are in this study regarded as internal processes of company, i.e. support process.
In following figure, the author has tried to explain how business processes are divided; what is the functional difference between different process types.

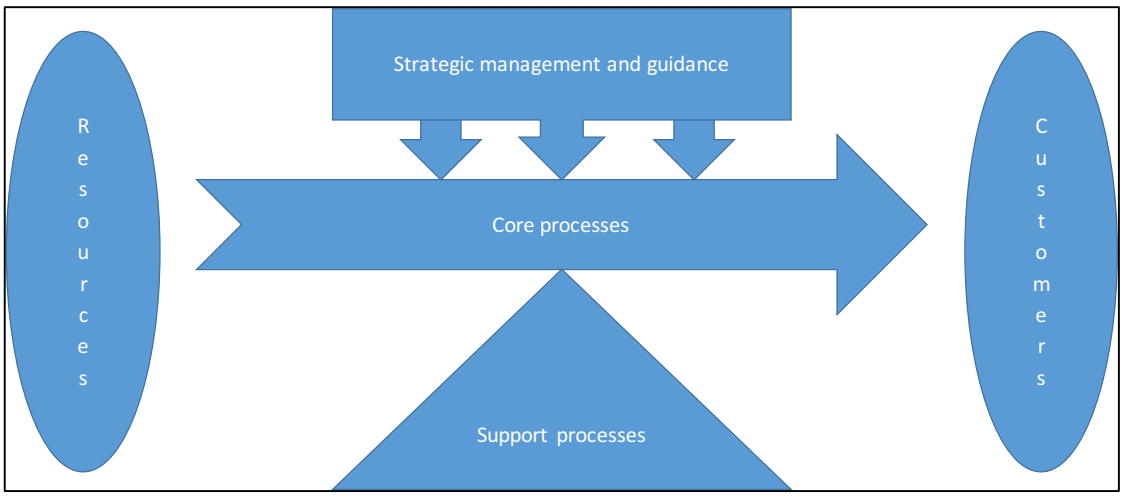


Figure 1 Business process division simplified

Even though the business process division is a highly simplified illustration, it has the most important key elements in place (JUHTA 2012):

- Resources responsible of delivering Core processes to Customers
- Core processes balancing oneself on top of support processes
- Strategic management and guidance bringing stability and harmony to business processes
- Customers receiving value from the provided service.

Please notice that “Strategic management and guidance” could also turn from “harmony giver” to an unbalancing factor if one of its pressure points becomes stronger than another one. This encourages the fact that matters must be kept in balance by management.

3 Goals, structure, method and frameworks

In the following chapters the Author is describing the goals and structure of the thesis work. Aim here is to give audience better understanding of why and how thesis is formed, what are the delimitations and how process from initial thoughts to conclusions actually took place.

3.1 Goals and focus for the thesis

This thesis focuses on how ISMS will help especially small and medium size companies to achieve their business goals and why having ISMS is that important. To find this out the thesis clarifies why cyber security is everyone’s concern, what is the estimated size and total loss caused by cyber criminals globally and what makes estimating these losses difficult. One of the goals while making initial planning of the thesis was that it somehow must be pragmatic and practical. That for the thesis has aspect on how to improve a company’s security, what are such subliminal threat factors that have effect on observations and which would not necessarily be even noticed until it is too late, and finally, how to possibly take this into consideration. As a telescope to put matters in focus the OODA loop was selected, and this thesis explains how it could possibly help to form actions to improve cyber security. Beside of this, a look at the other possible alternative is taken to find out if it is worth of consideration in matter of subject.

These aspects were one stimulus why this thesis was written. Another one was that this work should serve an organisation’s practical purposes and aim to clarify and reduce problems faced every day – difficulties in decision making and particularly in the field of cybersecurity. Hypothesis is that friction in decision making could be greatly reduced with help of planned practices, or in other words, processes. That was the reason why the title of this thesis is “Implementing Information Management Systems as a part of business

processes”. In this thesis aim is to prove that ISMS is a “must have”, also for SMB factor companies aiming to grow successfully and that the OODA loop is an appropriate tool to help an organization to form an outlook on how ISMS should be implemented to gain the maximum benefit from renewed practices.

3.2 Structure of the thesis

Chapter 1 opens discussion about technology’s significance and its positive effect to everyday life in modern society. Chapter underlines the fact that cybersecurity is not a standalone silo but a matter that might have effect to each and every one of us.

Chapter 2. tells about significance of trust and how to maintain it. Chapter also delivers a view point of how cybersecurity’s negative effects could be mitigated and turned in to positive ones with help from skilled personnel and structured, well defined security processes. This chapter also presents division of different processes and limits the number of processes which are covered in the thesis work.

Chapter 3. introduces goals and focus of the thesis work and the motivation behind it. This chapter also introduces the structure of the thesis work and some essential concepts to delimit the issue.

In chapter 4. a look to public discussion is taken. Meaning of this is that it is important to understand why cybersecurity is important, what are the costs caused by cybercriminals worldwide and why cybersecurity’s importance should be emphasised even more.

Chapter 5. examines why possibly the best way to raise the security level, security culture, is so hard to implant in companies and to each one’s everyday life and manners. Chapter 6. explains what are the different factors to be considered while forming management structures and why the harmony is so important. The Cynefin framework and its idea from different responses to different situations is presented there.

Chapter 7. gives more detailed introduction of the OODA loop and what possibilities there are to opponent while they are trying to destabilise our structures and why open minds are important while making decisions.

Chapter 8. gives aspects of how organisations could achieve better performance and benefits with firm security in place prior conclusions and motives for further studies given in chapter 9.

In total, an effort was made to find out which approach might be the most suitable one for a SMB company while implementing ISMS and what aspects should be considered in particular. The aim for the thesis is to show the significance of a structured way of implementing security, and demonstrate that it can help SMB companies to perform better.

3.3 Method

The thesis work in Master's degree programme is determined to be carried out as improving research aiming at a practical application implemented on the basis of some new knowledge serving the needs of local businesses (JAMK University of Applied Sciences 2014).

Experiences of researcher play (naturally, would one say) an important role while carrying out research work in actual operational business environment. To reflect these experiences in prepared research, it is essential to select Experiences of researcher play (naturally, would one say) an important role while carrying out research work in actual operational business environment. To reflect these experiences in a prepared research, it is essential to select a method, approach and framework to keep the research scope in focus.

While considering thesis work topic and area it seemed obvious that action research would be such a method to suit the branch of activity where one has the need to continuously improve (security) practices based on evolving security requirements raised by business needs and customer requirements. As a thesis writer the aim is to point out that ISMS could be an important tool while developing communication and sustain co-operations in and between groups (Strategic, tactical and operational level, see Figure 9 Roles in information security domain), selecting action research seemed appropriate. One of the primary motivational drivers for Kurt Lewin, the father of action research, was to find out how to develop those (Adelman 1993, 7).

As the selected research topic is closely related to a phenomenon which is considerably large, polymorphic and has many variations and angles, the selected approach should take these into account as much as possible and still leave room for further development and interpretation. Also, the dynamic nature of decision making process in companies under research should be taken into consideration, as flexibility is recognized to be one of the most valued key factors to be distinguished. The problem here was that to keep the thesis work in reasonable length and width, the writer should find such a view-point which could take the previous into account while at same time limiting the scope of the thesis to essentials only. After careful consideration and comparisons as described later, OODA loop was discovered to be the choice to meet the given criteria.

Hermeneutic approach was used for orientation, meaning that understanding and interpretation of related phenomena is made by comparing the evolving situation and progress to trends and progress of information security trends elsewhere in the surrounding society. In practice, the mentioned progress and trends are common awareness of information security needs, customer requirements, public trends and changes in regulations.

3.4 Framework – Why selecting OODA loop?

Based on previous it felt natural to select such an approach that is developed for operational needs demanding a fast response in multicultural environment and emphasizing continuous improvement. Even though co-operation between people is more or less fluent and includes a great deal of self-organizing possibilities as is, it still has a considerable amount of different variations and alterations, which creates disadvantages while compared to actions performed in a structured way. As said by Tuomo Takala, “All organizational theories and studies so far have, at least in some level, emphasized that co-operation of people requires some sort of structure as a frame” (Takala 1999, 161). I cannot argue, conversely I see similar needs to create structures to make systematic approach possible while aiming for better results can be observed. The author’s opinion is that model of OODA loop could answer all of these requirement given in this and previous chapters. Although it looks simple at first glance, it has many dimensions

which take in to consideration numerous variations. Like Hammond say, life itself could be described in a simplified way as double helix of DNA. OODA loop represents similar ultimate abstraction that will not take into consideration its nearly limitless variations. OODA loop is full of possibilities, and nearly infinite in its variety, even if it is simple, it is yet comprehensive and elegant. (Hammond 2004, 188-189).

Of course, as Osinga put it into words; "*there is no single, all-embracing formula explaining, describing and predicting strategy and its outcome*" (Osinga 2006, 11). From a writer's perspective, OODA loop and related insights could help the emergence of an evolving, open ended process to provide a conceptual base for security system implementation. An important factor to select OODA loop as framework was its emphasis of human significance, and it aligns with the writer's interests. With the help of OODA loop as framework, information security's operational level could be organized by actors themselves and in such a way that respects natural selection to gain maximum effectivity.

OODA loop gives more responsibility for decisions and acts to where it matters most; the actual operator. Positive effects are that each operator gets familiar with systems and relations between them, which raises knowledge of those to a higher level. When knowledge is higher, operators could better contribute to those developments. This way commitment and responsibilities are increasing while process quality improves. By recognizing the power of people, an organization could unleash their potential and benefit from it by using its resources in an optimal and more effective way. In Boyd's thinking this is called "organic design" (Boyd 1987).

3.5 Characteristics of the target organization

This research was written with a certain target audience in mind. As mentioned earlier in the introduction, one of the motivational issues for the author was to unveil the need to ISMS in small and medium sized companies, and to be more specific, especially such where business is closely related to information systems, e.g. software vendors and outsourcing partners.

One possible way is to define SMB companies based on their amount of employees. For example Gartner has defined small company as such which have less than a 100 employees and medium-sized company as such with over a hundred but less than a thousand employees (Gartner, Inc. 2016). The assumption is that the pressure to form a more structured way to manage business is growing as companies grow. Most probably, the very smallest companies do not have strict policies for security in place if compared to medium and large scale companies (Prior Konsultointi Oy 2016). The author also assumes that need for standardization is growing rapidly from companies with 50 employees and up. The steps aiming for proven maturity are (and should) be taken around at the same time as the line between small and medium breaks up.

Therefore, the fictional target organization in this thesis is having more than a 100 employees in it. Since most of the authors experience originates from information technology branch, and challenges of that industry are hence familiar, the target organization will act in same line of business as well.

Often SMBs are led by entrepreneurs, same persons that have established them, and so is the case with the target organization. Growth so far has been organic, therefore, the whole firm share the same mental attitude that has been encouraged by the owner himself. One of the top priorities in the company is that technical controls are on appropriately high level and the company is aiming at constantly better results. Currently it seems that technical controls only do not provide added value anymore so that the company could grow as expected and thus the company has to look for new ways to make succeed.

The organization’s current hierarchy is low in order to reduce organizational friction and to maintain agility. On the other hand, the formal structures are immature and management is largely based on each manager’s personal abilities, not on a common shared vision. The performance of the company comes from leadership and responsibility of single persons, and it could not be counted as management’s merit.

During the years the company has created some formal structures to fulfil customer requirements, and the performing processes are on appropriate,

good level. These processes are described, documented and maintained on a regular basis, and their quality has been recognized in vendor and customer audits. So far the company has been able to gain good results, however, lately the situation has changed due to growing numbers of requirements demanding a recognized management system. This means that in order to grow and succeed, the company has to fulfil stricter requirements given by a growing numbers of larger customers. The question is how to hold onto the virtues of agile family business and at same time respond to market demands.

Especially in small and medium sized companies cybersecurity has been the task of few technically oriented persons and security management has been more or less neglected. In a research made for The Federation of Finnish Enterprises and Finnish tele operator Elisa during the autumn 2015, only 6% of respondents thought that information security is among major problems for their business, less than a half named a responsible person for information security in company and only 25% had written an information security guidance or a plan. (Prior Konsultointi Oy 2016, 22). Here the target organization is an exception, as they have recognized the need for a better management system for information security.

To improve their position on the market, the company management has decided to start preparations towards ISO27001 certificate as their goal. The question is how to get there as efficiently as possible, and what is needed before the aim is achievable.

4 Viewpoint's to discussion around information security

Public could read fresh news about different security related issues daily. Current discussion around cybersecurity is vivid and different aspects to matters could be observed from discussions. Somewhat dominant feature in the discussion is that the experts do the talking and great audience seem to be a bit confused on what is actually happening.

4.1 Am I safe?

The question how to protect oneself from different kind of unwanted intelligence and cybercrime has risen to one of the daily themes in publicity during the past few years. This question has been presented depending on which sector the questioner acts or in which position she/he is. There is no matter if you are working in the public sector, in private business or in the third sector, they all are compromised and suffer from cybercriminal actions. According to World Economic Forum Insight Report, "*Businesses in all industries and of all sizes have been affected by the increased complexity, novelty and persistence of cyber-attacks, with consequences ranging from the reputational to economic and legal. A sharp increase in high-profile cases in 2014 has continued into 2015, and shows no sign of slowing dow*n" (World Economic Forum 2016, 82).

For example, the third sector charities could be thought as such a domain that will not interest criminals. Unfortunately, criminals do not leave charities alone, instead they are used to alluring persons to donate money to criminals themselves (Grossman 2014). While news headlines concerning cybersecurity are heard of more frequently, this hot topic has made the common public worry more about their security and privacy in this modern day interconnected, data centric and ubiquitous world.

Even though the rise of awareness has been going on for years, one remarkable milestone in public awakening have been the vast revelations made by Edward Snowden during early summer 2013 to The Guardian newspaper "*as a matter of principle*" (Greenwald 2013).

Snowden exposed that U.S. National Security Agency's (NSA) information collection with its partners has been even more extensive than thought and "*The government has granted itself power it is not entitled to. There is no public oversight. The result is people like myself have the latitude to go further than they are allowed to*". (Greenwald 2013).

Whistleblower's comments have caused a situation where the public awareness of legal and illegal data collection and cybersecurity is constantly rising. This awareness boost could mostly be considered as a positive matter,

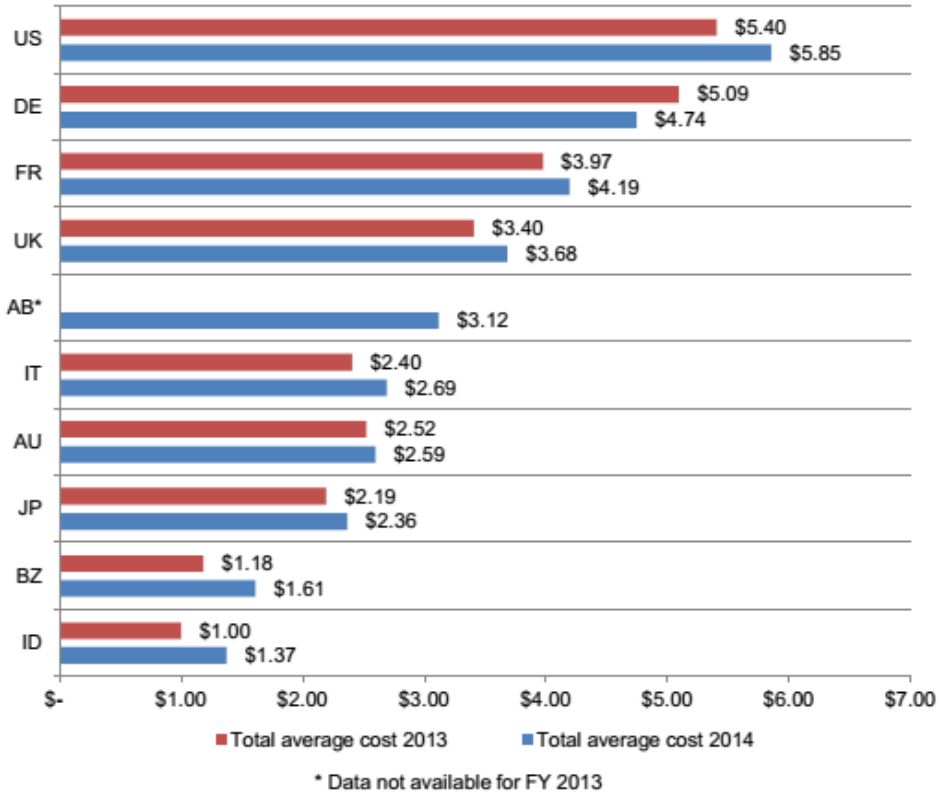
while on the other hand, it gives possibilities to “snake-oil” merchants using media hype to sell such countermeasures which do not have desirable - if any - effect on customer’s true information security.

This thesis work shows why cybercrime and security have risen onto the top of the table, a glimpse is taken of what estimated costs are caused from cybercrime worldwide and what challenges are related to its research. Based on the previous the writer intends to show what administrational controls might be the most effective ones and what kind of actual benefits could be achieved in business if those are taken into everyday use.

4.2 Cost and value of cybercriminal activities

In light of “2013 Cost of Cyber Crime Studies: Global Analysis” made by Ponemon Institute, customer demands seem to be more than justified. For example, the average annualized cybercrime related costs in the participating organizations increased within one year (from 2012 to 2013) as much as by 30 per cent (Ponemon Institute LLC 2013, 2). This trend seems to be continuous, while Ponemon institute’s May 2014 benchmark study shows still growing numbers. According to the research, the average total cost of a data breach among the participating companies increased by 15 percent when compared to previous benchmark (Ponemon Institute LCC 2014, 2). Even the latest study available so far shows an increase in costs caused by data breaches (Ponemon Institute LLC 2015, 2).

Table 1 Average total organizational cost of data breach over two years (Ponemon Institute LCC 2014, 6)



The Center for Strategic and International Studies estimated in their report that "*the likely annual cost to the global economy from cybercrime is more than $400 billion*" (CSIS 2014, 2). Also, the British insurance company Lloyds estimated in 2015 that the cost of cyber-attacks to businesses is over $400 billion annually, including direct damages plus post-attack disruptions to the normal business. At same time, other estimates claim current annual losses to be over $500 billion, while Juniper research predicts that total (business & private) losses will gain due to rapid digitalization amount of $2.1 trillion until 2019. (Morgan , Bank of America's Unlimited Cybersecurity Budget Sums Up Spending Plans In A War Against Hackers 2016).

According to European Commission (EC), the value of the cybercriminal economy is not precisely known yet, however, the losses are estimated to be billions of euros per each year (European Commission 2013). Even though precise numbers are unclear, EC estimated in 2012 that victims lose around $388 billion worldwide as a result of cybercrime. According to EC Communication, this makes cybercrime more profitable than the global drug

trade of marihuana, heroin and cocaine combined (European Commission 2012, 2).

As companies currently tend to suffer cybercrimes more and more each year, what is the situation with the common internet user, or so to say “online adult”? According to 2013 Norton Report, it looks like the rising trend has turned down lately. Even though the number of cybercrime related costs is still slightly growing due to higher cost caused to each victim, the number of actual persons that have experience of cybercrime (online adults) is decreasing according to this research. (Symantec Corporation 2013, 8). Unfortunately, this possible consequence of Snowden leaks and the higher level of awareness seem to be only temporary and latter studies show that overall counts are on the rise again (Symantec Corporation 2015, 16).

One striking issue is that while the fight against traditional crime, like drug trade, lies mainly on shoulders of official authorities’, actions against cybercrime might be considered more as everyman’s responsibility. This has raised a kind of tempest in a teapot, because the public often seem to think that cybercrime and precaution against it is not their responsibility. If looking from traditional way this makes sense, because traditional crime often not have direct and immediate implications to common citizen’s life. Further law enforcement actions, such as securing public environment and traffic controls are, in this sense, “outsourced” to authorities.

It is good to bear in mind that some precautions are needed dependent on the context or in other words, despite the context being physical or digital. Cases like locking the doors, keeping keys in a secure place, having burglar alarms etc. are considered as common sense and normal everyday actions in the physical world. In cyber-world common sense means, despite its technical and somewhat more complicated nature, firewalls and strong passwords stored in a safe place, for example.

Here is good to notice that when talking about person(s) behaviour, it is irrational and usually discipline dependent multidimensional concept that is dependent on context and also varies with a person’s life experiences (Xu, et al. 2008). In short, if the threat is not in a tangible and concrete form, it is easily perceived as something that is not in my responsibility. The public seem

to forget that cybercrime, just like traditional crimes, might have a deep, direct and immediate influence on their everyday life. The consequences could affect anyone, even those not in possession of a computer.

4.3 Challenges of data gathering

As could be assumed based on the previous chapter's EC statement, it seems that gathering data from costs of cybercrime economy is a demanding task. Due to cybercrimes' outcast and international nature collecting reliable statistics is challenging. In Finland there were no statistics from cybercrime costs however, there is no reason to doubt that matters would differ remarkably from the rest of the world. In their report made for European Commission, Neil Robinson et. al reflect why cybercrime is so hard to measure and why cybercrimes are often not reported to authorities. In their work they state that "*Members of the public do not report cybercrimes to the police or other national authorities*" (Robinson 2012, 44). The reason for this kind of unconcerned behaviour is assumed to be an outcome of several issues. For example, cybercriminals make scams which are intended against a large number of individuals, however, the losses for each individual remain relatively small. Businesses might be unwilling to report as it may affect their share value or cause other reputational damage. According to CSIS, most cybercrime incidents go unreported (CSIS 2014, 4).

Also it is mentioned that cybercrimes are international, while law enforcement is mostly national. That for national laws have very limited authority to cybercriminals. Indeed the draft report of the United Nations recognized "*the impact of fragmentation at international level and diversity of national cybercrime laws on international cooperation*" as one of the key findings and concern issues of their study (United Nations 2013, 13) while excogitating loopholes of international laws.

In addition, it would be justified to say that citizens and companies are not familiar in ways to handle and report cybercrimes. Also, they might not see any sense to report security incidents to the authorities because of the lack of benefits in practice, instead they are willing to keep losses for themselves to keep up a good reputation.

Besides not reporting on cases, the lack of true statistical surveys is recognized in Microsoft Research paper “Sex, Lies and Cyber-crime Surveys”. The paper states that surveys made are heavily focused and present a very dense population, which means that a representative sampling of the population does not match with the representative sampling of the losses. The second matter that makes scientific research harder is that results are often built on inaccurate and unconfirmed data given to researchers by victims themselves (Florêncio and Herley 2011, 3) or as CSIS researchers state in their report: “*The lack of data means that any dollar amount for the global cost of cybercrime is an estimate based on incomplete data*” (CSIS 2014, 5).

To sum up previous, it should be clear that cost estimation is not an easy task to complete or at least it is not very accurate and the results are somewhat staggering. Despite of this lack of accuracy, the estimates are still remarkably similar, and the scale currently is from $375 to $575 billion (CSIS 2014, 2). Based on this enormous sum, it should be clear to anyone that cybercrime should be concerned seriously and controls should be given to fight against it in such a value they are entitled to. Most probably one of the best ways to improve accuracy of cybercrime reporting is to form a strong security culture for companies and manage it with best practices. In other words, this means ISMS.

4.4 Cybersecurity in public sector

Public sector has reacted to cyber threats on several levels. European Commission presented 2012 a Communication on a European Cybercrime Centre to be established within Europol (European Commission 2012, 4). The Centre, which started its operations in January 2013, supposed to act as the focal point in the fight against cybercrime in the European Union (European Commission 2013). Separate union member countries have also published cyber strategies of their own, like Finland did in January 2013 (Secretariat of the Security Committee 2013).

The rise of public awareness has put the whole scale of companies in a situation where they have to have some kind of security program to satisfy customers’ growing knowledge and demand. Currently it is simple as that:

Show that you have security measures in order or we will not deal with you. From information security's perspective demand and justified, rightful requirements are absolutely a positive matter. At least this is true as far it shows a true concern about the total security of their business and it is understood, that requirements have influence on production costs.

If demand is only an attempt to outsource the responsibility for security, requirements could also be seen partly as a negative matter. It is good to bear in mind that responsibility for security is something which cannot be outsourced, because responsibility *always and without exceptions* stays with the owner. Even if responsibility from security could not be outsourced, different ICT vendors are part and have a remarkable effect on customer's security as a whole and for that purpose it is crucial for their business to take care of security on their side. On the other hand, outsourcing might be a good idea if outsourcing is considered carefully and only such portions of the whole are outsourced which could not be covered by your own and that way adding to the total sum of security. Currently, in real life it seems that outsourcers are simply covering their own backs and add security phrases in their request for quotations, however, at same time have forgotten to take care of their own nest on a deeper level. This, of course, adds to business possibilities for reasonably achievable security services.

4.5 Difference on talks and admitted resources

While management and leaders all around the world at least partially recognize the importance of cybersecurity and pledge themselves to commitment, actions to increase resources are in practice very limited in most countries and businesses. Catharina Candolin, Section Chief of the Cyber Defense Section in Finnish Defense Forces, put measures in scale in her interview held at July 2nd 2014 in Mikkeli Päämaja Symposium: "*If we're looking at National Cyber Security Centre Finland, which got one million euros to its operations and at same time City of Helsinki is using more for repelling rabbits, so there is a small drawback*" (Candolin 2014). Even though this is most probably exaggerated by generalising, in January 2013 the Finnish government stated in Finland's Cyber security Strategy that "*by 2016 Finland will be a global forerunner in cyber threat preparedness and managing the*

disturbances caused by these threats" (Secretariat of the Security Committee 2013, 3). According to Limnéll's report written in early 2016, none of the Finnish members of parliament (MP) ranked the current level of being forerunner higher than 7 while the scale was from 1 to 9. The average of the grades was 4.69, which could be count relatively low compared to the very ambitious plan. (Limnéll 2016, 9).

Comparing the amounts of resources used and the aims which should be achieved in quite a limited period of time, there is a certain gap between those which tells about the lack of true commitment. For comparison, the United Kingdom House of Commons report stated that U.K Ministry of Defense (MoD) has spent £650 million for National Cyber Security Programme (NCSP) in its first year. Coordination, trend analysis and incident management / response alone cost £9 million. (House of Commons Defence Committee 2013, 38-39).

4.6 Cybersecurity resources on private sector

If this is the situation in the public sector, how are matters then in private businesses? It would be expected that due to to increasing consciousness and regulation, investments for security should be growing. The increasing regulation is actually thought as one of the major drivers for private sector to avoid underinvestment, which researchers see as a challenge (Gordon, et al. 2015, 3-4).

Implementing robust security might seem costly and difficult from a company's management point of view, and in most cases costs are not justified by risk calculations. Security is often considered as loss management instead of a profitable business (ENISA 2012, 2), or even an unnecessary expenditure if looking at it purely from financial perspective. Matters get even worse when security and business management do not understand security related terms in the same way. For these reasons, it is unlikely that an organization will succeed in moving from ROI-based thinking to more security culture driven approach. ((ISC)² 2009, 7). But there might be an alternative point of view for this for the management to consider. Instead of a cost factor, management

should achieve such a mind-set that security and ethics are essential virtues while pursuing profitable business (Culnan and Clark Williams 2009, 685).

Also, investing voluntarily to security might give better a feedback and good will from the buying audience than acting forced by legislation. Companies should somehow develop organizational preparedness (both technical and management) in order to reduce business impacts of possible future cybersecurity incidents (ICC 2015, 11). At the same time, it might be reasonable to take advantage of these measures already in advance by taking those as a part of companies' sales pitches for example. Direct marketing is not meant here, as it might cause an opposite effect as planned but to emphasize quality and security of one's offerings.

The problem seems to be such that while direct or budgetary costs are recognized, possible costs caused from cybercriminal activities are not recognized, which is followed by the fact that many companies do not even know if they are compromised nor what the costs caused by a possible scenario would be.

Below is an illustration from Ponemon Institute's "Cost framework for cybercrime" where the Institute's researchers have tried to find out the actual experiences and consequences of cyber-attacks. Based on research made, they have divided costs into two "streams": internal cost activities and external consequences and costs. This division might help with creating cost estimates for next budgetary negotiations by clearing the concept between *actual costs* (Internal cost activity centres) and *possible costs* caused by external an evil doer (External consequences and costs). Here it might be righteous to ask if all internal costs should be put on top of cybercrime, as part of the controls should be available anyway to protect customer's information and divide their systems from each other as required by legislation. Car keys or door locks would not be considered as assets against crime although they are such from a certain aspect. One's opinion is that they should, since they have a certain lifespan and they must be maintained and replaced on a regular basis and they are causing constant costs due to to this.

More complex is the question on how external consequences and costs could be estimated. Certainly it is not easy, however, based on a statistical survey

and research it is doable. Even then, from SMB company's point of view, it might look far too complicated and painstaking. The thesis can offer no good advice on that, but it could be tired through risk management and estimations - Once again a matter covered by ISMS.

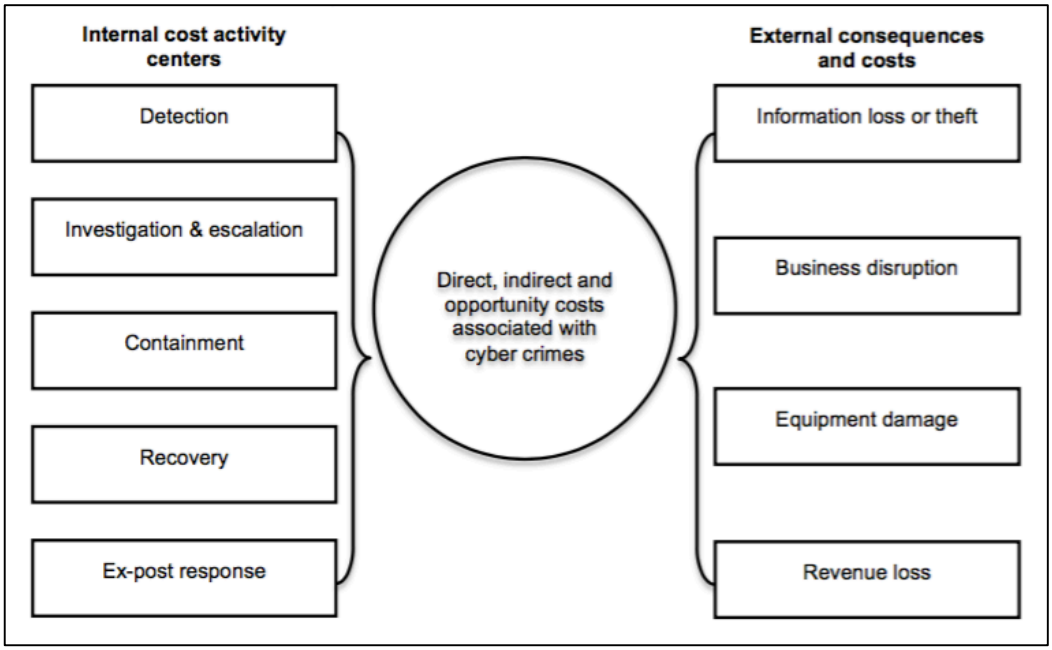


Figure 2 Cost framework for cybercrime according The Ponemon Group (Ponemon Institute LLC 2015, 22).

4.7 Security providers and consumers

For *security providers* increasing consciousness and regulation can mean a kind of a honey pot while business opportunities are obviously growing. Some sources anticipate that the current global cybersecurity market worth of $75 billion is expected to reach $175 billion by a five-year timeframe, which means over $100 billion on new spending on cybersecurity products and services over the next coming years (Morgan, Cybersecurity Market Reaches $75 Billion in 2015 2015).

From another perspective this means increasing challenges, while *consumers of security* still have to find a balance between regulations, amorphous security threats, uncertain benefits and demands of profitable business like described by The Wall Street Journal (Yadron 2014). While demands are increasing and there is a growing pressure against IT budgets, it could be thought that companies would gladly outsource their IT systems and at same

time, parts of their cybersecurity. In this way they might have the benefit from a stronger, better managed IT environment with less costs, which sounds like a good bargain; however, once again the reality hits back. According to Keppel, based on ISG's 2014 research, the trend seems to be such that outsourcing is actually increasing, however, the size of contracts is smaller than earlier (Keppel 2014). The latest reports show that this trend continues (Information Services Group 2016).

From the information security aspect this could be interpreted in (at least) few different ways: firstly, smaller companies with limited resources for IT security, outsource to achieve such security level which their customers are demanding, which definitely would be positive. On the other hand, it might be possible that larger companies have outsourced their activities to such parties operating with less money, however, not necessarily according to best practices and standards. This budgetary approach is of course understandable, however, not the way how it should be, and in order to manage that a strong security culture must be available from both parties (outsourcer and vendor). The third and the most probable explanation is that companies divide outsourcing into larger amount of companies, which causes challenges for provider management and puts pressure against security structures and culture. This way demands even more strict policies and procedures to be successful.

4.8 Best policies for outsourcing security

In any case, security is something that is difficult, if not impossible, to outsource. According to expert advices and best practices, when outsourcing security, one should keep a calm head while considering possible benefits and defects and keep security management always in one's own hands (Schneier 2002). Otherwise managing security and its process could be turn into "mission impossible". By holding security management domain in one's own hands, more technical tasks could be outsourced successfully. (Jirasek 2012).

Even if outsourcing security functions, the responsibility always stays with the outsourcer. Hosting providers do have certain responsibilities, however, the liability of hosting providers is limited by law as far as the hosting provider has

no actual knowledge of illegal activities or illegal content stored in its servers. It is also good to know that the hosting provider does not have general obligation to monitor the information which they transmit or store according to European Union (EU) directives (Gercke 2012, 285-286). So it is the writer's recommendation to strictly hold on to security management and put requirements to vendors according to one's own policies. This might not be the cheapest alternative short term, however, while considering it in a longer run, it most probably is the only right one. Also, it should be remembered that remarkable service providers do have security measures in place and they do have verified indicators, like 3rd party certifications available.

5 Raising level of common understanding

First thing to achieve apprehension from how to raise a level of understanding, is to realize why the cybersecurity is somehow overlooked even its significance is publicly admitted. In following chapters this contradiction is slightly opened.

5.1 Why is information security is being overlooked?

Even though a namely commitment to information security exists, people still act carelessly dependent on their working position. Some issues that could encourage unwanted behaviour are e.g. limitless usage of company equipment at home and employee-owned devices at work. A possibility to extend working outside of office hours with usage of company ICT equipment might sound charming from both the employer's and employee's point of view. It also seems that it blurs the line between private and working life, at least what comes to devices. Using work devices at home is one matter which lowers security awareness and possibly creates negligence behaviour. On the other hand, Bring Your Own Device (BYOD) culture is doing the very same thing, however, in the opposite way by allowing the usage of personal devices at work. According to Colwill, a growing numbers of IT workforce is willing to have "*a greater freedom to use the IT applications and devices of their choice in order to communicate and conduct their work more effectively*". Colwill also states that when the millennial generation to whom digital devices are an

essential part of their everyday life get into working life will challenge the established modes of IT and with it security management in organizations. (Colwill 2009, 4).

No doubt this kind of “mixed use” has come here to stay, however, it is causing at least grey hairs to CISO’s while they are trying to find a cure to make the dynamic usage of equipment possible both at home and work and also secures company information with an arguable cost.

This point of view and need for strong security culture get support from Mariam Merrit’s saying, that “*lots of working folks have blurred the lines between the office and home when it comes to using their devices (reflecting the whole BYOD to work conundrum) and storing their personal and work information*” (Merrit 2013).

As it could be observed from several studies and reports, one of the most remarkable ways to secure critical infrastructure and functions is a company’s own, strong built-in security culture supported by constant training. To establish such a culture, creating company’s Security Policy and Information Security Management System have essential roles, while they are the basis for systematic actions and continuous improvement. The significance of those with spices from previous experiences are vital for creating what is considered as culture. Late USAF colonel John R. Boyd put that in words according to Astrachan et al. as follows: “*Without our genetic heritage, cultural traditions, and previous experiences, we do not possess an implicit repertoire of psychophysical skills shaped by environments and changes that have been previously experienced*” (Astrachan, et al. 2012, 552). In cybersecurity context this means that to prepare unexpected, there is a constant need for education and training, and to learn lessons from exercises and apply those to the practice.

5.2 The best way to secure information services

It has been examined that having a strong security posture, the incident response plan in order and proper CISO appointment have reduced the costs caused by cybercrime (Ponemon Institute LCC 2014, 3). Besides reducing of the costs, response plans and strong commitment to security could serve both

companies and society's resilience, including preparedness to adversities. The researchers at the Finnish Institute of International Affairs have put this into words (while talking about hybrid warfare) in the following way: "*Hybrid warfare is difficult to prepare for, but the mental and physical resources put into preparedness would serve to strengthen society's overall resilience and capability to withstand unexpected events, whether caused by a natural disaster, a self-inflicted major catastrophe or an external state actor*" (Salonius-Pasternak and Limnéll 2015). The previous statement could be expanded for cybersecurity as well and same issues serve both matters equally.

Also, the U.S Department of Homeland Security (DHS) has reported that organizations should go on about building a more effective security culture. It has recognized that executive leadership should be engaged and the role of education and awareness should be emphasized (U.S. Department of Homeland Security 2013, 13, 21). Based on previous, it could be expected that these controls which make common sense, would be in use in each and every company. Unfortunately, the situation does not seem to be so bright in practice.

For example, ThreatTrack Security's study (ThreatTrack Security 2013) pointed out that 57% of malware analysts have reported that their companies, which are supposed to do business within cybersecurity, have never disclosed data breaches which they have investigated or addressed. This might be a clear indication of lack of commitment from the company management. The very same study revealed that devices of companies' senior management members had become infected from such reasons which could be avoided with proper advices and training, again matters which are essential parts of security culture. CompTIA's security research, published in 2013, seems to confirm this, as it stated that more than a half of the factors in security breaches involve a human element (CompTIA, Inc. 2013, 5). Previous researches' indicate that even if a company has written security policies and procedures approved by the management in place, there are still serious lacks on what comes to understanding possible losses caused by data breaches and the meaning of true commitment. That for the need for a strong security culture to correct these shortcomings is obvious.

Challenges in education and training are one main reason for incidents analysed as “human errors”. After IBM’s study (IBM Corporation 2014, 3), human errors were involved in more than 95 per cent of the security incidents investigated in year 2013. Ponemon Institutes “Cost of Data Breach Study” (Ponemon Institute LLC 2013, 19) conforms to this, and Computer Weekly’s article based on the previous, expresses that strong security postures and appointment of a CISO could significantly reduce costs caused by data breaches (Ashford 2013).

When examining the main concerns and challenges in cybersecurity, lack of know-how, unpredictability of human behaviour and different ways of acting form serious challenges. When VTT, Technical Research Centre of Finland, researched shortages of automation industry systems in Finland, the main reasons for negative effects in cybersecurity were caused by:

1 *Lack of common information security standard*
2 *External factors and pressure*
3 *Difficulties in managing long lifecycles*
4 *Challenges in education and training.* (Ahonen 2010, 18).

In common those all seem to be indications of lack or weaknesses in security management, especially challenges in training and education. These kinds of matters could be handled with a strong security posture maintained with the help of Information Security Management System (ISMS). Handling the previous tasks is recognized as a critical success factor for ISMS (SFS 2010, 21).

6 Structures for the security management

The following chapters discuss the factors to be taken into consideration while implementing security structures for a SMB company. The focus is in the OODA loop, however, also alternatives are examined which might give a deeper understanding of how to react differently in different situations, how to manage that and how to implement and maintain harmony on the different levels of an organization with the help of an ISMS.

6.1 Outside factors and pressure forming security structure

As seen, many external factors have their effect on cybersecurity. Customer requirements, regulations and laws added with morale of individuals and companies have been discussed in the previous chapters. To complicate matters even more laws could be national or international, there are many kinds of standards, which even are partially overlapping, instructions and auditing criteria which all have influence on the subject of matter. Together these form a kind of crisscross spider web which might feel aversive to persons not familiar with it. Depending on each actor's background and culture, they see issues in a different way and demand different matters from their security. So it could be said that each actor perceives reality in a different, unique way.

To achieve a more uniform approach to this, one must decide which the key functions are to focus on, and what kind of commitment they are able to make to fulfil the demands placed on it. ISMS is definitely one way to achieve this, and normally it is based on some of the different information security standards available in several institutions like ISO, BSI or IEC. Which one to choose, depends on one's needs. One key issue that should be considered is support available nationally, and which standard has the most influence on local legislation and requirements. An advantage is that even though details between different standards may vary, each one has a remarkable effect on the other ones and this compensates their differences.

In Figure 3 Outside factors and pressure to an Information security management system, the writer has tried to explain how factors that have to be considered while creating an Information Security Management System are perceived.

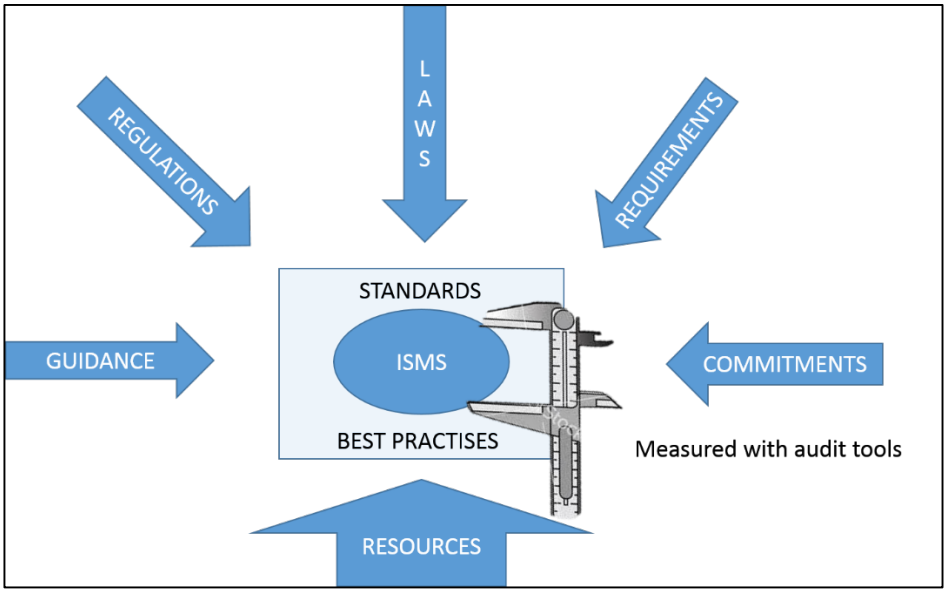


Figure 3 Outside factors and pressure to an Information security management system

The guidance to ISMS comes often from third parties like consultants, security firms and device vendors. Characteristic for these is that they often have strong opinions on how to handle matters based on their products and services, which is not necessarily a bad thing, however, it might put pressure on the decision making process when deciders have conflicting opinions about costs and the effectiveness of different controls.

Regulations and laws should be relatively easy to understand due to their obligatory nature. What makes this a challenge here is that often they are not unambiguous and instead demand interpretation from legislative experts. As they are obligatory, effort must be put to clarify these.

Requirements could come from customers or their customers. An example of these could be the requirement to fulfil certain security standards or limitations on access policy.

Commitments are promises made by provider itself to maintain or gain advantage compared to rival vendors. They could be e.g. better availability, extra physical security, clustering of the devices and the most significant one in this thesis aspect, certified information security management system.

To fulfil all these voluntary and obligatory needs, a provider should have enough resources available, which concerns both the technical and administrative personnel. Without technical personnel there is no capability to

create security on a physical levels and if lacking administrative personnel, there is no ISMS available, which in turn reduces the total security of the company and the possibility to convince customers about that. As can be seen, maintaining security structures demands balance and harmony between different factors.

6.2 Security, processes and how to improve those in harmony?

Despite of the domain, everyone working with processes knows that it is work which demands strict, systematic approach and plenty of discipline. To proceed with continuous improvement, well organized structures should be available. To achieve systematic approach to process development, matters related to a phenomenon should be closely investigated to find issues to be improved, further investigation results must be chewed into smaller pieces and decide which actions should be determined and how to the wanted results are to be concluded. Finally, the work should be grasped and plans be actualized. As could be seen from previous, processes require strict order to succeed.

Kurtz and Snowden describe aiming for strict order as follows: "*Ordered-systems thinking assumes that through the study of physical conditions, we can derive or discover general rules or hypotheses that can be empirically verified and that create a body of reliable knowledge, which can then be developed and expanded*" (Kurtz and Snowden 2003, 466). The previous describes quite comprehensively the characters of process driven development, which could be seen as an essential element of different management systems like ISMS.

Quite often different versions of Deming Wheel, like PDCA loop for example, are used to describe the idea of continuous improvement in literature. One example of those is presented in Figure 4 Reproduction of Framework for managing IT Security (The IT Service Management Forum, 2009, p. 80), where version available in ITIL V3 Foundation Handbook is reproduced by writer.

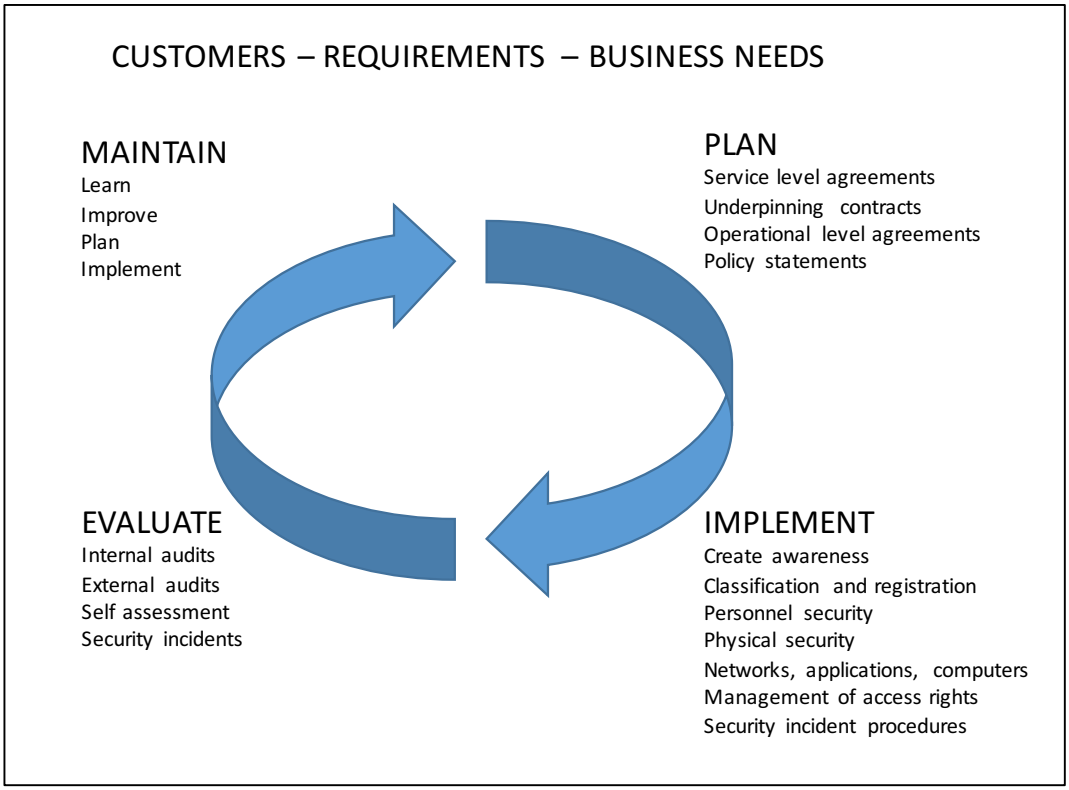


Figure 4 Reproduction of Framework for managing IT Security (The IT Service Management Forum, 2009, p. 80)

The origins of Deming Wheel and its predecessor (Shewhart Cycle) are in the teachings of the philosopher C.I Lewis who, according to Moen, set out three main ideas in his book *Mind and the World Order* to further the pragmatist's influence:

- *"a priori truth is definitive and offers criteria by means of which experience can be discriminated;*
- *the application of concepts to any particular experience is hypothetical and the choice of conceptual system meets pragmatic needs; and*
- *the susceptibility of experience to conceptual interpretation requires no particular metaphysical assumption about the conformity of experience to the mind or its categories."*

Lewis's thoughts were practical and fitted well to manufacturing. They had remarkable influence of Shewhart and later on Deming, who was the editor of Shewhart 1939 book where the first version of the continuous loop was published. The idea of the loop was to emphasize constant, ever-going nature of process development with the quality of product and service as the aim, which was achieved simply by presenting phases of the process in a loop instead of a linear form. (Moen 2009, 2-3).

For higher-level process demanding regular follow-ups and actions PDCA loop with its different applications could be appropriate. This is needed to give executive level processes a backbone to which the organization could rely on and which could further give the necessary driving force to lower level (tactical & operational level) actions. The driving force here could be understood simple as budget (money and resources) to achieve the given goals. As an example of this ISMS Year Clock is produced, once again one practical application of Deming Wheel, which is presented later in Figure 5 Example of planning level loop - Year clock for ISMS. As can be seen in the figure, the phases are logical, following each other in such an order which creates harmony and could act as a guideline for constant acts demanded by ISMS. ISMS Year Clock could definitely act as a baseline for regular actions following each other annually.

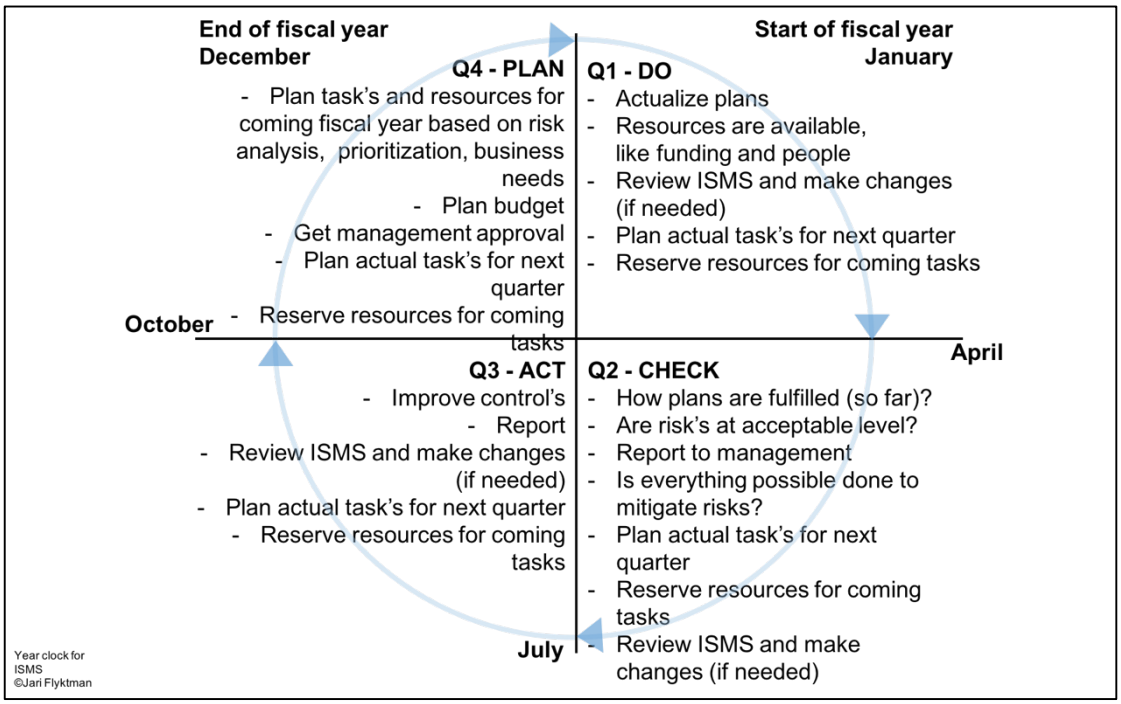


Figure 5 Example of planning level loop - Year clock for ISMS

Though practical in nature and roots tightly in practice of management, the Deming Wheel as it is does not seem to support actions demanding more possibilities for variation and changing tempo, i.e. situations where order is missing and time frame for actions is limited. Even though Deming Wheel's idea was distinctive at time when it was presented and it seem to stand the test of time well, a better way insists something more to be growingly dynamic and less bureaucratic. This is despite of the fact that PDCA loop supports

ISMS well in constant tasks and is obligatory element to fulfill standardization requirements like one's given for ISO20000 service management system (ISO 2011) and ISO27001 (Pelnekar 2011).

As any person with experience from practical tasks could easily notice, the previous example from decision loop is not very practical at all, at least if performing (operational) level is discussed. Security incidents do not come steadily in a row one after the other, nor do they respect company's planning cycle. But, as stated earlier, the ISMS year clock is a higher-level planning loop, which purpose is to guarantee the needed resources for security. With these resources the persons responsible for security could ensure that security is in line with the company's needs, e.g. business needs, or obligatory needs e.g. laws and regulations and that company's security position is constantly followed and improved. So it is important that information security is part of the planning cycle. Otherwise it might drop out of loop causing resource reduction for the next fiscal years that further decrease its ability to fulfill its tasks.

Accepting the inevitable, e.g. some sort of bureaucracy of management systems, could also be described as an adaptation for achieving harmony with a larger pattern's slower rhythm associated with the more general aim for information security and larger effort of strategic development. Shortly it could be set as cohesion within several levels of organization as described by Osinga (Osinga 2006, 156).

6.3 Maintaining harmony on performing level

When getting back to performing level, other tools to describe the process would fit to process owner needs better than PDCA loop. Life on the performing level could be hectic. Fast performing everyday work will not reduce the need for a systematic approach, even though other needs for processes might be different. For each one working in such tasks it is essential to know which are company policies for information security, what company has been committed to, what are the obligations forced by law and what has been done so far to achieve these high level goals to ensure the customers good as required (by customers) and promised (by company).

To find a proper tool to describe this process on the practical level the writer familiarized himself with OODA loop and its usage as framework for information security management system (Figure 6).

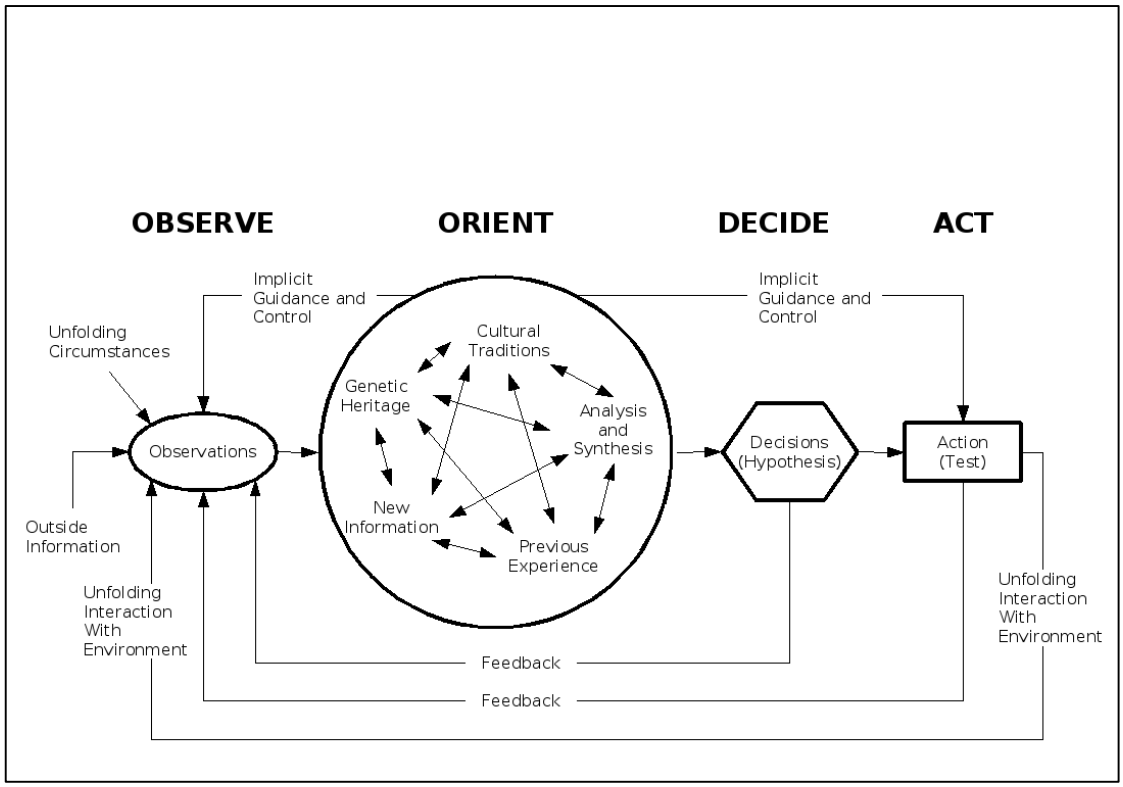


Figure 6 The OODA loop as presented in John R. Boyd's summation of "A Discourse on Winning and Losing" (Hammond 2004, 190)

At first sight, the charm of the OODA loop could be found in its simplicity and quite practical approach without bureaucracy. The more one gets familiar with it, the richer it gets and the more levels and tones could be found behind it. These, admittedly, are not easily found, however, they are there if one is willing to spend some time to get to know the loop itself, the evolution and stories behind it. On the other hand, the OODA loop does not take much into consideration on what one has to have before achieving the wanted performance, unless general level mentions in the orientation part of the loop are not considered as such. This leaves disregarded much of preliminary requirements, such as requirements for recruiting, training, personnel administration, logistics, planning and their numerous sub processes. This is noticed in the criticism against the OODA loop. (Hasik 2012, 6). If thinking about planning the cycle described Figure 5 Example of planning level loop - Year clock for ISMS and the OODA loop, the criticism seems righteous. The OODA does not take business processes into consideration, and its reactive

approach seems to fit poorly to such a long term actions as planning could be considered.

The OODA loop is an ultimate concentration of ideas and thoughts forming John R. Boyd's life work. It is synthesis, or the "Big Squeeze" as Boyd called it, of what he had studied, learned and experienced. A quite impressive effort as such, but which could be easily overlooked due to its simplicity. The idea behind the OODA loop is that properly understood the world is not as complex as one might think. Anyway, the possibilities and varieties of the process itself are numerous, some might say even close to infinity (Hammond 2004, 188 - 191).

The essence here is that one must understood the possibility of different variations, accept the existence of unexpected, leave room for reactive behaviour and get prepared for those. This is the hard core of the OODA loop and the reason why the writer sees it as charming. Understanding here means that each one knows that one's observations are made from one's own perspective and are most probably partial, i.e. they are not the whole truth. Because our observations are not the whole truth, there must be some uncertainty which we must be accept and be prepared for. Leaving space for uncertain and preparing for it means from ISMS's perspective that operators must have freedom to react in such a manner that they find appropriate in the dominant situation, however, they should not under- or overreact. By adopting this approach, one would probably gain at least some time advantage on reaction and this might save our assets from serious consequences. Of course this kind of "responsible freedom" could be achieved only by common, recognized goals and understanding – In this context this is meaning the ISMS.

6.4 Different situations – Different actions

According to contingency theory based on Takala, leaders should act and do decisions according to existing situation. Claim is that there is not a single universal model of leading, instead there are group of models for leading which are tightly dependent of prevalent situation (Takala 1999, 123). Possible approach to manage knowledge and courage responsible for creative thinking

in different, constantly changing and evolving situations is The Cynefin framework.

Cynefin is developed by welsh Dave Snowden and his team "*to help people make sense of the complexities made visible by the relaxation of these assumptions*" (Kurtz and Snowden 2003, 462).

The framework provides a classification of five contexts (domains) and it is trying to show what sort of different solutions and management styles might probably apply best in different situations. Basic message in the framework is that you should lead, think and analyse differently in different situations.

The currently presented domains are:

- Obvious
- Complicated
- Complex
- Chaotic
- Disorder.

And in following chapters the author will try to explain what are the characters of those and how do they adopt to cybersecurity field.

6.4.1 Obvious

In the Obvious domain relationship between cause and effect is clear and obvious to all. The approach is to Sense - Categorize - Respond and we can apply best practice even by pre-defined process. Basically obvious situations are such to which we could find right approach relatively easily without high degree of expertize. In the information security field, for example, reactions to known threats could be such and actions to these threats could be automatized. Good example of automatization could be different anti-virus programs which react to known threats without operator's influence.

This is also the domain where support from structured system like ISMS is highest. Pitfall here is that classification might be wrong as information is condensed too much and something obvious is left without attention. This could also be thought caused by over simplification and it might be easily led to domain lying next to the Obvious – Chaos.

Even training and previous experience often help in reacting, they could also reinforce certain, familiar reactions by leading thoughts to same track that have proved to be successful earlier. There is saying by Abraham H. Maslow "*I suppose it is tempting, if the only tool you have is a hammer, to treat everything as is it were a nail*" which describes possible problem quite well. In other words, this means that our focus is significantly narrowed by the limits of what we already know or think we know. That for CISO should stay away with certain distance from operational actions and watch over the general view and sense possible changes on it. (Snowden and Boone, A Leader's Framework for Decision Making 2007).

6.4.2 Complicated

In complicated domain the relationship between cause and effect requires analysis and at least some expert knowledge. The Complicated domain is domain of experts, persons which know unknown and can investigate several possible options, also in team. Danger (also) here is that focus is too tight and concentrating on too specialized insights causing lack of understanding of phenomenon's actual nature. In complicated situations the approach is to Sense - Analyse - Respond and we can apply a good practice. Like in the Obvious domain, structured system gives good rest for actions to be fulfilled here also. From information security point of view, new threats like rapidly changing ransom wares or targeted threats like APT's, could belong to complicated domain. In this approach threat must be analysed and find out its typical features. After finding these it could be tackled with known or relatively easily developed countermeasures. Those could be, in this context, for example heuristic anti-virus program or IDS /IPS rules. After developed countermeasures are taken into use and are discovered successful, threat could be moved from the Complicated to the Obvious domain.

6.4.3 Complex

Complex domain is one in which the relationship between cause and effect cannot be noticed in beforehand, but it could be found afterwards. It's realm of "*unknown unknowns*". In Harvard Business Review article Snowden and Boone compare the Complex domain to rainforest, which is constantly

changing (Snowden and Boone, A Leader's Framework for Decision Making 2007). Here the recommended approach to situation is to Probe - Sense - Respond and we can sense emergent practice. Here sensing is the important and interesting part and it is kind of approach which could be compared to "*fingerspitzengefühl*" (fingertip-feeling in German) emphasized by Boyd (Hammond 2004, 6, 160). In the field of information security this kind of threat could be kind of unknown threat including multiple contaminated payloads inside of each other trying to lead defender on wrong tracks by exposing one, but hiding others. Here the problem is that you do not actually know what control might work. Complex domain demands more experiment, which reduce effectiveness and might raise risks. You must probe, then sense if that is the right solution, test solution, possibly try again and finally act. If all necessary acts are not done, situation can be turned into chaotic, but anyway situation is in disorder from defender's aspect, because they do not know where they actually are. Once again, when typical characters of new threat(s) are found out, they could be moved to complicated or even obvious domain. One observation that was made is that these phases have remarkably similarities with OODA loop phases which supports the theory that OODA loops suits well in complex situations without order in place.

6.4.4 Chaotic

Already a name give hint from the nature of fourth domain in the Cynefin framework. In Chaotic domain there is no relationship between cause and effect at systems level, and that for it is the hardest domain to find appropriate way to react. It is the domain of unknowable's. This is because you do not even know what you are dealing with, because there is no clear evidence to which one should react on. Chaotic situations demands act to establish order before you even know if they are actually working. The Cynefin frameworks recommended approach to chaotic situations is to Act - Sense - Respond and eventually one's can discover a novel practice. In the cybersecurity domain this could be basically anything unknown causing serious harm. An example could be such that you're driving a car, while somebody other takes control over it. You cannot throttle, brake and even capability to steer is lost. You just have to act to survive and do measures of which influence you do not have

any actual evidence prior trying one. When symptoms are known, cure could be found and attack vectors could be blocked. Afterwards the threat can be moved to other domain. Interesting from cybersecurity's point of view is that this is the domain where skilled opponents are willing to hit. When thinking the features of chaos, it is seldom caused by only one event. Instead typical for chaos is that several events happen in same time or within narrow timeframe, depending or dependent of each other. Purpose for the chaos might be to cover other actions at same time by bringing opposites attention and resources to managing chaos. In cybersecurity chaos could be delivered by Zero Day –attacks, for example.

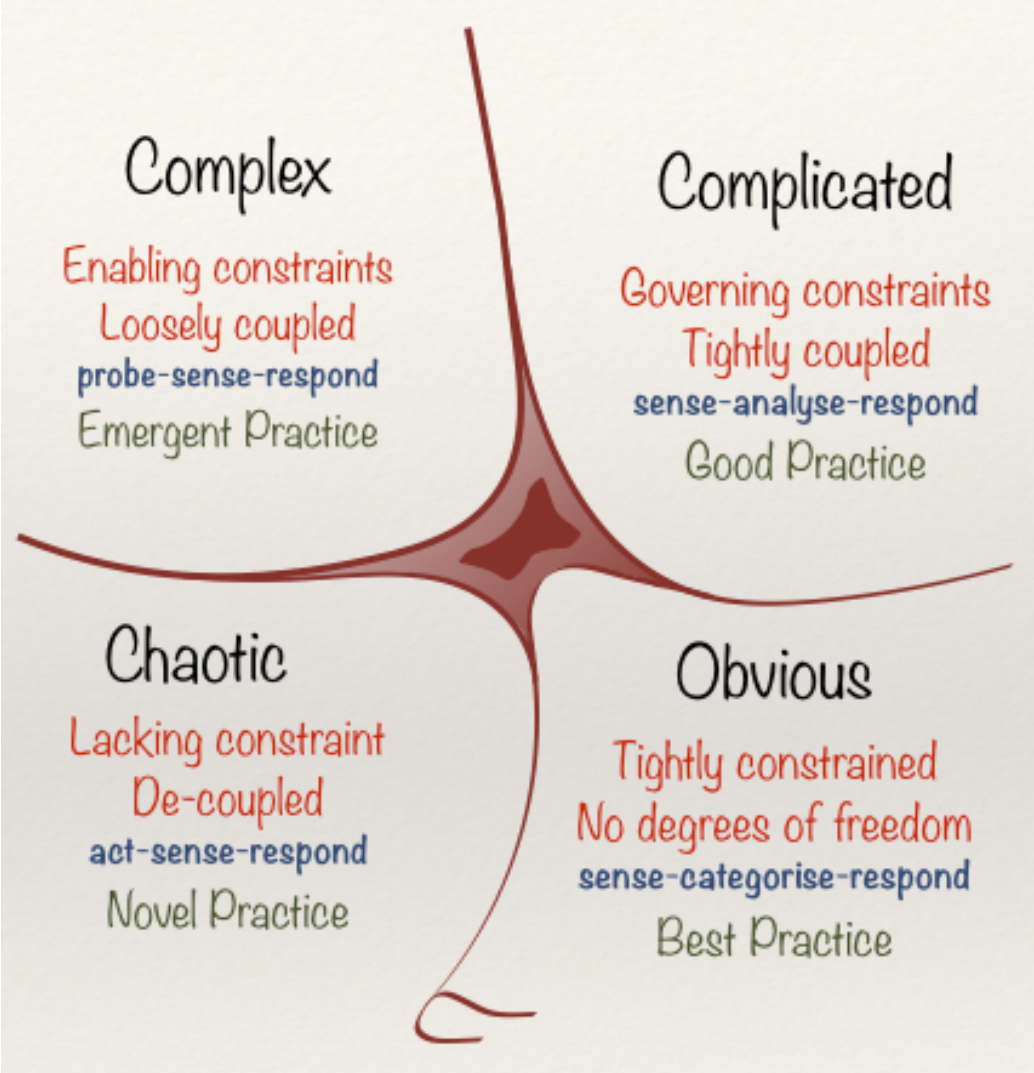


Figure 7 Five domains of the Cynefin framework
(Snowden, Cynefin as of 1st June 2014 2014)

6.4.5 Disorder

The fifth domain of Cynefin model is Disorder, rust brown area without explanatory text in the middle of the picture. Disorder is the state of not knowing what is actually happening and what to do next. In Disorder domain you do not (yet) even know of which four previous domains you are in and do not know appropriate way to react. Disorder is the domain, which is out of your comfort zone. You are unprepared and do not know if any type of causality exists between act and consciences. The Disorder domain could also be described with word indecisive, state where no planned or unplanned reaction has not yet take place. Time spended in this domain should be as short as possible to prevent opponent's possibilities to take over and to reduce damages done.

Boundaries between domains are thin and the line between obvious and chaotic could be seen as line between order and disaster: For example, you think that you know what you're dealing with, react as expected to do, but actually you do not understand what is actually happening and you will eventually fail. It's kind of ambush situation where one gets due thinking that in current situation all is right and obvious, no suspicion exists. To put it short: Complacency leads to failure.

Lessons from this chapter based on David Snowden's et. al work, are that management style should change after changing situations and that leaders, like CISO, should not get fixed to certain aspect, but consider case as whole with larger scope. Interesting, and the reason why this chapter exists here, are commonalities between Cynefin framework and OODA loop, specially in the orientation phase.

6.5 Power of processes

Even otherwise could be sensed from previous chapter, processes are good to have. It just has to be realized that processes are not answer to everything, especially what comes to sudden situations like one's in the Chaotic and Disorder domains in the Cynefin framework. Instead processes do fit well in such actions which should be done repeatedly time after time, like in domains

Obvious and Complicated. Here achieving common understanding meaning of the ISMS is important, because it creates frame for “operational handbook”. Operational handbook could be thought to be a set of standard operating procedures (SOP), standards of actions which should be followed and procedures which should be taken care of. To have these procedures in place, the organization can gain higher standardized level of trust and respect from the executive level and customers. Without standards you are not capable to show that you have prepared and are a trustworthy actor. Receiving trust and respect might sound a bit naïve, but those are needed to get resources for information security, which is further needed to make business. Respect and trust are not achieved if your value is somehow vague, is not recognized or is impossible to show off. As unscrupulous it sounds, everyone, even tasks and processes, should show their necessity time to time to earn right to live and evolve and that is done via processes capable to measure.

Right, that is clear then? Actually this is not the case. Previous might be true while considering it from executive level perspective, but performing level still has lack of time and no one there is not actually interested of dusty paper taste policies that do not meet the real life as it actually is. This for sure is true from operative level perspective. Even insights from these perspectives are different, that do not mean that those should be. To raise performance, it is vital that these two perspectives can achieve common understanding. This could be done for example by dividing a ISMS to such sections that are easily understood by both levels. This is normally done by adding executive approved policies on top of the standard procedures. These policies describe company management approved higher goals, while SOP’s include practical level guidance et examples of how to implement controls. Here it is essential that executive level requirements and practical level operative instructions meet and appropriate language for both are used.

One practical example of this kind “standard procedure” which is mentioned in ISMS, could be from incident handling. If and when an incident occur, it should be categorized, analysed and handled according to detailed process. Afterwards the organization should found lessons learned from situation, especially if there was something which did not go “by the book”. It is important to educate personnel responsible of incident further, because they

might encounter similar situations in the future. This increased knowledge could be reported to executives to give them resources for planning and to support risk analysis. Results of the analysis could be used to improve company's own risk handling or give to customers and improve their abilities respectively. This in turn might increase company's possibilities for profitable business and turnover.

When you do this procedure relentlessly time after time, each decision loop should be smaller and smaller each time. As well time consumed per loop should be significantly less when compared to first ones'. At same time, as desired by-product, maturity and quality of process improves by being more accurate. This is achieved with better knowhow throughout company, because each loop improves knowledge and skills related to security domain.

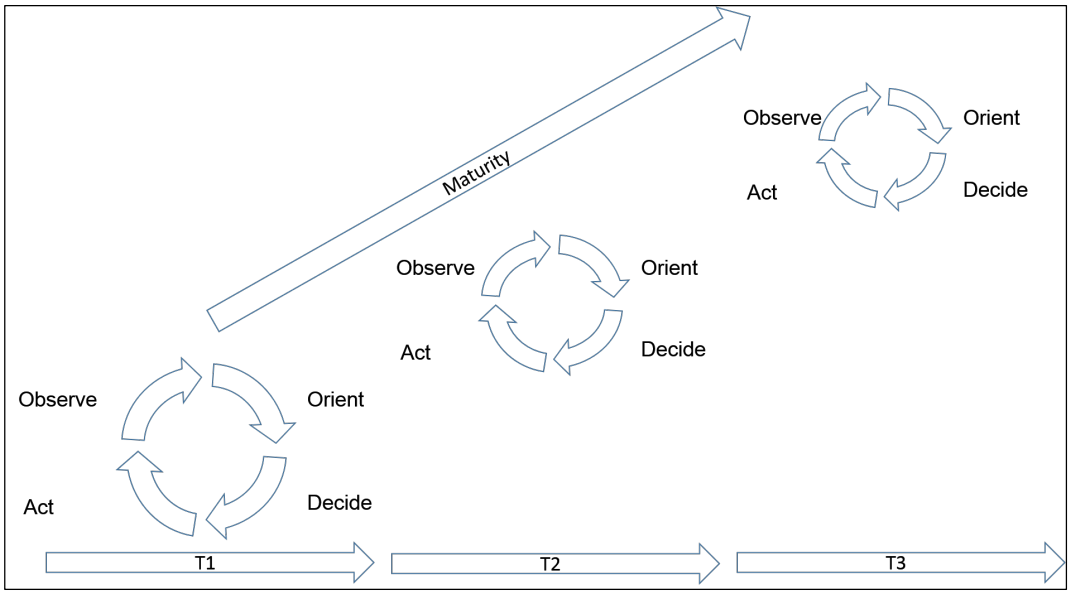


Figure 8 Delivering security is continuous improvement. Each loop cycle improves maturity of security processes and is faster compared to previous one.

According to Boyd, "*An entity (whether an individual or an organization) that can process this cycle quickly, observing and reacting to unfolding events more rapidly than an opponent, can thereby "get inside" the opponent's decision cycle and gain the advantage*" (Boyd 1987). Even John Boyd grind his thoughts mainly for the military audience, his findings are valuable for the business as well. There the word opponent could be understood as rivals within the same business domain and advantage as shorter throughput time for service processes, meaning overall effectiveness and reduced costs bringing benefits for the company and its customers.

If comparing previous process driven sight to the Cynefin framework, it is known that the Obvious domain is the one where issues are known, in order and cause-and-effect relationships are clear and easily discernible by everyone. This means that incidents categorized as “obvious” must be handled with the most mature processes. This also means that the obvious domain is a good starting point for less experienced personnel to start further learning and gathering experience towards less balanced Cynefin domains. Delivering this kind of learning path is important, because it should not be expected that unexperienced personnel could achieve top level performance without possibility to learn from previous experiences. Boyd claimed in notes from his talk “Organic Design for Command and Control” that “*all decisions are based on observations of the evolving situation tempered with implicit filtering of the problem being addressed. These observations are the raw information on which decisions and actions are based. The observed information must be processed to orient it for further making a decision”* (Boyd 1987). Explicitly this mean that each resource dependent of its type (personnel, process), should be given time to mature.

In information security observations and decisions based on those, could be seen as building blocks for security awareness. To establish permanent influence and to achieve higher level of maturity, it would be recommended that company should establish structures to handle security issues. Here maturity is understood so that a more mature organization is, the better defined and managed its security related processes are. This systematic manner of approach is defined in ISO-standard 27001:2013 (SFS 2013 a) and is comprehensive with service management processes described in ISO 20000:2011 (SFS 2013 b).

To improve the ability to effectively transition to an improved process models to measure process maturity has been developed. The International Systems Security Engineering Association (ISSEA) defines 5 level of capability in their capability maturity model (CMM), which has later been recognized as standard ISO/IEC 21827:2008.

1 *“Level 1*
Base practices are performed informally

2 *Level 2*
Base practices are planned and tracked
3 *Level 3*
Base practices are well defined
4 *Level 4*
Base practices are quantitatively controlled
5 *Level 5*
Base practices are continuously improving"

(Philips 2003, 4).

While comparing maturity model and previously mentioned standards, the capability maturity model and ISO standards share a common concern with quality and process management throughout standard series. As ISMS rely largely on standards, this approach could be found from it as well.

7 Different levels of decision making and the OODA loop

In this chapter a decision making process in different levels are studied shortly. After we have understanding on how and on what level decisions having effect on ISMS are made, the OODA loops suitability to support ISMS is examined.

7.1 Strategic, tactical and operational decisions

In Business management functions are often divided in three levels: strategic, tactical and operational levels.

While forming an ISMS, the strategy could be seen as backrest which is giving legitimacy for tactical level decisions and actions of operational level. As described by Woolridge and Canales, that is how formalized rules, social mores, norms and other constraints of individual behaviour become justified. Here legitimacy of strategy refers to the extent to which organizational actors accept, support and are willing to put forth effort towards an organizational strategy. (Woolridge and Canales 2010, 218).

In this perspective, creating an ISMS is, and must be, a strategic decision. Purpose of this decision is to transfer managerial knowledge, vision of the future from managerial level to acting level and this way it "*emerges as an appropriate course of action*" (Woolridge and Canales 2010, 219). Here

strategic level is such executive managerial level that approves the policies, risks, requirements etc. frameworks defined in tactical level. Characteristics for the strategic decision makers is that they present company's top management, are executives or equal. They do not often work full time with security related matters and look information security mainly from business or business administrative point of view. Company incomes, return of investments (ROI) and costs are in their main focus. This makes essential for CISO that he speaks fluently "business" and that he is capable to justify needs of information security management based on business needs and benefits.

Tactical level is the actual level which creates guidelines and standard operational procedures for security policies, evaluates threats and risks and follows actualized information security level metrics. If there are problems on those, strategic level should be informed and possibly issues should be handed over to them find appropriate actions.

Tactical decisions in this context are decisions which are based on strategy and are implemented in operational level according the SOP's to meet the requirements. Tactical level is responsible of maintenance of ISMS and that the followed metrics are at acceptable level. Tactical level also produces plans and requirements to operational level for implementation, but does not involve in actual accomplishment, even is following that controls take place as planned. Important task for the tactical level is to follow that appropriate controls are respected and given guidelines are followed. To ensure this, internal audits are used as tools.

In practice, especially in small and mid-sized companies (SME), tactical level prepares decisions for strategic level for decision making and is that for in key role what comes to actual implementation of information security. Here SME's are enterprises having less than 250 employees and annual turnover is less than 50 m€ (Statistics Finland N.A). Tactical level managers should be rather experienced and possess good knowledge of the security domain and its role in the company. Tactical level role is at first administrative role, even tactical level often shares responsibilities with both strategic and operational level.

In the following figure, Figure 9 Roles in information security domain, the division between different levels roles and communication between those are

described. Here importance of correct and homogeneous communication should be noticed and emphasised. This is one example where the need for ISMS is obvious, as it could deliver coherent vocabulary and consistent processes to deliver information from one actor to other.

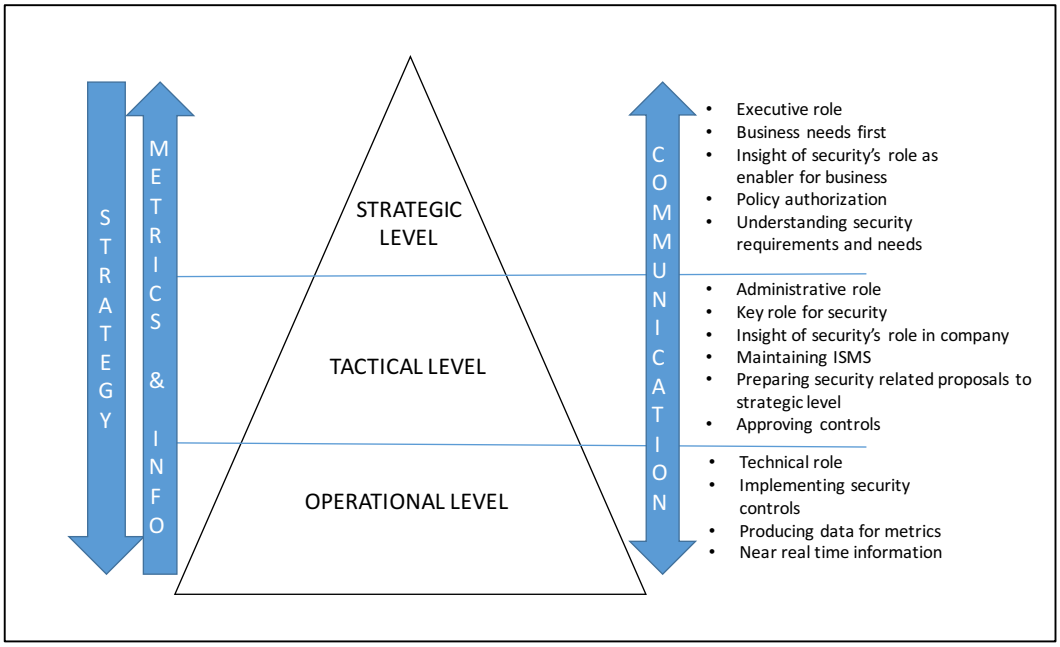


Figure 9 Roles in information security domain

Last, but not least, is the operational (performing) level. It involves planning, implementing, maintaining and monitoring the enforcement of information security policies and their metrics. Operational personnel skills should be more technical and their work is most of all practical in nature. Operational personnel produce trustworthy, quality data needed for metrics and information about current situation to maintain operational security awareness. As operational personnel role is expert technician, they have rather large level of responsibility and high requirements while implementing their tasks. That for they should have as well quite high level of independence and freedom to perform their tasks, even tactical level supervisors have control over them. This dependency over each other creates need for efficient communication and co-operation to provide frictionless functions.

7.2 OODA loops suitability to support ISMS

Based on previous chapter, selecting OODA loop as framework is implicitly a strategic decision even implementing it in practice is a tactical one. OODA

loop's support for the operational and tactical levels seem appropriate, especially what comes to increasing common understanding from requirements and nature of tasks in those levels in hierarchy. For longer term decision making other applications of Deming's Wheel, like PDCA, seem more suitable. There are opposite opinions as well (Lenane 2013), but agility, low response times and recognizing that information on which decision making is based on, is always incomplete, are typical characters for both OODA loop and everyday acts in operational level. Correspondingly PDCA should have implicitly analysed and structured information available to make strategic, longer-term decisions or to help create such actions that are needed for fulfilling bureaucracy needs like budgeting etc. Example of this is year-clock, a Deming wheel application seen Figure 5 Example of planning level loop - Year clock for ISMS.

Even there are some differences between these two applications (PDCA and OODA loops), it is good to recognize that a most important thing is that you have systematic approach to security issues and that you make justifiable decisions that leads to proceeding. One good example of systematic approach is ISO27000 standard, which also is often described as continuous loop and where requirements are strict if ISO-certifications are maintained as should.

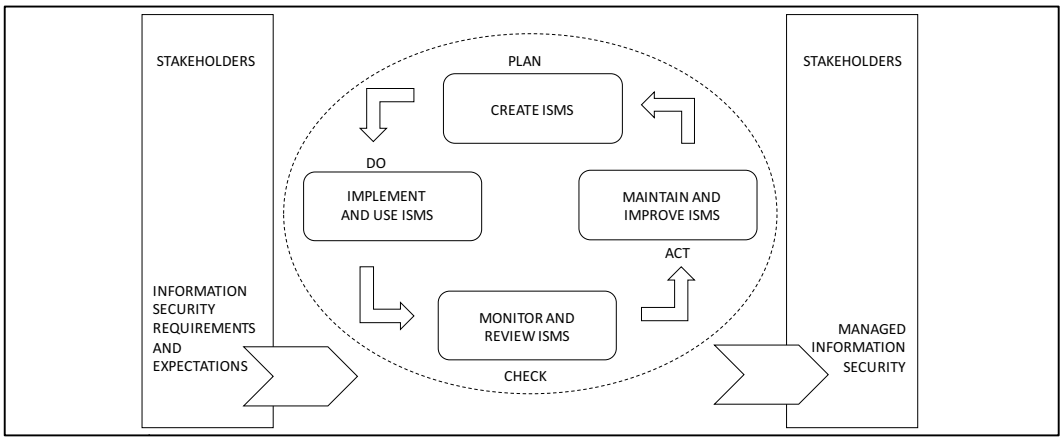


Figure 10 PDCA loop according ISO27000. Reproduction by the author after Finnish Standards Association manual 327 (SFS 2010, 35).

Above the writer mentioned proceeding as goal for decision making. In all loop-formed cycles continuously delivered decisions and acts have vital role to proceed and here they share same vision with lean process thinking. Proceeding after decisions is essential, because according to Ullmann

(Ullmann 2007, 23) based on Nutt (Nutt 2002), half of decisions made failed to have noticeable impact to making organization unless waste use of resources are not counted as such. This despite the fact that rank “Successful” was granted for such decisions which have sustained within two years from the decision made. If time limit is lowered for example to six months, how low will be the success rates then? While talking about information security, six months could be considered as a small eternity, even maintaining work itself should be done relentlessly and during long term. With continuous proceeding this could be avoided, but success requires constant monitoring and that problems are recognized and fixed as they appear. That for the actual operational level operator has important role in this which should be recognised and needed freedom to correct matters should be established. This is one essential reason why the OODA loop is suitable approach to support ISMS.

If the OODA loop do not include revolutionary thoughts, why it then delivers such enthusiasm? In my thoughts organizations and systems know that current methods could and should be implemented to be better. Often repeated phrases like *“… we must run as fast as we can, just to stay in place. And if you wish to go anywhere you must run twice as fast as that”* (by Lewis Carroll, from his book Alice in Wonderland) and “*Companies won’t die because of their false actions, instead they die because of the continuing of the same actions for too long (which once were right)*” (Jaakonaho 2010), are good examples that need of continuous improvement is at some level realized, but often overlooked fact.

As already stated, at first glance the OODA loop looks pretty simple solution, which however could be extended further for many levels and tasks in organization. Described as loop, even it actually is not such, as Brehmer demonstrates in his paper (Brehmer 2005, 4), OODA process could be presented and adopted in relatively easy way. Without further companies need descriptively adequate way to share understanding at a sufficient level of detail. It seems that loop does provide a concise framework for improving competitive power throughout an organization, which could be seen on of the main purposes for ISMS as well.

One challenge of selecting framework for this thesis was that it, as well its outcomes, is going to be implemented for practical good of family business. Company's business is constantly growing and is actively looking approaches to attract its customers. Good, valued services for customers are one of the most highlighted aspects in the company. While over 80% of its workers working on technical tasks, it is obvious that company lead is not willing to put extra effort on developing time horde and costly theoretical approach. Instead, at least in writer's side, demand was that theory should be such that it could be taken in to operational use without training of theory itself to audience. Finding a framework that is simplified, lean and put a lot of aspect to peoples personal development was highly appreciated. One view supporting adaptation of the OODA loop, was that Astrachan suggest that the Boyd's OODA loop, the framework and approach might suit relatively well to family businesses because of their characteristics beyond money making. In their work researchers noticed that Boyd himself underlined importance of moral bonds which according to them is comprised as a typical distinctive of family business. (Astrachan, et al. 2012, 556).

7.3 Criticism against Boyd's work

As all doctrines or strategies, also Boyd's work has met criticism. Even the OODA loop's activities are clearly distinct; they are not distinctive. One could even say that those are something that could be considered as self-evident, obvious cases to anyone having clear mind and enough common sense. It is true that Boyd never actually published anything besides of his briefing slides and even those are not officially published (Osinga 2006, 7). That for Boyd's ideas are not peer reviewed, like they should according to normal academic procedure. It is also true that OODA loop is generalized and missing important viewpoints. Claim that OODA loop hardly describes decision making in general, nor military decision making in particular (Brehmer 2005), seem righteous as well. Boyd's theories were said to base on controversial theories and suspicion of evidences have also rose up (Hasik 2012, 4-7). Much more important are aspects supporting learning and adaptation, which is supported by Frans Osinga's viewpoint: "*The OODA loop is much less a model of*

decision making than a model of individual and organizational learning and adaptation" (Osinga 2006, 250).

Criticism may not be agreeable from the targets mind, but it is necessary to call attention to state of matters to develop them further. From this perspective it seems to fit into wide scale of the OODA loop itself. Boyd himself seem to be quite insensitive for criticism. Instead for him it was important to have long discussions with different people to find out different angles to subjects and to teach himself to further teach other. In these missions he was relentless and hard headed as described in his biography. Seems that his goals were altruistic, for example he did not accept even travel expenses of his lectures. (Hammond 2004, 14).

In this phase it is good to remind that there is not only one truth according Colonel Boyd's own words: "*If you're going to regard this stuff as dogma, if it's going to keep you from thinking, you'd be better served to take it out and burn it.*" (Richards 2012, 2). So Boyd himself obviously encouraged his listeners for independent thinking. This encouragement is such a trait which is useful in the security and as well in the family business.

7.4 OODA loop phases one by one

7.4.1 Observe

Observe in OODA-loop means making observations from outside information, unfolding circumstances and interaction with unfolding environment which is influenced by the constant feedback got from other phases of the loop (Hammond 2004, 190 - 191). Based on that it could be said that observations are seeds of information that enrich and evolve during the time. While continuing this paradigm, observations are later on refined as material to following phases in the OODA-loop, orientation and decision-making.

To make beneficial, high quality observations, they should answer questions like below:

- What's happening in the surroundings that directly affect to us and our environment?

- Is out there something that indirectly affects to us and our environment or our capability to understand what's actually going on?
- What's happening that may cause residual affects later on?
- Were my predictions accurate and are there areas where fingertip-feeling and what actually happened has significant differences?

Observation itself is of course important, but capability to further refine previous questions is essential. Compared to Cynefin framework handled earlier in this thesis, these questions are aligned to it and share common concern about observation accuracy and capability to understand those.

Observations could be at first detection that something is going on or even hunch of such. In Cyber world this might be difficult and signals might be relatively weak and extremely difficult to notice. Partially this is caused by waste amount of transactions in cyber world, which create considerably amount of white noise and thus making finding of relevant information somewhat challenging.

When interest is turned in to found notice, one could obtain more observations, which in turn provide more information about phenomenon and related issues and so on to make observation "richer". This evolving iterative cycle is also described as targeting cycle in Pasi Hakkarainen's master's thesis (Hakkarainen 2014, 10). Process of observation that allows us to detect events in the environment should be "continuous and is constituted by the development and maintenance of interaction of various kinds with the environment" (Osinga 2006, 193). In information systems environment this should be considered as 24/7 monitoring, from which flow of information data is derived and interpreted to analysis later on. As amount of data is considerably large, in most cases it is wise to filter essential data available by machine driven algorithms.

One thing worth of notice while thinking about observations, is that how trustworthy information available actually is. David G. Ullman has stated that managing observations is actually managing information that is constantly evolving, inconsistent, uncertain, incomplete and dependent (Ullmann 2007, 22). Here lies also pitfall for machine algorithms. If algorithms are static, how could they manage with dynamic data? This is answered by different vendors

which are delivering “next-generation” appliances and services and (at least on marketing material) are offering more trustworthy and dynamic capabilities by adding human touch to their implementations.

Here I must admit that partially qualifying data and estimating it are already matters of orientation, the next phase of OODA-loop. Anyway I myself think, that observations and orientation are such closely bound to each other that mixing conceptions at least some level is inevitable and line between those is pretty thin. So we are going to handle a bit of quality of observations and issues that have bias on those already here in the roots of decision-making loop, in context of observations.

What kind of observations could be then used as source for good, rightful decisions? Here quality is perceived as characteristics or features that observation has before refinery (raw data). Beside of actual correctness of information also sources of information and context are meaningful. If information source is unknown and context is somewhat vague, it diminishes quality of the observation at this time and in current context. Even observations quality might be get lower in desired context due this, observation might have unidentified value on some other time and correlation. This of course demands that observation itself must be recognized and it should be available later at this particular moment. These ways logically separate OODA-loops of different actors could have influence to others. This, I think, matches with Boyd’s vision of evolving, open-ended cross-referencing process of projection (Hammond 2004, 191). Once again, removing barriers to create better communication between groups and individuals throughout organization is key factor. Especially previous is true in data gathering (market intelligence) and cyber intelligence sectors where all data have certain value in right context.

Compared to previous it seems relevant that there must be several sources of information and much effort should be put in to analysing gathered data. Also it could be thought that the more you have data available, the more precise your information gets. Analysed data should be further turned into information (refined data) and such operational picture of which decision-making could be based on. This is put in words in Finnish Institute of International Affairs

comment: "*It is essential for decision-making to be based on both a robust common operational picture and the identification of weak signals. This entails anticipation, the importance of physical and network intelligence gathering, and international collaboration to improve situational awareness*" (Salonius-Pasternak and Limnéll 2015). This is partially observations and partially orienteering prior to decision making, but anyway obligatory phase to make decisions best possible.

Without such system (human or machine) which could analyse and present data fusion from several sources, gathering data in large amounts could be unnecessary and resource wasting. According to Nutt, all human beings have difficulty extracting diagnostic information from the signs and signals attracting their attention – Including decision makers. People become attached to the first information they observe and give it more weight than information that arrives later on. This might cause that decision makers are tend to using information that is easily available, overlooking information that may be more analysed and might give better tools for decision making and this way better decisions. (Nutt 2002, Kindle Locations 1033-1042). In this context this notice definitely belongs to next phase (orientation), but is presented here to show that data refinement in some degree is necessary before handing results forward.

If information available is overwhelmingly rich in amount and it is not extracted before presentation, there is a danger that decision makers adopt only such information to which they were somehow familiar in beforehand and which support and possibly boost their existing preconceptions. If pre-handled data is used this way, decision making become tinted with selective perception. Obvious is, that same could be happened if data refining is tightly instructed.

Data refinement and abstraction could also reduce amount of essential information if it is not recognized as such (relevant and essential) at time of analysis. Also prejudices of operational personnel, algorithms and schemas created in software during programming by programmers are limiting factors and should be recognized and considered as such. That for data handling algorithms, rules and principles should be openly available for review.

Previous underlines that neither persons nor systems alone are good enough for creating absolutely or, in worst case, even truthful enough situational picture. Instead it is essential to combine personnel insights and experience already while implementing data fusion system with “finger-tip feel” (fingerspitzengefühl) used in data analysing phase. In some sense this is kind of conflicting way. This is because systems mentioned earlier are created to help finding out such data that is essential to make decisions precise enough within given timeframe. Aim for this is to refine data to such on which decision-making could rely on and this way to reduce amount of fingertip feel and intuition needed in decision-making process. Due previous characters this approach is particular suitable when dealing with “known unknowns” and to find anomalies to filter up “unknown unknowns”.

As a gathering from this chapter, it is important to recognize incompleteness of information, technical systems and persons using those.

7.4.1.1 A way to affect one’s mind - Strategic communication

One factor is essential while considering incompleteness of information and this factors impact on it. Every piece of information and technical systems processing it are made by humans trained by humans. This way all information is “contaminated” by humans and have certain aspect to subject in matter.

Strategic communication is such a phenomenon that might change information security’s horizon more than we could actually understand right now. Thus far it is recognized, but is somehow not taken into consideration in planning and training, except in military. Even later examples of strategic communication are happening in national and international levels, phenomenon itself is something that must take into consideration while giving training to security personnel in private sector as well. Perhaps the best model to training could be found from education sector, where importance of source criticism is recognized and where it is emphasized throughout the education.

7.4.1.2 Influencing to observation sources and orientation

How could we then make influence for observations and orientation phases of the OODA loop? One possible way might be opinion shaping by means of reflexive control (RC), which aim “*is to put subordinates to make actions*

oriented in a certain way in given timeframe and based on certain kind of information" (Riihijärvi 1999, 132). In principle RC could be used to have effect either human (mental) or computer-based decision-making processes and evidence of its effects exists (Thomas 2004, 237-238, 252-253).

Where origins of RC are in former Soviet Union and currently in Russia, its western counterpart is Perception management (PM). Difference between these two are that where RC is focusing more to controlling decision making, PM counts managing the way how perception is made (Thomas 2004, 237). Here perception is understood as The Oxford Dictionary defines it: *"The way in which something is regarded, understood, or interpreted*" (The Oxford Dictionaries n.d.).

Both RC and PM could be seen as forms of opinion shaping. If opinion shaping is good or bad thing, depends of the aspect of observer. While opinion shaping methods could be used for training to achieve desired results, same psychological mechanisms could be used to affect to opponent's mind as well. Taking advantage of psychological methods is particularly interesting while considering ISMS as a tool for sharing common understanding.

One example to support this aspect comes from Russian Major General (ret.) M. D. Ionov, who wrote according to Thomas, "*one can assess human targets of reflexive control either by personality or group depending on the specific individual's or group's psychology, way of thinking, and professional level of training*" (Thomas 2004, 245). This statement demonstrates that training has effect on the way how one perceives observations and this way has influence on orientation as well. Realizing this is positive thing and should be taken into consideration while planning ISMS.

In opposite, adversary's aim is to shake foundations to create chaos and disorder in all levels of decision chain and in that way to influence on decision-making process. Cyber world makes no difference on this. To achieve the deepest effective influence throughout opponent's decision chain, influence should be tactful and must be made during longer time period having effect already observation and orientation phases of the loop. This way might be obscure, but it has most probably influence on decisions and actions in all levels of organization, including strategy and tactics and even assisting

systems. While considering opinion shaping at operational level, it seems to be more like “hatchet job”, not so delicate anymore, instead being rude and for trained person kind of obvious.

7.4.1.3 Examples of strategic communication operations

Maybe the most blatant examples of strategic communication operations are claims, opinions and colourful discussions on different medias about Russia’s actions in Crimean Peninsula in spring 2014 and later in eastern Ukraine. Even it is not recognized by Russian government, exact circumstantial evidence of Russia’s existence in areas and from information warfare do exist (Bellingcat 2015). Based on previous independent research, it seems righteous to claim that Russia’s government uses strategic communication to shape opinions in their homeland and in abroad. One example, from which again have no such indisputable evidence that Russia’s government has acknowledged, is using paid troll’s to strongly emphasize their pre-defined vision to deny Russia’s armed forces existence in area and endeavor to dilute anti-Russian opinions in social media little by little (Aro 2015). Compared to straightforward propaganda of earlier days, current opinion shaping is more tactful and name has also changed to “Strategic communication”.

For example we could take a further look from Russia’s Federation point of view, where opinion shaping is part of information security and justified as follows: “*By the information security of the Russian Federation is meant the state of the protection of its national interests in the information sphere, as determined by the overall balanced interests at the level of the individual, society and the state”* as told in Information Security Doctrine of the Russian Federation (Russian Federation 2000). From previous we can see that strategic communication is holistic and it has effect on every level of communication.

What are then the typical features for strategic communication and could those be recognized if seeing one? As we can see from Russian Federations Security Doctrine, aim of strategic communication is to enhance strategic positioning and competiveness of the organization. Further characteristics of strategic communication is “*that strategic communication must be clear, true, repeated, consistent and delivered with passion*” (Financial Times n.d.). So

strategic communication could not be successful, if ones presenting it are not trustworthy and reliable.

Further on, according to Jantunen (Jantunen 2013, 79) Strategic Communication is a one way process going down from the top, aiming of transferring meaning to something else. This “something else” is such point of view or opinion that is given by organizations top level and exact guidance and leadership is the top most priority to achieve wanted aim. According to Ginos, “*Existence of consolidated central government is essential to successful strategic communication*” (Ginos 2010, 39), which could be clearly seen in in-line opinions in autocratic societies like Russia, Iran and North-Korea for example.

In other hand opinion shaping is something which we humans do and meet every day. We change opinions with each other while we discuss and changing opinions is something what we are encouraged to do in work, everyday life, school, politics and so on. It is something that is relevant to make compromises and to avoid crashes which black and white opinions undoubtedly cause. Marketing and advertising are one form of it, lobbying other one. So opinion shaping is kind of vague area, as are many other matters in human life and that for it could not be classified strictly to good or bad.

Also openness to share information and do co-operation could be seen as one reflection of opinion shaping. For example, sources in this thesis are predominantly western origin and to be more precise, from commercial and government sources located in United States or countries recognized widely sharing similar values. This is because materials are easily available in such language which one understands and, as far I could say, identified to include valid, proven information. This way it is justified to ask if this unilateral approach is recognized to cause certain inequality and unbalance and how this could be avoided. Here I could only say that openness in sources and each readers’ careful considerations and intelligent arguments for source are the keys.

7.4.1.4 A further look to the opinion shaping

Decision-making is seldom easy and by making observations vague, it could be hampered greatly. Possible way to take benefit from disinformation and opinion shaping is to use it as asset for hybrid warfare to bring uncertainty and chaos to society and this way to make decision making harder. New York Times magazine (Chin 2015) describes in its article way in which pseudonym writers used social media to cause disorder and confusion in St. Mary Parish, Louisiana, United States, September 11th 2014.

In modern world where information floods thru different social media channels continuously, this kind of given disinformation could to be very effective way to achieve and fortify disorder. St. Mary Parish this evil hoax does not succeeded and perhaps it could be seen as failed experiment? While example from St. Mary Parish is still quite fresh while writing this thesis, there are good examples of successful campaigns utilizing disinformation in the past. During World War II (WW II) allied forces successfully carried out operations like Fortitude and Mincemeat and lessons learned from those are still relevant to gain advantage over adversary (Bacon 1998, 24-25).

One difference that inevitably comes to one's mind is that what is difference between somehow unsuccessful and successful maskirovka operations? Here I see a big difference that when successful operations during WW II were made, opponent was vigilant and waiting for such signals which actually amplified Germans initial thoughts that something trickery is going on. Also it looks like quality of information was somehow poor or it was not available enough. Presumably in that particular time it was hard to get data confirmed due the fact that parties were in open war, i.e. situation was black and white. Accordingly, St. Mary Parish case event was unexpected, which of course created some confusion among local authorities. But here value of information sources (mainly social media) were disputed and instead asked information straight from claimed party to have more precise situational picture.

As a conclusion of this, it seems righteous to claim that data that is available from several independent, confirmable sources is more accurate and has more qualified features compared to data which is given from somewhat obscure sources.

7.4.1.5 Thinking outside of the box

As told in previous chapter, while opponent is waiting something to possibly happen sometime in the near future, it seems to amplify signals and that for not enough notice is given to collected data's quality. Instead of amplifying data available, it should be important to search existing data and nuggets of information that do not fit with the current orientation (Astrachan, et al. 2012, 552 - 554). This, of course, makes heuristic approach as virtue while considering observations based on available information. In Boyd's OODA-loop this is taken in the consideration by describing implicit guidance and control plus continuous feedback as building blocks for successful accomplishment (Hammond 2004, 190). Why implicit instead of explicit? Perhaps Boyd noticed – based on his own experiences and possibly his own way of learning – that teachings stay better in mind if you realize meaning of those by yourself. That for more experienced could guide less experienced to right direction, but not explicitly giving ready chewed answers to the given questions. This way learning might be more efficient and leaves also room for one's own interpretations and thinking. Yet this can lead to new inspirations that could give further boost for next cycle of the loop.

While looking amplifying problem from other aspect, you should try to encourage your opponent to self-deception and mismatches. This could cause either early actions or delay, so that long that adaptive changes become either impossible or so costly, that they are not worth of implementation any more. Beside of independent thinking, previous underlines importance of right timing for successful operations, which could be seen as one expression of experience.

Boyd himself emphasized importance of independent thinking out of the box by "A Boyd Quiz" which is illustrated below in Figure 11. In the Boyd's Quiz there are three simple outline diagrams; a square, a triangle and square with diagonal lines from corners to opposite ones.

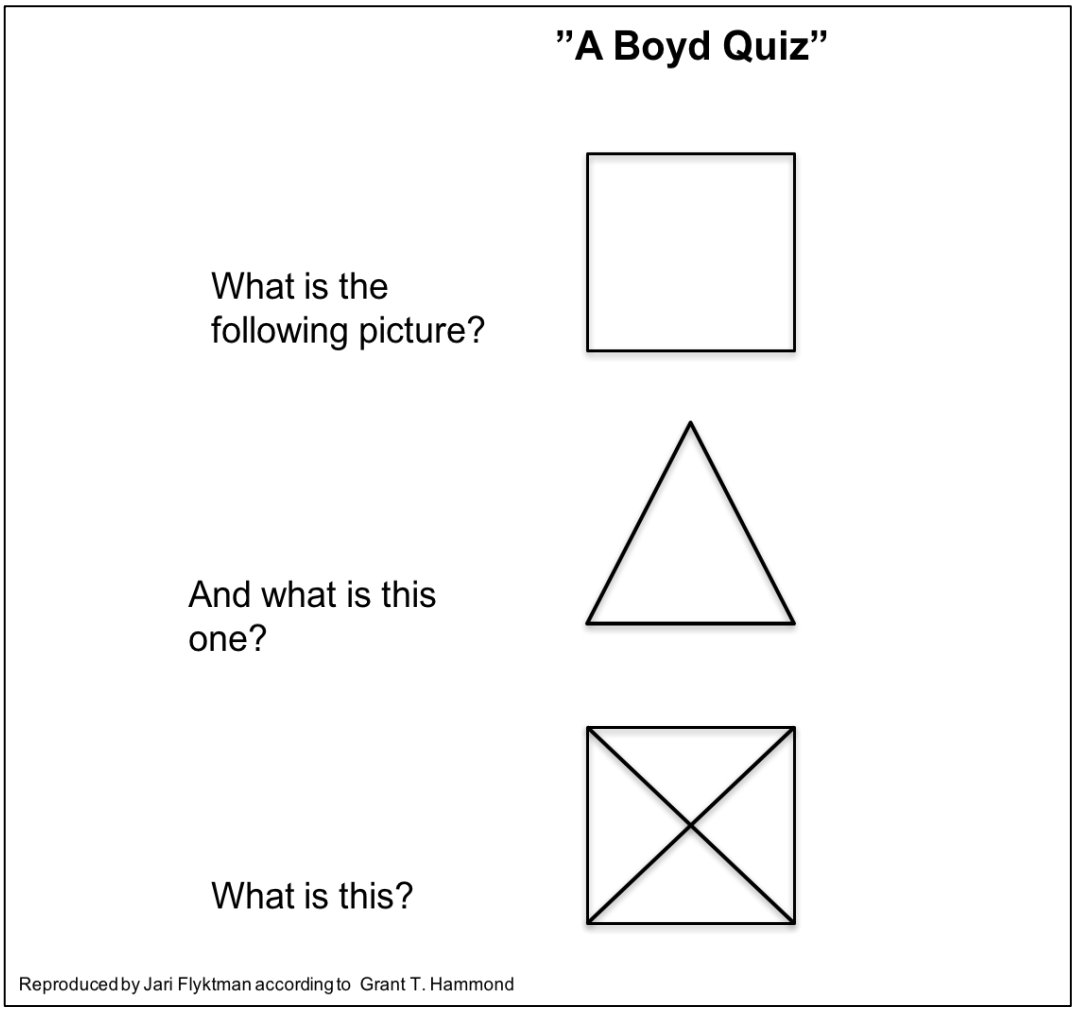


Figure 11 A Boyd's Quiz (Hammond 2004, 181).

Boyd argued that that all three diagrams in the illustration are the same; a pyramid viewed from different angles. First one is pyramid looked from down, second is a pyramid looked from the side and last one is pyramid looked from the top (Hammond 2004, 180 - 181). The middle one, “pyramid form the side”, could present view of the normal person, Average Joe, who is standing in the earth surface and looking at the pyramid. First view (square) could be characteristics of excavator operator, for example. They work with blueprints and they look buildings from makers’ objective, where base dimensions are important. Third, from the top point of view could be view of bird. Again, matters do not look the same from excavator operator’s or bird’s angle compared to Average Joe’s view. This simple example demonstrates that interpretation of the same thing could vary greatly depending on who makes it and from where it was made. Realizing this could make great benefit for one

and leads us smoothly to the following phase of the OODA loop, in orientation phase.

7.4.2 Orientation

In “Handbook of research on strategy process” Astrachan et al. describe orientation as “*the lens through which what is observed in the environment is perceived and interpreted*” (Astrachan, et al. 2012, 551). As found out in previous chapters, everything in our environment affects to our mind and how do we observe and understand issues; environment itself, genetic heritage, our training and cultural traditions, lessons learned from previous experience and information gathered during observation phase. If observations are not unambiguous and could be understood in several ways, orientation is the point where wrong and inadequate observations are noticed and weak signals are amplified either justified or unjustified way. Importance of orientation could not be overestimated, because it is the conclusion of weighing and thinking. To put it short, orientation is active process of understanding.

7.4.2.1 A brief look to things that have effect on our orientation

What then has affect to our orientation? Already a new born has certain abilities. New born baby could suck mother’s breast, they can also smile and cry for example. These abilities could be found from all normal neonates throughout the globe discarding nation where they have born or race they are. Education, culture or other non-genetic or non-environmental matters have not affected to new born yet.

Babies react more or less with similar way to similar issues. That for these skills could be considered as a part of human race’s genetic heritage. Some of the babies are more sensitive than others and they do react in different way to environment factors. In later age persons react in a different way to stress, which could be easily seen in everyday working life. So each person has different way to react to different issues and each one perceive matters differently. It is explained that genetics can have an influence on normal day-to-day levels of the stress hormone cortisol, on the reactivity to stressors, and due this even in the way that we perceive the world (Juster and Marin 2011, 2).

While young person grow he meet considerable amount of different matters that shape his mind. First among those is family; parents, siblings, grandparents, aunts and uncles. They hand over their habits, believing's and thoughts to youngster. Later on education has major effect. Persons learn read and write, mathematics, chemistry, physics and foreign languages among other useful skills. As it could be easily imagined, teachers and teachings shape youngsters mind and the way in which they see the surrounding environment. This is also the ground where strategic communication can have its affect.

It is inevitable that experience gathers during one's life. While person gathers experience, he starts to learn from those. When receiving new information, it is combined to previous learning's and experiences. This all put together form synthesis that is base for every decision making. "*These are not activities, as the elements of the original OODA loop (except for analysis and synthesis), but factors that affect the outcome of the Orientation stage*" (Brehmer 2005, 4).

Due its deep, elementary nature, Orientation is perhaps the most important phase in OODA loop. "*Orientation is an ongoing, interactive process, whose outcomes at point in time are images, views or impression of the world, shaped by the factors above*" (Astrachan, et al. 2012, 551). John R. Boyd explains mentioned "factors above" so that without our genetic heritage, cultural traditions and previous experiences, we just do not have needed psychophysical skills to survive (Osinga 2006, 245). To say that in other words, without those skills we just do not understand what is going on and our view to environment is incomplete, because we do not have material for analysis and cannot even form the needed synthesis.

As could be concluded from previous, persons are different and in different phases of their cycle, which in this context is OODA loop. Then it is natural that all personnel available to company do have different skills and experiences, thus similar, "standardized" performance could not be expected throughout available resources. To modify common understanding, ISMS has big role.

7.4.3 Decision making

The Merriam-Webster dictionary defines that decision making is "*the act or process of deciding something especially with a group of people*" (Merriam-Webster Dictionary n.d.). This definition is good in that sense that it underlines significance that decision making is a process and it is made with a group of people, or in other words, under the influence of many. This is true even decision itself could be made by one person only. Inside of OODA loop, decision is the component in which actors decide among action alternatives that are generated in the orientation phase (Osinga 2006, 232). Here the words "among alternatives" are essential ones. Decision itself could be one of the many possibilities, it might be right or wrong. When decision is made, we do not actually know which one it eventually will be. Alternatives and possibility to make wrong decisions make decision making a demanding work.

But without decisions made we cannot act. Where reactions come as response from sub consciousness, acts need always some kind of decision on their basis. From actions made, we get valuable feedback, which further evolves our processes. That means that without actions we do not evolve nor make progress and that makes decision making extremely important. Without decisions whatever loop stop spinning.

Col. Boyd himself clarified Decision part of the OODA loop in later versions with word "hypothesis" (Astrachan, et al. 2012, 553). Word hypothesis opens complex of decision making quite well. A dictionary clarifies the meaning of word Hypothesis as follows: "*an interpretation of a practical situation or condition taken as the ground for action*" (Merriam-Webster Incorporated n.d.). Decision is hypothesis based on gathered data, synthesis and analysis of it spiced with ingredients of our genetic heritage, cultural traditions and previous experiments. Decision maker could only assume that decision made is right one for that particular time and moment, but we could evaluate it only afterwards.

This Boyd's observation from the nature of decision making (hypothesis) gets valuable consolidation from science, astrophysics as an example. Albert Einstein published his general theory of relativity in 1916. In his work he made hypothesis based on his observations and analysis, of "*universe in which*

space and time are interwoven and dynamic, able to stretch, shrink and jiggle" (Overbye 2016). In measurements that aimed to verify existence of gravitational waves, researchers of LIGO laboratories were successful and published results confirming Einstein's hypothesis nearly 100 years after hypothesis was originally created (LIGO Caltech 2016). Previous is of course an extreme example of hypothesis, as consequences of decision are viewable much faster in normal life. But at same time it shows well characters of hypothesis and decision making – Only future can tell the truth of being right or wrong.

To conclude this chapter, decision making is kind of apex after long period of digesting information and trying to find best way to handle it so that it makes possible the most beneficial approach towards given goal for your organization. To simplify this further, decision making is putting right pieces together in right time and place. This is based on observations and synthesis and analysis formed from those with experience of life.

7.4.4 Act

On previous chapters I have long tried to interpret different phases of OODA loop and what affect to those and how do them look to me. After having needed amount of good quality observations and orientation based of long experience you can make hypothesis of what would be the most suitable action based on previous. That should not be too difficult, as most appropriate sakes are already knew and act is only putting those to realization. Well, of course matters are not that simple. Act is expression of all previous in real life, kind of extraction, and that way it shows how we have adopted causes and puts those in test.

Test is also mentioned in Boyd's OODA loop's final version as presented in his summation of "A Discourse on Winning and Losing" (Hammond 2004, 190). If looking meaning of "Act" from "Test" perspective, one usually do test(s) because we would like to have results which show how different variables change the Act itself or if Act is working and giving such results as we expected it to do. Finding this out we should constantly monitor test environment and results and found out how different changes in parameters or

environment change results. In OODA loop presentations this is put in words “Unfolding Interaction with Environment".

According to our empiric experience incidents usually have at least some matters which go wrong. There we must change the process according new perceptions, gladly as soon as possible to keep loop rolling and to gain possible advantage. But what if matters go as planned and as they should go? Results achieved from actions are wanted and our operations rolls smoothly forward? Have we changed conditions so that we would receive wanted results? Do we act as should, is process tempo as fast as it should? Are our tests formed right? Could that be true and how could we improve our process if there is no mismatches and discontinuity? If this is truly the case, we cannot. But then we could ask ourselves if we’re having a right process and if it is possible to change one to more efficient way of doing either by changing technics or technique. Also question if we should even have such process available anymore might be justified. Important here is that one should never stop evolving, even constant disputing and questioning might feel stressful. Management should be aware of this and that for allow different opinions and ways of act in their areas of responsibility. This is despite that requirements by performing processes in standardized way are high and they often might be interpreted so that everything considering those should be done one, uniform way.

If looking this from ISMS perspective, this is misunderstanding and standardizations should not think as limiting factor. Standards and frameworks, like ISMS, should be considered as tools which are used while aiming for better results. They are giving only the frame in which actions should be considered while aiming towards better results to achieve minimum level which must be accomplished. Purpose of the processes is that level of requirements should be raised constantly to gain better, more efficient results.

Other aspect while looking for Actions, results from those and significance of ISMS while managing previous, is that each Action should provide measurable results in the end of the day. Without such we cannot prove that our processes are worth of something. And if we cannot prove that, why such processes are existing at all?

To sum up chapter telling actions, is that each action is acme of long chain; it is showing in real what are our observations worth of, how well can we do orientation and can we make right hypothesis based on those. Results of act are the sources of evaluation. How to proceed faster, more efficient way and how we have managed so far? And as reminder, act-phase is not the endpoint as loop does not recognize such. Instead it delivers fuel for loop's next evaluation round.

8 How to achieve better organizational performance with ISMS?

While thesis works name is "Implementing Information Security Management System as a part of business processes", it should, at least some level, give answers how this could and should achieved. If you have read so far hoping to find undisputable answer to previous, I must unfortunately disappoint you. Aim here is nor to describe business processes in detail or give exact advisory how one should implement ISMS. I'm pretty sure that I'm not right person to do so on your behalf and that there is no need for that either.

Standardized processes, like one's according ISO20000 or ISO27003, are far better on that. Instead I aiming for better understanding from meaning of ISMS for companies, especially in SMB sector and if it truly can help organizations and what should be considered while implementing ISMS.

Here we should understand that business processes in general are such processes which aim to provide benefit for organizations and its members during certain period of time. ISMS processes do not make difference on this. Benefit here could be understood as making cases easier, more predicted, precise, measureable and so on. As we can see here, benefit from process aspect is not a single matter, even at last it could be extracted to such one, like company's profitability.

My claim here is, that processes can bring benefits for companies, without dependencies of their size or line of business. With processes companies ensure predictability of the process outcomes, meaning certain quality and level of profit for company. In this sense disturbances in processes could

mean less incomes and profit, which is the key result in business life. Same idea means in opposite that executing processes in more efficient way delivers better results and making business is more profitable. This deduction of thoughts is of course quite straightforward and highly simplified, but why it should be more complicated if its nature is known?

But how ISMS could make business processes more efficient, because it does not exactly provide anything measureable like dollars or euros? Here I must agree. ISMS is tool, supporting system for security processes and does not provide profit alone or by itself, even processes have at their best remarkable role while improving companies' performance. Even security could not see as source of profit per se.

Possible way how ISMS could bring financial benefits for company is by reducing insurance costs. So far, at least in Finland, insurance companies have not offered lower taxes for companies having certain information security base level, but this might change in the future according Paavo Porvari's doctoral dissertation. (Porvari 2013, 70). But if insurers could benefit themselves of lower risk frequency of companies having working ISMS, part of the gained benefit could then be forwarded to their respected customers. This beneficial win-win situation could interpret to born in situation where business parties have trust to each other's doing.

As previous example shows, business could be considered as matter of confidence instead of just being transaction of goods. One definition of confidence is "*A feeling of self-assurance arising from an appreciation of one's own abilities or qualities*" (The Oxford Dictionary n.d.). This describes well confidence needed in business relations. Remarkable is, that definition includes words "abilities and qualities". So security is quality needed to create confidence.

Further to create quality, abilities are needed. Brigadier general Mikko Heiskanen, Chief Information and Cyber Defense officer of Finnish Defense Forces, emphasized skills of individuals as source of trust and explained that cybersecurity require discipline and compliancy and those could be achieved by training and education (Heiskanen 2016). Creating needed abilities for security, ISMS is the tool to be used as guidance forward discipline, coherent

system fulfilling compliancy needs. With ISMS I here mean any system providing framework and model for maintaining and improving security despite of the name we are calling it. Of course for clarity's sake it is important to use unambiguous terms and names.

8.1 Better common understanding and communication

According to organization theorist Christopher Argyris based on Takala, healthy organization forms when all members of organization are aware of and understand company procedures and when these procedures are shaped to fit in persons need. Based on results given by done research, Argyris proposed that organization management should create such a working atmosphere where each worker has possibility to grow and mature both as person and as member of the group. (Takala 1999, 128).

Having such system as ISMS is important because otherwise we could not have common agreement of what are our goals for security, what actions are needed to get in there and how to measure level of our system currently. Without capability to measure, we cannot know if we are fulfilling presented requirements and if we are on such level that our customers implicitly do expect from us. In practice having an ISMS and its components in place could be seen as a matter of communication and based on that, following simple manifest was created:

1. Information Security Policy is an executive level manifest that company has ISMS in place and the company follows certain commonly agreed principles. This is to achieve required level of confidence to make business with other companies and security policy could be delivered further to customers to show management's commitment.
2. ISMS is an agreed baseline, collection of certain security related matters which must take into consideration while maintaining desired level of security and while improving it. ISMS is company's internal document and not meant to customers, but should be available for the company's personnel.

3 Certification is evidence provided by third party that the company fulfils given requirements. Essence of the certification is showing that the company is capable, capability is recognized and verified by objective third party.

8.1.1 Learning from the practice

Other possible way to improve company's overall performance is to raise performance level by guiding and teaching less experienced personnel by implicit guidance and control (as described in OODA-loop). Basically this, just like the formal means in previous chapter, is improving communication by sharing. Here means are bit different and could instead of written form presented in informal vocal way. One example of this could be sharing lessons learned by members of the team with "greener" personnel, i.e. which is not such familiar with matter of question. To support this, ISMS processes has remarkable influence. If "hot wash up's" and certain way of handling reclaims are not supported and demanded by formal processes, I dare to say that most of us will not arrange those even positive influence is publicly recognized.

To unleash the full power of organization encouraging informal communication should take one of the goals. Easy example to proceed could be "master – apprentice" model. There experienced person guides inexperienced co-worker towards better performance by helping in first steps of analysis and synthesis. This might make adaptation of new employees faster, meaning that they could raise level of their skills faster than they otherwise might do. Of course it should be noticed that training demand valuable time and resources from expert level employees, but personally I consider benefits higher than possibly losses. Again, ISMS has role to enable master – apprentice relationship and also as provider of common agreed vision. Particularly in this kind of process I see a lots of possibilities and value from ISMS, where its process could provide systematic approach for each company worker about insights to company's information security. This makes adaptation of security easier to understand and equalizes the way how meaning of security is perceived in company.

8.1.2 And what that does mean in practice?

What should ISMS framework then include if you're looking it from the new, unexperienced workers point of view? Remember, that world is changing from newcomer's aspect and flood of information and possibly whole new experiences giving over boost for brains to handle. ISMS framework must offer simple, sell structured matters first, like ones what are we here for and what justifies our work related costs. More commonly that is called the Visio. Purpose of the Visio could be here that ISMS should give the idea for the existence before getting in to deeper and make sense for why processes are done in certain uniform way. This means that ISMS is source of sense-making in complex environment reducing uncertainty and risks by sharing pertinent information.

Secondly a newcomer cannot know what is abnormal if you are not familiar to what is normal. With this I mean that ISMS should provide information of what is normal, what are the features of normal /abnormal and how to react if something abnormal happens. With this uniform way we are able to manage uncertainty and risks and develop possible courses of action to reduce friction and latency caused by uncertainty.

Prompt, quick response is many cases the most desirable action and it could be supported well by having an ISMS guidance available. But as discussed earlier, without realization of matters that have influence to one's focus points and opinions, decisions made based on given information could be wrong ones. This is perhaps the most common pitfall for structured systems and it became even worse if decisions are made without filtering existing information or with limited insight. This is the case if one only relies on processes and systems and do not do evaluation (analysis) of those before making a decision.

8.1.3 How to avoid process blindness and can ISMS help on that?

To avoid this "process blindness" we need capability for proper orientation to find out if existing data we have is correct and appropriate in this particular case. Are there any mismatches and such discontinuity what might not fit in to reality or our perceptions of it? For example, it is essential to understand

which part of the data is positive and which part of it is false positive, wrong or even misleading. To understand it, you must know why it is so. Why are you having “fingerspitzengefühl” that everything is or is not right? Would training from what is normal and what is abnormal help you to achieve more trustworthy feeling? I guess that most of us would answer “Yes”.

Understanding that our mind and systems that we use for analysis shape information to certain way (biases) and that people are having tendency to think in a certain way, are important while creating clear understanding of existing incidents. As studies have shown, that beside of being blind to the obvious we could be blind to our blindness as well (Kahneman 2011, 24). That for need for open-minded evaluation (orientation) of evidences (observations) is needed before making a decision (hypothesis) of how to act. Daniel Kahneman, a winner of Nobel Memorial Prize in Economic Sciences, has described decision making process in metaphorical way that every human have two systems working together to make decisions, System 1 and System 2.

System 1 is automatic, impulsive, and fast, it is working based on impressions, intuitions, intentions and feelings. Information to which System 1 establish its operations, are stored in memory and can be accessed effortlessly and without intention. Despite of System 1’s spontaneous, automatic nature, it makes appropriate decisions most of the time and it can generate complex ideas, which are further refined by System 2. Decisions which do not need further chewing, can be left in concern of System 1.

System 2 is that part of the system which is analytic, deliberate and conscious. System 2 makes decisions which require attention and effort and only System 2 can construct thoughts in an orderly series. These are formed mainly from impressions and feelings gathered by System 1. System 2 is not willing to have responsibility of decisions all the time, indeed it is rather lazy and adopts suggestions from system 1 with little or without modifications if they seem appropriate. (Kahneman 2011, 21-24).

This sharing of responsibilities could be thought as a handicap of decision making system. Actually it is not so simple and division of System 1 and 2 is efficient one while it minimizes effort and optimizes performance. System 1’s

immediate reactions are needed to produce response in situations where such are needed and where System 2 is not capable to produce such. This is true especially in situations where intense focusing is needed (Ibid. 23). Example of this is given in demonstration by Cristopher Chabris and Daniel Simons in their book The Invisible Gorilla and related video, where circa half of audience did not noticed gorilla suited woman crossing basketball field while they were concentrated to count passes made by other team (Chabris and Simons 1999).

Well, what all this has to do with cybersecurity and ISMS? I think that they have much in common, especially if you compare previous observations to OODA loop. One thing I found remarkably encouraging in Kahneman's theory: System 1 is able to execute skilled responses and generates skilled intuitions after adequate training (Kahneman 2011, 104-105). For ISMS's perspective this means that we can create a system working fast and producing appropriate answer to most of the cases with help of training and education. Adding knowledge is so claimed to add and improve capability to intuition as well. Even ISMS has nothing to do with "fingerspitzengefühl" and intuition is not certainly mentioned in it, ISMS has big role what comes to enabling of peer training and educational support itself.

To make conclusion from previous chapters, I found adequate to cite person which was Boyd's contemporary and whose thoughts were most probably familiar to Boyd. In his book Kahneman is quoting Herbert A. Simon as follows: "*The situation has provided a cue; this cue has given the expert access to information stored in memory, and the information provides the answer. Intuition is nothing more and nothing less than recognition.*" (Kahneman 2011, 236-237).

9 Conclusions

Current success of cybercrime is corollary. Significance of cybercrime is remarkable already in its current and it's still increasing, while role of information systems is turning increasingly into ubiquitous. This evolution might enable such possibilities to cybercriminals in such scale which we can only imagine. At least partially, due irresolute behaviour of large audience

cybercrime has become a vital community which is organically growing and “remaining as growth industry” (CSIS 2014).

If reflecting conclusion’s to war-related concepts, cybercriminals have achieved advantages with time-based strategy despite opponent’s superiority in size and available technology. Cybercriminals are unpredictable, rich of imagination and could use standard, cheap equipment to preparations and crime execution. For cybercriminals network crimes offer opportunities and income, while defenders see cybercrimes as troublesome and costly and are that for trying to minimize resources dealing with it in sprit of optimization. This of course could be thought as negligence or lax behaviour, but I claim that this kind of optimization is right and justified – at least from executive’s perspective. As far as person in charge of security in company cannot provide calculations and exact figures of possible losses and threats caused by criminals, resources are not going to grow. Better results could then be achieved in long sight by adopting security in to company’s business processes like budgeting in example. This way company’s cybersecurity could move from reactive mode to predictive role and align security and business goals better.

Personnel’s irresolution could be diminished by adding knowledge and knowledge can be added thru communication, education and training. Better trained, aware persons create faster and more accurate actions in strategic, tactical and operational intent. This is achieved due balanced mind and certainty, and could be concentrated in one word - harmony. Security aware and adequate trained personnel are also capable to execute skilled responses and generate skilled intuitions reducing time between notice, awareness and appropriate reaction to incident.

To sustain harmony throughout the organization and its processes, ISMS support is must-have, rather with support from other business processes to deliver one coherent process model. In practice support from business processes towards security processes is the only way to ensure appropriate resources like money and personnel to proceed with security. Even the OODA loop itself was not found the most suitable solution for longer term management and planning cycles, it is not contradictory to those either.

Adaptation of the OODA loop and the Cynefin framework are recommended and they are found appropriate to support management (planned reactions and actions) and leadership (emerging response) in constantly evolving, changing and emerging situations which reactive situations often are. Specially understanding motivational drivers behind OODA loop might help company to gain stronger security posture.

Most effective resource in cybersecurity field is capable personnel and with adequate, planned and constant training people can make the difference. Especially people need guidance in emerging situations because of human's implicit nature. We are lazy (just like System 2) and not willing to put more effort to anything than it is necessary and here communication is no exception. By having ISMS, you can create structure for security management, its goals and purposes and could communicate it forward to all organizational levels efficiently and in uniform way.

With working ISMS in place, you create touch that security matters are in order. This can and must be communicated to your own organization, as well to customer organizations. While having recognized ISMS in place, it crates trust on which business can further rely. Effectively leaded and organized security structure can be valuable resource helping a company meet its business goals by improving efficiency and aligning with business objectives. Organization can create competitive advantage with better leadership and fluent processes formed with help of the ISMS. To support this, management structures should be existing and be in working order prior implementing the ISMS to gain needed support from top-management. That for my recommendation is that if company aim's for recognized security certificate like ISO27001, company's management structures should be already in place. That could be achieved by implementing the ISO9000 certificate first. Also service management aspect should be recognized before, as security is supporting its processes. So recommended path to integrate the ISMS to business processes goes along management and service processes, like in example described in Figure 12.

Figure 12 Recommended certification path

Concluding previous, implementing Information Security Management System as a part of business processes is necessary if cybersecurity is aimed to be as one of top priorities (main processes) in company. With help of an ISMS sharing same organizational aspects and knowledge can be shared among different interest groups. Proceeding in this is very OODA-like process, even OODA loop itself is not the most suitable for long term planning process as is. If some particular things should be emphasised, those would be need of coherent communication with continuous training and education. These are needed to strengthen security posture in efficient manner in all levels of organization. To gain best results while integrating the ISMS to business processes, management processes should be in place to deliver base for other processes. Secondly company's service processes should be implemented and alongside of those security structures and processes should take place. By doing matters as described security is built in, not glued on top, of business processes.

9.1 Possible topics for further research

During the time consumed writing this thesis several subject for further research raised in mind. For example, research of how BYOD practice has influence on security behaviour in companies that have strong security culture compared to one's which lacking it. As particularly interesting thought, I found research of outsourcings effects to security management processes and security culture in companies which have outsourced their infrastructure.

References

(ISC)². 2009. "Securing the Organization: Creating a Partnership Between HR and Information Security." *The International Information Systems Security Certification Consortium, Inc.* The International Information Systems Security Certification Consortium, Inc. Accessed March 24, 2016. https://www.isc2.org/uploadedfiles/industry_resources/hrwhitepaper.pdf.

Adelman, Clem. 1993. "Kurt Lewin and the Origins of Action Research." *Educational Action Research* (Taylor & Francis Group) 1 (1): 7-24. http://www.tandfonline.com/doi/abs/10.1080/0965079930010102.

Ahonen, Pasi. 2010. *TITAN-käsikirja. VTT:n päätuloksia Tekesin Turvallisuusohjelman TITAN-projektissa.* Research notes, VTT Technical Research Centre of Finland, Espoo: VTT, 152. Accessed July 10, 2014. http://www.vtt.fi/inf/pdf/tiedotteet/2010/T2545.pdf.

Allen, Julia H., Gregory Crabb, Pamela D. Curtis, Brendan Fitzpatric, Nader Mehravari, and David Tobar. 2015. "Structuring the Chief Information Security Officer Organization." *CERT Software Engineering Institute Carnegie-Mellon University.* Carnegie-Mellon University, Software Engineering Institute. September. Accessed March 24, 2016. http://resources.sei.cmu.edu/asset_files/TechnicalNote/2015_004_001_446198.pdf.

Aro, Jessikka. 2015. *Yle Kioski.* Antti Hirvonen. November 9. Accessed March 19, 2016. http://kioski.yle.fi/omat/my-year-as-a-pro-russia-troll-magnet.

Ashford, Warwick. 2013. *Human error causes most data breaches, Ponemon study finds.* June 5. Accessed July 11, 2014. http://www.computerweekly.com/news/2240185378/Human-error-causes-most-data-breaches-Ponemon-study-finds.

Astrachan, Joseph H., Chester W, Richards, Gaia G. Marchisio, and George E. Manners. 2012. "The OODA loop: a new strategic management approach." In *Handbook of Research on Strategy Process*, edited by Pietro Mazzola and Franz W. Kellermanns, 592. Cheltenham: Edward Elgar Publishing Limited.

Bacon, Donald J. 1998. ”Second World War Deception - Lessons Learned for Today's Joint Planner.” *Wright Flyer Paper No. 5.* Air University Press. Alabama: Air Command and Staff College Air University, December.

Bellingcat. 2015. "Bellingcat - by and for citizen investigative journalists." *Bellingcat Investigation – Russia’s Path(s) to War.* Brown Moses Media Ltd. September 21. Accessed March 19, 2016. https://www.bellingcat.com/wp-content/uploads/2015/09/russia_s_path_s__to_war.pdf.

Boyd, John R. 1987. "Organic Design for Command And Control." *Defense and the National Interest Project on Government Oversight - John Boyd Compendium.* Project On Government Oversight (POGO). March. Accessed July 14, 2014. http://www.dnipogo.org/boyd/pdf/c&c.pdf.

Brehmer, Berndt. 2005. "The Dynamic OODA Loop: Amalgamating Boyd's OODA Loop and Cybernetic Approach to Command and Control." *The Command and Control Research Program.* June. Accessed July 14, 2014. http://dodccrp.org/events/10th_ICCRTS/CD/papers/365.pdf.

Candolin, Catharina, interview by Jussi-Pekka Rantanen. 2014. "Specialist: Finland invest to Cybersecurity less than City of Helsinki to rabbit repelling." *Yle News 20.30.* Yle, Finnish national public service broadcasting company. Yle News, Helsinki. July 2. Accessed July 3, 2014. http://areena.yle.fi/tv/2191024.

Chabris, Cristopher, and Daniel J. Simons. 1999. *The Invisible Gorilla.* Accessed March 30, 2016. http://www.theinvisiblegorilla.com/videos.html.

Chin, Adrian. 2015. *The Agency.* June 7. Accessed August 7, 2015. http://www.nytimes.com/2015/06/07/magazine/the-agency.html?_r=0.

Cho, Matthew. 2003. "Mixing Technology and Business: The Roles and Responsibilities of the Chief Information Security Officer." *SANS Institute InfoSec Reading Room.* SANS Institute. Accessed March 24, 2016. http://www.sans.org/reading-room/whitepapers/assurance/mixing-technology-business-roles-responsibilities-chief-information-security-of-1044.

Colwill, Carl. 2009. "Human factors in information security: The insider threat Who can you trust these days?" *Information Security Tech. Report* (Elsevier Advanced Technology Publications Oxford, UK, UK) 14 (4): 186-196. Accessed March 14, 2016. http://dl.acm.org/citation.cfm?id=1860488.

CompTIA, Inc. 2013. "CompTIA 11th Annual Information Security Trends." *Slideshare.* November 16. Accessed July 2, 2014. http://www.slideshare.net/comptia/comptia-11th-annual-information-security-trends#.

CSIS. 2014. *Net Losses: Estimating the Global Cost of Cybercrime.* Report, Santa Clara: McAfee Inc., 24. Accessed June 27, 2014. http://www.mcafee.com/hk/resources/reports/rp-economic-impact-cybercrime2.pdf.

Culnan, Mary J, and Cynthia Clark Williams. 2009. "How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches." *MIS Quarterly* 33 (4): 673-687. Accessed July 10, 2014. http://misq.org/how-ethics-can-enhance-organizational-privacy-lessons-from-the-choicepoint-and-tjx-data-breaches.html?SID=miap7usiak5r515qoevod1p6s5.

Dahlgren, Taina. 2016. "Kaikki ovat pian korkean teknologian yhtiöitä." *Keskisuomalainen* 13. Accessed April 17, 2016.

Davenport, Thomas H. 1992. *Process Innovation: Reengineering Work Through Information Technology.* Boston, MA: Harvard Business School Press.

ENISA. 2012. "Return on Security Investment." *ENISA Investing in Security for ROI?* December 12. Accessed March 24, 2016. https://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment.

European Commission. 2013. "Organised crime & Human trafficking." *European Commission.* August 29. Accessed June 26, 2014. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime/index_en.htm.

European Commission. 2012. "Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre." *Communication from the commission to the Council and the European Parliament - Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre.* Brussels: European Commission, March 28.

http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/pdf/communication_european_cybercrime_centre_en.pdf#zoom=100.

Financial Times. n.d. *Definition of strategic communication.* Accessed July 24, 2015. http://lexicon.ft.com/Term?term=strategic-communication.

Florêncio, Dinei, and Cormac Herley. 2011. *Sex, Lies and Cyber-crime Surveys.* Technical Report, Communication and Collaboration Systems, Redmond: Microsoft Research, 11. Accessed June 27, 2014. http://research.microsoft.com/apps/pubs/default.aspx?id=149886.

Gartner, Inc. 2016. *Gartner IT Glossary - Small and Midsize Business (SMB).* Accessed April 5, 2016. http://www.gartner.com/it-glossary/smbs-small-and-midsize-businesses.

Gercke, Marco. 2012. "Understanding cybercrime: Phenomena, challenges and legal response." *International Telecommunication Union.* September. Accessed July 11, 2014. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf.

Ginos, Nathan D. 2010. "The Securitization of Russian Strategic Communication." *A Monograph.* Fort Leavenworth, Kansas: School of Advanced Military Studies United States Army Command and General Staff College, December 2nd. http://www.dtic.mil/dtic/tr/fulltext/u2/a536578.pdf.

Gordon, Lawrence A., Martin P. Loeb, William Lucyshyn, and Lei Zhou. 2015. "Increasing cybersecurity investments in private sector firms." Edited by Tyler Moore and David Pym. *Journal of Cybersecurity* (Oxford University Press) 0 (2015): 1-15.

Greenwald, Glenn. 2013. "Edward Snowden: the whistleblower behind the NSA surveillance revelations." *The Guardian.* June 6. Accessed 6 26, 2014. http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

Grossman, Wendy M. 2014. "Secure Giving: Information Security Challenges in the Third Sector." *Infosecurity .* February 13. Accessed July 21, 2014. http://www.infosecurity-magazine.com/view/36918/secure-giving-information-security-challenges-in-the-third-sector/.

Hakkarainen, Pasi. 2014. ”Cyber Weapon Target Analysis.” Jyväskylä: Jyväskylä University of Applied Sciences, 15. March.

Hammond, Grant T. 2004. *The Mind of War John Boyd and American Security.* Edited by Lorraine Atherton. Washington, Washington D.C.: Smithsonian Books.

Hasik, James. 2012. "Beyond Hagiography - Theoretical and Practical Problems in the Works and Legacy of John Boyd." Vers. 2.4. *James Hasik Industrial analysis for global security.* May 15. Accessed August 13, 2015. http://www.jameshasik.com/weblog/2012/10/beyond-hagiographymy-paper-at-the-2012-boyd-beyond-symposium.html.

Heiskanen, Mikko. 2016. *Cybersecurity is a team sport.* Video lecture. Prod. Aalto University School of Electrical Engineering. Espoo: Department of Communications and Networking, April 12.

House of Commons Defence Committee. 2013. *Defence and Cyber-security; Sixth Report of Session 2012–13, Volume I.* Public report, London: Stationary office limited. Accessed July 9, 2014. http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/106/106.pdf.

IBM Corporation. 2014. *IBM Security Services 2014 Cyber Security Intelligence Index.* Research report, IBM Global Technology Services, Somers: IBM, 10. Accessed July 11, 2014. http://public.dhe.ibm.com/common/ssi/ecm/en/sew03039usen/SEW03039USEN.PDF.

ICC. 2015. "ICC Cyber security guide for business." *International Chamber of Commerce Advocacy Codes and Rules.* International Chamber of Commerce (ICC). Accessed April 12, 2016. http://www.iccwbo.org/Advocacy-Codes-and-Rules/Areas-of-work/Digital-Economy/Cyber-Security-Guidelines-for-Business/ICC-Cyber-Security-guide-for-business/.

Information Services Group. 2016. *ISG Outsourcing Index®: Industry Ends Year on High Note.* January 14. Accessed March 24, 2016. http://www.isg-one.com/web/media-center/press/160114-US.asp.

ISACA. 2009. "An Introduction to the Business Model for Information Security." *ISACA IT Professional Networking and Knowledge Center.* Information Systems Audit and Control Association, Inc. Accessed April 4, 2016. http://www.isaca.org/knowledge-center/bmis/documents/introtobmis.pdf.

ISO. 2011. "ISO/IEC 20000-1:2011(en)." *ISO Online Browsing Platform.* The International Organization for Standardization. Accessed May 5, 2016. https://www.iso.org/obp/ui/#iso:std:iso-iec:20000:-1:ed-2:v1:en.

ITSMF. 2009. *ITIL V3 Foundation Handbook.* Second edition. London: The Stationery Office.

Jaakonaho, Jussi. 2010. "Zenbundit.com." *Guest Post: Shipman on Boyd and Beyond, 2010.* October 15.-16. Accessed August 12, 2015. http://zenpundit.com/?p=3573.

JAMK University of Applied Sciences. 2014. *Study Guide Master's Degrees.* Accessed July 14, 2014. http://studyguide.jamk.fi/en/Study-Guide-Masters-Degrees/Studying-at-jamk/masters-thesis/.

Jantunen, Saara. 2013. "Strategic communication : practice, ideology and dissonance." *National Defence University Department of Leadership and Military Pedagogy Publication Series 1: No. 11.* no. ISBN:978-951-25-2489-1. Helsinki: National Defence University, August 2. 216. Accessed February 23, 2015. http://urn.fi/URN:ISBN:978-951-25-2489-1.

Jirasek, Vladimir. 2012. *Security Think Tank: Outsourcing of IT security is not for everyone.* May 3. Accessed July 9, 2014. http://www.computerweekly.com/opinion/Security-Think-Tank-Outsourcing-of-IT-security-is-not-for-everyone.

JUHTA. 2012. "JHS suositukset - JHS152." *JUHTA - Julkisen hallinnon tietohallinnon neuvottelukunta.* JUHTA Advisory Committee On Information Management in Public Administration. October 5. Accessed April 4, 2016. http://www.jhs-suositukset.fi/web/guest/jhs/recommendations/152.

Juster, Robert-Paul, and Marie-France Marin. 2011. "Genetics and Stress: Is there a link?" *Mammoth Magazine, Issue 9, January 2011.* Centre for studies on human stress (CSHS) . January. Accessed August 22, 2015. http://www.humanstress.ca/documents/pdf/Mammouth%20Magazine/Mammoth_vol9_EN.pdf.

Kahneman, Daniel. 2011. *Thinking, Fast and Slow.* London: Penguin Books.

Keppel, John. 2014. *Outsourcing 2014: The New Normal.* February 6. Accessed July 9, 2014. http://www.cioinsight.com/print/it-management/expert-voices/outsourcing-2014-the-new-normal.html.

Kurtz, Cynthia F., and David J. Snowden. 2003. "The new dynamics of strategy: Sense-making in a complex and complicated world." *IBM Systems Journal* (The International Business Machines Corporation (IBM)) 42 (3): 462-483.

Lenane, Dean. 2013. *Deming collaboration.* October 6. Accessed July 14, 2014. http://demingcollaboration.com/pdsa-ooda/.

LIGO Caltech. 2016. *LIGO Laboratories.* February 11. Accessed march 20, 2016. https://www.ligo.caltech.edu/news/ligo20160211.

Limnéll , Jarno. 2016. *Kansanedustajien arvioita Suomen kyberturvallisuuden nykytilasta ja tulevaisuudesta.* Research, Department of Communications and Networking, Aalto University, Helsinki: Unigrafia Oy, 28. http://urn.fi/URN:ISBN:978-952-60-6687-5.

Lotila, Sami. 2016. "Viestinnän professori Anu Kantola: "Sote meni sekoiluksi"." *Suur-Jyväskylän Lehti*, April 20: 14-15.

Merriam-Webster Dictionary. n.d. *Merriam-Webster Online Dictionary.* Merriam-Webster Incorporated. Accessed March 19, 2016. http://www.merriam-webster.com/dictionary/decision%20making.

Merriam-Webster Incorporated. n.d. *Merriam-Webster dictionary.* Accessed March 27, 2016. http://www.merriam-webster.com/dictionary/hypothesis.

Merrit, Marian. 2013. "Norton Report Finds Higher Cybercrime Costs per Victim, Social Stressors and Blurred Lines." *Norton Community : Norton Blogs : Ask Marian.* October 1. Accessed July 1, 2014. http://community.norton.com/t5/Ask-Marian/Norton-Report-Finds-Higher-Cybercrime-Costs-per-Victim-Social/ba-p/1030435.

Moen, Ronald. 2009. "Foundation and History of the PDSA Cycle." *The W. Edward Deming Institute.* September 17. Accessed March 25, 2016. https://www.deming.org/sites/default/files/pdf/2015/PDSA_History_Ron_Moen.pdf .

Morgan , Steve. 2016. *Bank of America's Unlimited Cybersecurity Budget Sums Up Spending Plans In A War Against Hackers.* January 27. Accessed April 13, 2016. http://www.forbes.com/sites/stevemorgan/2016/01/27/bank-of-americas-unlimited-cybersecurity-budget-sums-up-spending-plans-in-a-war-against-hackers/#4ad0440c434b.

Morgan, Steve. 2015. *Cybersecurity Market Reaches $75 Billion in 2015.* December 20. Accessed April 13, 2016.

http://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#4bf38ec62191.

Nutt, Paul C. 2002. *Why decisions fail: Avoiding the Blunders and Traps That Lead to Debacles.* 1st. San Fransisco, California: Berrett-Koehler Publishers.

Osinga, Frans P.B. 2006. *Science, Strategy and War.* Taylor & Francis e-Library.

Overbye, Dennis. 2016. *The New York Times.* Edited by Margaret Sullivan. The New York Times Company. February 11. Accessed March 19, 2016. http://www.nytimes.com/2016/02/12/science/ligo-gravitational-waves-black-holes-einstein.html?_r=0.

Pelnekar, Charu. 2011. "Planning for and Implementing ISO 27001." *ISACA Journal* (ISACA) 4: 28-35.

Philips, Mike. 2003. "Using a Capability Maturity Model to Derive Security Requirements." *SANS Reading Room Best Practices.* March 13. http://www.sans.org/reading-room/whitepapers/bestprac/capability-maturity-model-derive-security-requirements-1005.

Ponemon Institute LCC. 2014. *2014 Cost of Data Breach Study: Global Analysis.* Benchmark report, Traverse City: Ponemon Institute LCC.

Ponemon Institute LLC. 2013. *2013 Cost of Cyber Crime Study: Global Report.* Benchmark report, Traverse City: Ponemon Institute. Accessed June 26, 2014. http://www.hpenterprisesecurity.com/ponemon-2013-cost-of-cyber-crime-study-reports.

Ponemon Institute LLC. 2015. *2015 Cost of Cyber Crime Study: Global.* Research Department, Ponemon Institute LLC, Traverse City, Michigan: Ponemon Institute LLC, 29.

Porvari, Paavo. 2013. *Tietoturvallisuus liiketoiminnan johtamisessa, prosesseissa ja henkilöiden toiminnassa.* 2nd Edition. Helsinki: Unigrafia Oy.

Prior Konsultointi Oy. 2016. "Tutkimus - Jopa 6000 PK-yritystä on joutunut tietomurron uhriksi." March 18. Accessed April 1, 2016. http://hub.elisa.fi/jopa-6000-pk-yritysta-joutunut-tietomurron-uhriksi/.

Richards, Chet. 2012. "Boyd's OODA Loop (It's not what you think)." *J. Addams & Partners, Inc.* March 21. Accessed August 23, 2015. http://www.jvminc.com/boydsrealooda_loop.pdf.

Riihijärvi, Petri. 1999. "Operaatioiden suunnittelu ja johtaminen - Tarkastelua suomalaisen, yhdysvaltalaisen ja venäläisen johtamisprosessin näkökulmasta." *Tiede ja Ase* (The Finnish Society of Military Sciences) 57 (1999): 115 - 141. Accessed March 31, 2016. http://ojs.tsv.fi/index.php/ta/article/view/47820.

Robinson, Neil et. al. 2012. *Feasibility study for European Cybercrime Centre.* Feasibility study, Directorate General Home Affairs, Directorate Internal Security , European Commission, Cambridge: Rand Europe. Accessed June 26, 2014. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/pdf/20120311_final_report_feasibility_study_for_a_european_cybercrime_centre_en.pdf#page=1&zoom=100.

Russian Federation. 2000. *Information Security Doctrine of the Russian Federation.* September 9. Accessed July 24, 2015. http://archive.mid.ru//bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument.

Salonius-Pasternak, Charly, and Jarno Limnéll. 2015. "Finnish Institute of International Affairs." *Preparing Finland for hybrid warfare.* no. 6/2015. Helsinki: Finnish Institute of International Affairs, February. http://www.fiia.fi/fi/publication/488/preparing_finland_for_hybrid_warfare/.

Schneier, Bruce. 2002. "The case for outsourcing security." *Computer* (IEEE) 35 (4): 20-26. Accessed July 10, 2014. doi:10.1109/MC.2002.1012426.

Secretariat of the Security Committee. 2013. "Finland's Cyber security Strategy." *Government Resolution - Finland's Cyber security Strategy.* Helsinki: Ministry of Defence, January 24. Accessed June 27, 2014. http://www.defmin.fi/en/publications/strategy_documents/finland_s_cyber_security_strategy.

SFS. 2013 a. ”Information technology. Security techniques. Information security management systems. Requirements.” *SFS-ISO/IEC 27001:2013.* Helsinki: The Finnish Standards Association SFS, 9. December.

SFS. 2013 b. "Information technology. Service Management. Part 1: Service management system requirements." *SFS-ISO/IEC 20000-1:2011.* Helsinki: The Finnish Standards Association SFS, December 9.

SFS. 2010. *SFS-ISO/IEC 27000.* Vol. 1st, in *SFS-Käsikirja 327*, by The Finnish Standards Association SFS, translated by Jari Flyktman, 7-30. Helsinki: The Finnish Standards Association SFS.

Siponen, Mikko T. 2000. ”A conceptual foundation for organizational information security awareness.” *Information Management & Computer Security* (Emerald Group Publishing Limited) 8 (1): 31-41.

Snowden, David. 2014. *Cynefin as of 1st June 2014.* Accessed March 30, 2016. Own work. https://commons.wikimedia.org/wiki/File:Cynefin_as_of_1st_June_2014.png.

Snowden, David, and Mary E. Boone. 2007. "A Leader’s Framework for Decision Making." *Harvard Business Review.* November. Accessed March 25, 2016. https://hbr.org/2007/11/a-leaders-framework-for-decision-making.

Statistics Finland. N.A. *Concepts and definitions, Small and mediumsize enterprises.* Accessed March 27, 2016. http://www.stat.fi/meta/kas/pienet_ja_keski_en.html.

Symantec Corporation. 2013. "2013 Norton Report: Cost per Cybercrime Victim Up 50 Percent." *Symantec Press Releases.* October 1. Accessed July 2, 2014. http://www.symantec.com/about/news/release/article.jsp?prid=20131001_01.

Symantec Corporation. 2015. "2015 Internet Security Threat Report, Volume 20." *Symantec Security Center Security Response Publications.* April. Accessed March 2, 2016. https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf.

Takala, Tuomo. 1999. *Liikkeenjohdon kehityshistoria.* Second. Translated by Jari Flyktman. Jyväskylä: Atena kustannus Oy.

The International Chamber of Commerce (ICC). 2015. "The ICC Cyber security guide for business." *The International Chamber of Commerce (ICC).* Accessed April 2, 2016. http://www.iccwbo.org/Advocacy-Codes-and-Rules/Areas-of-work/Digital-Economy/Cyber-Security-Guidelines-for-Business/ICC-Cyber-Security-guide-for-business/.

The Oxford Dictionaries. n.d. *The Oxford Dictionaries.* Accessed March 31, 2016. http://www.oxforddictionaries.com/definition/english/perception.

The Oxford Dictionary. n.d. *Oxforddictionaries.com.* Accessed March 29, 2016. http://www.oxforddictionaries.com/definition/english/confidence.

Thomas, Timothy L. 2004. "Russia's Reflexive Control Theory and the Military." *The Journal of Slavic Military Studies* (Routledge, Taylor & Francis Group) 17 (2): 237-256.

ThreatTrack Security. 2013. *Majority of Malware Analysts Aware of Data Breaches Not Disclosed by Their Employers.* November 6. Accessed July 2, 2014. http://www.threattracksecurity.com/press-release/majority-of-malware-analysts-aware-of-data-breaches-not-disclosed-by-their-employers.aspx.

U.S. Department of Homeland Security. 2013. "Cyber Risk Culture Roundtable Readout Report." *Official Website of the Department of Homeland Security.* Edited by National Protection and Programs Directorate. May. Accessed July 2, 2014. http://www.dhs.gov/sites/default/files/publications/Cyber%20Risk%20Culture%20Roundtable%20Readout%20Report.pdf.

Ullmann, David. 2007. ""OO-OO-OO!" The Sound of Broken OODA Loop." *Crosstalk The Journal of Defense Software Engineering* (USAF Software Technology Support Center) 20 (4): 22-25. Accessed July 15, 2014. http://www.crosstalkonline.org/storage/issue-archives/2007/200704/200704-0-Issue.pdf.

United Nations. 2013. *Comprehensive Study on Cybercrime.* Draft report for open-ended intergovernmental expert group on cybercrime, United Nations Office on Drugs and Crime (UNODC), New York: United Nations, 320. Accessed June 30, 2014. http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

Woolridge, Bill, and J. Ignacio Canales. 2010. "Managerial interplay: linking intent to realized strategy." In *Handbook of Research on Strategy Process*, by Pietro Mazzola and Frantz W. Kellermanns, 207 - 239. Cheltenham: Edward Elgar Publishing Limited.

World Economic Forum. 2016. "The Global Risks Report 2016." *The World Economic Forum.* The World Economic Forum. Accessed March 12, 2016. http://www3.weforum.org/docs/GRR/WEF_GRR16.pdf.

Xu, Heng, Tamara Dinev, H. Jeff Smith, and Paul Hart. 2008. "Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View." *ICIS 2008 Proceedings. Paper 6.* AIS Electronic Library. 16. Accessed July 10, 2014. http://aisel.aisnet.org/icis2008/6.

Yadron, Danny. 2014. *Companies Wrestle With the Cost of Cybersecurity.* February 25. Accessed April 13, 2016. http://www.wsj.com/articles/SB10001424052702304834704579403421539734550.