TALLINN UNIVERSITY OF TECHNOLOGY

Faculty of Information Technology

Department of Computer Engineering

IDK70LT

Jesse Deboise Wojtkowiak II

ADDRESSING INSIDER THREAT VECTORS IN AN INFORMATION SOCIETY

Master's Thesis in Cyber Security

Alexander Norta

TU-Eindhoven

Associate Professor at Tallinn University of Technology

Mauno Pihelgas

Tallinn Technical University

Doctorate Candidate Tallinn Technical University

Tallinn 2015

Author’s declaration of originality

Author’s declaration of originality is an essential and compulsory part of every thesis. It always follows the title page. The statement of author’s declaration of originality is presented as follows:

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Jesse Deboise Wojtkowiak II ……

(Signature, date)

Student’s code: 132127

Student’s e-mail address: jesse.wojtkowiak@gmail.com

Supervisor Associate Professor Alexander Norta:

The thesis conforms to the requirements set for the master’s theses

……

(Signature, date)

Supervisor Mauno Pihelgas:

The thesis conforms to the requirements set for the master’s theses

……

(Signature, date)

Chairman of defense committee:

Permitted to defense

……

(Title, name, signature, date)

Abstract

Insider threats are becoming more common and with devastating consequences. Espionage in the information age has become the vocation of everyday citizens. Estonia is a nation committed to e-governance and the development of its information society. Is their information security management systems doing enough to protect Estonian's e-government and information society from insider threats? This research uses triangulation methodology to make qualitative analysis of three aspects of Estonians insider defense. The artifacts of interest are Estonia's information security management systems, Riigi Infosüsteemi Amet (Estonia's information systems authority), and historical insider cases. They will be examined beside the insider threat profiles provided by CERT Carnegie Mellon and their supporting research. It was determined that CERT profiles provide valuable information lacking from current information security management systems. Riigi Infosüsteemi Amet's operating and personnel profile match CERT profiles and are suitable for further analysis. Lastly that espionage is a considerable threat for the Estonian state and that insider threat programs have capabilities that help address this issue. Initial research indicates that Estonia's information security management system does provide an elite level of protection, but is not as robust as the possibilities offered by an insider threat program. Based on research results the author recommends five actions pursuing the possibilities offered by insider threat programs to enhance the nation's security profile.

This thesis is written in English and is 69 pages long, including seven chapters, one figure and three tables.

Annotatsioon

Sisemiste ohuvektorite haldamine infoühiskonnas

Siseohud on sageduselt, mõjult ning kahjult kasvav probleem ja nende tagajärjed on laastavad. Eesti riik, kes on pühendunud E-riigi ja oma infoühiskonna arendamisele, teeb seda ajastul, mil spionaaž on muutunud tavakodanike tegevuseks. Kas olemasolevad infoturbe haldussüsteemid on piisavad, et kaitsta Eesti E-riiki ja infoühiskonda siseohtude eest? Käesolev uurimustöö on kvalitatiivne analüüs Eesti riigi võimekusest sisemisi ohte hallata. Uurimistöö huviorbiidis olevad objektid on Eesti infoturbe haldussüsteemid, Riigi Infosüsteemi Amet ja varasemad siseohuga seotud juhtumid. Autor kõrvutab need CERT Carnegie Melon poolt koostatud siseohu kirjeldustega ja sellekohaste uuringutega. Leitakse, et CERT ohuprofiilid pakuvad väärtuslikku lisainfot, mis olemasolevatest infoturbe juhtimise süsteemidest puudu on. Tuvastatakse, et Riigi Infosüsteemi Ameti tegevuse ja personali profiilid vastavad CERT profiilidele ja on seega edasise analüüsi jaoks sobilikud. Spionaaž on märkimisväärne oht Eesti riigi turvalisusele ja väljapakutud siseohu programmid pakuvad võimalusi, mis on abiks selle probleemiga tegelemisel. Analüüs näitab, et Eesti infoturbe haldussüsteem pakub kõrgetasemelist kaitset, kuid ei ole piisavalt mitmekülgne võrreldes võimalustega, mida pakub siseohu programm. Tuginedes analüüsi tulemustele pakub autor pakub välja viis soovitust, et viia Eesti riigi infoturve järgmisele tasemele.

Käesolev uurimustöö on kirjutatud inglise keeles, on 69 lehekülge pikk, koosneb seitsmest peatükist ning ühest joonisest ja kolmest tabelist.

Terms

Ambitious Leader: a leader of an insider crime who recruits insiders to steal information for some larger purpose. [1]

Entitled Independent: an insider acting primarily alone to steal information to take to a new job or to his own side business. [1]

Insider IT sabotage: insider incident in which the insider uses information technology (IT) to direct specific harm at an organization or an individual. [1]

Insider theft of intellectual property (IP): an insider's use of IT to steal proprietary information from the organization. This category includes industrial espionage involving insiders. [1]

Intellectual property: intangible assets created and owned by an organization that are critical to achieving its mission.

Insider Fraud: an insider's use of IT for the unauthorized modification, addition, or deletion of an organization's data (not programs or systems) for personal gain, or the theft of information that leads to an identity crime (identity Theft, credit card fraud) [1]

Identity Theft: the misuse of personal or financial identifiers in order to gain something of value and/or facilitate some other activity. [2]

Malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems. [1]

Personal Identifiable Information (PII) - information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, including any other personal information which is linked or linkable to a specified individual. [3]

Abbreviations

BSI	Federal Office for Information Security (Germany)
CERT	Computer emergency response team
CIA	Central Intelligence Agency
CMU	Carnegie Mellon University
CNSS	Committee on National Security Systems
DOD	Department of Defense
DoE	Department of Energy
EDPI	Estonian Data Protection Inspectorate
ETCB	Estonian Tax and Custom Board
FIMSA	Federal Information Security Modernization Act
GaaS	Government as a Platform
ICD	Internal Controls Department
INSA	Intelligence and National Security Alliance
InTP	Insider Threat Program
ISKE	Information baseline security system
IS	Information Security
ISMS	Information Security Management System
IT	Information technology
KAPO	Kaitsepolitseiamet (Internal Intelligence Agency)
MGDT	Multi-grounding of design theories
NIST	National Institute of Standards and Technology

NRC	Nuclear Regulatory Commission
NTAC	National Threat Assessment Center
PDPA	Personal Data Protection Act
PII	Personal Identifying Information
RIA	Riigi Infosüsteemi Amet (Information System Authority)
SEI	Software Engineering Institute

Table of contents

List of figures

List of tables

1. Introduction

1.1. Thesis motivation

Modern day organizations are becoming more and more networked and therefore dependent on one another [4]. These connections are not only the ease at which communication happens between the people of an organization, but also the velocity and ease at which their businesses process interconnect to produce their products [4]. Financial systems are the quintessential example. From consumer banking to private banking, and the exchanges that provide access to stocks, bonds, and commodities; these institutions and their services depend on being connected and communicating electronically. Banking is not the only example of service institutions that are vulnerable to disruption in the communication network. Essentially, the network is the economy [5].

Estonia, a nation heavily dependent on cyber infrastructure to provide many of its government's services, [6] was the target of a cyber-attack in 2007. Though the disruptions centered on a denial of service attack, and actual damage was minor, the disruption was significant. This provided a wakeup call for any organization that depended on this type of infrastructure in their day to day operations. It was argued by Rain Ottis in the Proceeding of the 7th European Conference on Information Warfare and Security in 2008 that such an event should be considered a threat to national security [6].

Eight years later, the dependence of the world's economy on networked Information Technologies (IT) has only increased [7]. The increased use of IT in every aspect of life has also increased the attack surface for cybercrime [8]. There is no end to statistics and surveys that tell the story of an epidemic of sorts [9] [10] [11] [12]. This is not to say that IT is defenseless. The industry has evolved. Firewalls, IPS, antivirus, Web filtering have all been developed and are in the midst of evolving again to become more useful tools that will help organizations lower their risk of a cyber incident. Additionally various frameworks have evolved to help organizations understand and address these issues from a strategic level [13] [14] [15] [16]. Defense in depth being a common strategy for achieving some level of Information Assurance (IA). The application of defense in depth is a best practices approach to achieving an organizations strategic goals [17] .

Despite the resources spent, easy money at a low cost and risk has only stimulated the growth of cybercrime and the damage that is inflicted [18]. Networked infrastructure is

becoming more secure, treats continue to evolve and continue to rise to the challenge that is offered with every new defensive technology. In essence, a cyber arms race ensues [19] [20]. It is reported that in 2007 that of 774 cases, malicious outsiders constituted 56.48% of incidents, malicious insiders made up 15.45% of all losses, while accidental loss (Unintentional Insiders) constituted 23.95% [21]. To date, the 2015 report has very similar percentages with a notable increase in events; malicious outsiders at 59.9%, accidental loss 22.58%, and malicious insiders 13.34%, spanning 1099 events [21]. Various sources report a resistance by organizations to report incidents [22] [23] [24] as this can also damage the organization [25] and the general health of society. What is clear from the statistics is that the largest threat surface is the infrastructure. Appropriately, the greatest efforts have been spent developing technologies, procedure, and methodologies to address the greatest percentage of weaknesses. Those presented by outsiders. Insider threats both malicious and non-malicious may have been seen as behavior no different than what took place before the introduction of networked communication. For non-malicious cases, or accidents, cyber training has been the accepted control across industry and government alike. Training works, but the result of training has not solve the problem or address the malicious insider. In large, malicious insiders can be prevented or detected early by implementing IS best practices [25]. While this is encouraging, CERT identified the need for a formalized process to address insider events [26].

An increase in reporting is noted and may indicate a shift in culture [21]. It also indicates that the number of threats has increased across the spectrum. Training has not helped to decrease the losses to unintentional insiders, if in fact those incidents are unintentional. Most concerning is that the number of intentional insiders has also increased, though not by percentage. This may be in response to organizations continuously improving their outward facing defenses. 74% of respondents to a 2014 SANS survey stated they are most concerned about negligence and the malicious insiders [27]. No matter what they may be spending or how well-run the IS program may be, their concern speaks loudly to a problem they know exists and are not adequately prepared for.

Information technology still advances today. The affects are both positively and negatively disruptive, and extremely profitable. The unintended and intended benefits that organizations reap from using this technology also creates similar benefits for malicious agents. The more dependent an organization is on the technology, the more vulnerable

they are to the technology. This creates a sense of empowerment in people. The newfound sense of empowerment has a significant sociotechnical [28] impact. Perhaps a useful metaphor that will describe this shift is that of H.G. Wells, “The Invisible Man.” The book raises a simple question; what are a human’s behavioral constraints when they cannot be seen? As you may guess, in some cases there is no restraint from moral or social norms that would otherwise guide our behavior in our day to day lives. With modern IT equipment the ability and ease at which information is duplicated, transferred, or destroyed, sets a fertile ground for insiders to operate. The author believes that the increase in the number of insider cases is an indication of a sociotechnical shift in the culture of today’s work environment. The belief by employees or agents is that they can act invisibly. Simply there is no mechanism in place to discipline the sociotechnical cultural shift that has taken place in the workplace.

The goal of this thesis is take a critical look at Estonia’s information society and the fruits of e-governance to determine what threat is posed by the insider threat vector. As insider threats are a managed risk in IS programs a comparison will be made to research developed from the Computer Emergency Response Team (CERT) division of the Software Engineering Institute (SEI) at Carnegie Mellon University (CMU) with regard to the Estonian situation. This thesis project offers the theory that an insider threat program addresses security risks that exist to Estonia’s national infrastructure which are not currently being considered. Insider threat programs are a relatively new paradigm in the struggle to provide IS. The insider threat has been studied in many useful and thoughtful ways that provide artifacts to currently existing IS programs. CERT at CMU has contributed extensively to this body of knowledge. CMU’s work is the foundation on which Insider Threat Programs (InTP) have been built.

1.2. Rational

Estonia is many way presents a challenge to study. It is lacking numbers for empirical scale in virtually every way to make it interesting to study or to have the results appreciated and accepted by the scientific community. Despite this, Estonia remains unique in many ways and therefore merits a look. A case in point is e-governance and the information society that Estonia has built. The greatest value to the rest of the world is how they did it. If a small country that has limited human, natural, and financial resources can create a world class model for e-governance it provides hope to the possibility that

such a success can be duplicated by nations with more of everything. The author would argue that such an accomplishment by a rich country is not such a tremendous feat or of interest to most nations of the world as they have providence of resource. Today the information security management system (ISMS) that is used may not provide the same level of protection offered by an insider threat program. This study is meant to gain clarity on how Estonia protects what they have built from insider threats and determine if additional protection is warranted.

1.2.1. Scope

This purpose of this research is to determine if an Insider Threat Program offers a degree of protection that is not being addressed by current insider threat detection methods.

1.2.2. The case

When the case study started the focal point was that of the e-residency program that has recently been added to the plethora of services that Estonia currently offers. This particular services is specifically for none Estonians who would like to gain e-residency for business purposes, allowing them access to European markets. It was quickly identified that the e-residency is not the most interesting vector for insiders and that Estonia may actually have greater concerns.

1.3. Methodology, theory, and research questions

This research will be a case study built along the guidelines of “Case Study Research in Software Engineering: Guidelines and Examples” [29]. When developing this thesis considerable difficulty in choosing an appropriate methodology for research was experienced due to the importance of behavior science in the research and deployment of InTP’s. Insider threats remain a behavioral problem no matter the number of technical indicators that are developed and implemented to detect them. A key point; information security programs allow the detection of insider activities, integration of these indicators with behavior indicator allow organizations to move from reacting to incidents to the prevention of incidents. In time, a well-developed suite of socio-technical indicator will provide predictive risk indicators which allow an organization to focus its limited resources on the riskiest people. It is because of the dependence of InTP on technical

indicators that are developed in information science, that a software engineering format was chosen.

1.3.1. Methodology

The case study for this research is the Estonian e-governance program. This includes the technical infrastructure that makes it possible as well as the organizations that support and develop the infrastructure. A triangulation methodology will be employed using alternative viewpoints developed during the research. Inductive reasoning will be applied to the empirical data that is developed to prove the theory.

The first set of data will be developed by comparison of the Federal Office for Information Security (Germany), or BSI model, to insider profiles. From this comparison a determination will be made if there is a difference in what an ISMS and InTP provide in the form of protection from insiders. As all organization on the X-Road are required to have ISKE implemented a weakness in the ISMS would constitute a weakness implemented throughout the entire existing infrastructure.

The second aspect of this case study will be to examine the X-Road and the role Riigi Infosüsteemi Amet (Information System Authority) RIA plays a key role in its development and protection. Though there are many other organizations, companies, agencies that are involved in e-governance the X-Road spans them all. In an effort to keep this work within scope it was felt that a weakness of the X-Road indicates a weakness that spans all the services provided along the X-Road.

The third aspect of triangulation for this thesis will be an examination of empirical data provided by the Estonia government. During this research attempts have been made to interview with various government agency to include the Estonian Police and Boarder Guard Board (PBGB) and Estonian Tax and Custom Board (ETCB). Though contact was made, access to key knowledge holders was not possible, limiting the amount of empirical data that could be applied in this section of the research. Statistic for privacy violations were drawn from the Estonian Data Protection Inspectorate EDPI annual reports. Kaitsepolitseiamet (KAPO, Estonian Internal Security Service) provided the information concerning cases of Espionage. Application of the insider profiles to these cases will also be used to determine if an InTP offer anything of value to Estonia’s current information security posture.

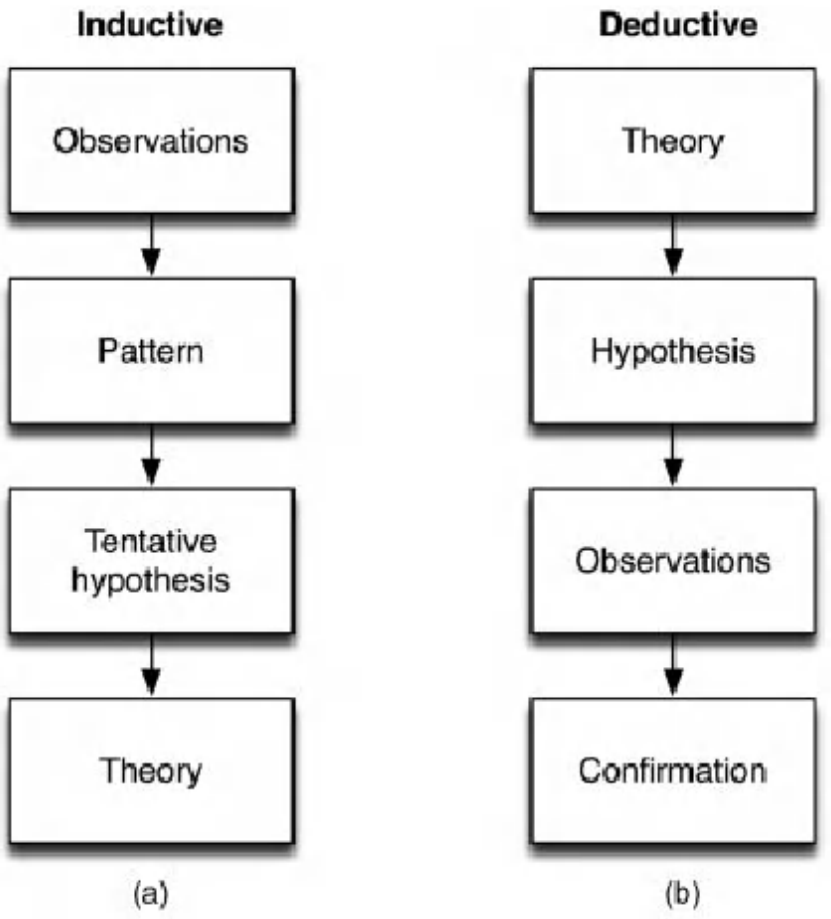

Figure 1. Inductive (a) and deductive (b) approaches to empirical research [29].

1.3.2. Theory

As this research will employ inductive reasoning, tentative hypothesis will be included at the end of each chapter, and any theories consequent of this research will be presented in the summary of this paper.

1.3.3. Research questions

The main research question is: Does an InTP provide a level of protection against insiders that improves Estonia's current security posture?

The research question that are used to support chapter research triangulation are:

RQ1: How do CERT profiles identify insider threats differently than protection currently offered by the current ISMS?

RQ2: Does RIA's operational profile appear to match any of the CERT profiles?

RQ3: What previous incidents can be found that indicate insider threats are an issue for Estonia?

1.4. Proposition

The following proposition questions are forwarded to aid in the development of tentative hypothesis.

RP1.0: If insider profiles identify insider threats in a more precise way, then information security programs can implements better controls to address insider threats.

RP2: If RIA's operational profiles do match the insider threat profiles, then RIA may have reason for concern and a deeper study is warranted.

RP3: If previous insider incidents are found to compliment the insider threat profiles, then an InTP are programs that will address insider threats in a more precise method than is currently being utilized.

1.5. Defines concepts and measures

The insider profiles presented provide the qualitative standard by which threats defined by BSI will be compared to. The Insider threat profiles are based on CERT research. CERT has over 1000 cases in their insider database which represents the largest collection of data in this field of study. A qualitative comparison will be made to determine to what degree the profile fits or does not fit the individual case.

1.6. Methods of data collection

Data collection at each chapter will be a qualitative comparison. Information will be drawn from open source documents. This information will then be considered against the profiles from figure 2.1.

Chapter 3 will cover the comparison of the ISMS used by Estonia. In this section the profiles are being compared to existing literature to determine which is more useful in understanding the insider threat and creating technical indicators to find the threat.

Chapter 4 will address RIA and determine which profiles are of concern to that organization. Individual traits will be compared to determine if the profile fits the organization. An absolute match is not needed to indicate that the profile does or does not fit their organizational need.

Chapter 5 will be the application of the profiles to previous cases that have occurred in Estonia. EDPI provides some statistics that are of value. In particular they have list complaints received, misdemeanors, and fines. Additionally cases provided by KAPO will also be compared to see if a trend along the CERT profiles exists.

1.7. Methods of data analysis

The quantity of data available is limited. This constraint will be overcome by determining if current empirically established profiles are useful in discriminating the Estonian situation. A useful profile simply is a positive indication. A profile that was not useful must be further investigated to determine why and is not necessarily a negative indication. A profile that does not apply may indicate the type of operation that the organization is preforming. If no profiles apply the case it may be a negative indicator.

The results will then be compared to determine the strength of each case against the results. A theory on the applicability of insider threat programs for Estonia will then be presented.

1.8. Case selection strategy

Cases have been selected due to their open source availability. The Estonian ISMS, ISKE is only available in the Estonian language and was therefore a direct assessment of the threats provided could not be accomplished. As the ISKE system was in large part an adaption of the German BSI system those threats descriptions will be used to complete the assessment.

RIA was selected to apply the CERT profiles to as they provide the data backbone that Estonia's e-governance relies on. RIA is the foundation on which to work from. The majority of insider threats that have been discussed are United States centric. There is also supporting documentation concerning insider activity in Western Europe nations but again this is reported by US sources [30]. The selection of Estonian insider activity is

primarily to determine if enough information is available from open source intelligence to determine if US centric information is actually relevant to the Estonian situation. If these cases do reflect the insider behavior then an argument can be made that the statistics and research completed in the US have relevance outside of that culture.

2. The state of the art

This chapter provides background information that is required for this thesis. The author gives fair warning that this chapter is long but also required. Due to the fact that insider threat programs are uncommon and usually only affordable by large well-funded organizations, the reader may not have any prior knowledge of their existence. As insiders have sub classification, confusion may result based on understandable assumptions. There are chapters to address this by explaining what an InTP is not and why. Additionally a cursory understanding of insider threat programs will be introduced and simplified for use in this research.

2.1. Insider threat program origins

Insider threats became a priority roughly around 2000. It was at this time that the Department of Defense sponsored research at CERT, focusing on military service and defense agencies [1]. Findings from the study warranted further investigation and the following year the Secret Service National Threat Assessment Center (NTAC) and CERT completed the Insider Threat Study [1]. During this study a database of incidents was created and has since evolved to become the only database of its kind available. To date they have collected over 1000 cases reaching back to 1995 till the present [26]. Many of CERTs publications are open source and provide the foundation for much of the U.S. Government and private sector programs. The details of many of the cases researched are in fact classified because of their association with critical infrastructure, government, and the financial sector [1]. Though insider threat programs did not exist at the time of the incidents, the preceding decade indicated that incidents against critical infrastructure where becoming more severe and happening more often, thus warranting greater attention. There are three activities in particular that require explanation to better understand how insider threats fit into and provide value for modern organization; Espionage, Counter Intelligence, and IS.

2.2. Insider threats vs espionage

Insider threats have been an issue long before the internet made its debut. It has been mused that spying is the world's second oldest profession, as documented in the Bible book of Joshua. Spies were sent into the holy land, giving special attention to Jericho, and

worked out of a brothel (home of the oldest profession) during their visit. It might be added that having the lords blessing was not enough, additional intelligence was required to ensure their victory. [31] A strong belief in our time, for nations, companies, and individuals.

Though there is a wealth of information on spying, this term has a specific contexts attaching it to nation states. The term insider has been used in the past to indicate someone with special knowledge of the inner workings of an organization. In the case of finance and banking, insider knowledge has been used to financially harm one entity to the benefit or another. The modern use of the term has expanded beyond the nation state. Businesses have grown large and the number of core competencies they are expected to manage has grown as well. Each competency gives the company a competitive advantage and therefore must be protected to ensure the health of the company. Today's working culture in the western world supports a high turnover rate for employees. This creates a perfect opportunity for people coming into and leaving an organization to take intellectual property with them.

CERT and the Software Engineering Institute have been major contributors to security studies across many disciplines in the cyber security realm, even before the term cyber was coined. Their most recent revision of the definition of insider is: **A *malicious insider threat* to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems**. [1]

From the definition it appears that anyone, who through daily intercourse, helps an organization fulfill its purpose, poses a threat. Of course there are varying levels of risk associated with each of those relationship and roles. Such a problem is too big to tackle and must be broken down into digestible actionable pieces. The first step has been taken by defining the malicious insider threat as opposed to the non-malicious. Non-malicious insiders will continue to be a threat, but our focus is on those who are actively pursuing information. Additionally espionage is an information gathering activity initiated and supported by a nation state. Though their targets may vary, the sponsor is the defining characteristic. Though the nation states behavior in the target country is likely illegal by

local and possible the sponsor states legal systems, it is a commonly accepted practice. Yet there is no written framework for the legality of espionage, the precedent is that spying is legal so long as you do not get caught. Though beyond the scope of this paper it can be argued that espionage is a stabilizing factor for nation states as it allows them to make decisions with better intelligence. The activity of Spying or Espionage may utilize insiders to accomplish their objectives, but Insiders are not necessarily spies or conducting espionage.

2.3. InTP vs counter intelligence

Counter Intelligence (CI) programs also have unique and relevant characterizes. Counter Intelligence, as defined by the Joint Publication 2-0, Joint Intelligence (2013) in [32] is; "Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities".

CI is focused on agents of a foreign government operating inside the organization or country. CI has traditionally been associated with intelligence agencies or security services which are exclusively government funded and sponsored. CI activities have the razor sharp focus to protect government interests against foreign espionage activities and agents. What happens when foreign nations turn their espionage activities toward the companies in your country? Simply, a CI organization would be overwhelmed. They do not have the capacity or resources to expand their operations to such at scale. CERT address this specific gap in capabilities. Insider Threat Programs (InTP) include government organizations but due to the ease with which industrial espionage is conducted in the information age, CI activities have been adopted and modified to compliment business and non-government organizations security requirements [33]. CI programs overlaps only a sliver with the scope that InTP will cover.

2.4. InTP vs IS

IS encompasses the use of physical and logical data access controls to ensure the proper use of data and to prohibit unauthorized or accidental modification, destruction, disclosure, loss or access to automated or manual records and files as well as loss, damage

or misuse of information assets [34]. This definition by Thomas Peltier is broad but still not all encompassing. It does reflect what IS has been trying to accomplish for many years. Just as Counter Intelligence is a sliver of the scope that an InTP would cover, InTP's overlap only a sliver of what IS entails. A response and solution to the insider threat problem is expected from IS programs in an organization as they are responsible for the targeted information and expected to have technological solutions, often ignoring behaviors or incidents all together [35] [36]. These expectations ignore that insider activities have always existed but only now manifest themselves through technology [37]. Behavior science has addressed insider activities and behaviors [38] but the industry as a whole has failed to realize that the solutions are not entirely technical [39]. In light of the recent Edward Snowden and Chelsea Manning revelations, major U.S. agencies made an initiative to address the insider threat problem. InTP are the result of years of research, necessity, and finally the will to act.

2.5. InTP definition

This vision of what an insider threat program is put forward by CERT:

Insider threat programs can be built in many ways to suit the needs of the organization. Programs provide a repeatable set of processes that the organization can use to prevent or detect suspicious activity and to resolve malicious incidents. The program sets the tone for the organization and creates a focal point for awareness about insider threats. Successful programs span the entire organization during development, implementation, and operation. Integrated data collection and analysis of technical and non-technical (behavioral) indicators for potential insider activity. Lastly they have a formal process of response, communication, and escalation. [33]

Though not stated explicitly an insider threat program can also be instrumental in building and managing a security culture. InTP's do have a role of watching others. It diverges from traditional bodies with this role in that it pulls people from the entire organization to solve the problems, and reports its finding so that learning a culture can change to address the problems rather than being isolated from them.

2.6. CERT profiles

Products from their research discussed in 2.1 include the “Common Sense Guide to Prevention and Detection of Insider Threats” which is now on its fourth addition. From the data collected CERT has been able to create profiles. These profiles allow organizations to understand the behaviors associated with a particular type of incident. This knowledge allow an organization to build their defenses to address specific vulnerabilities they may have been unaware of. There are three main categories; IT Sabotage, IT Fraud, and Theft of Intellectual Property. Additionally they have identified a miscellaneous category in which the agent or their actions did not fit into the three main categories or encompasses a combination of the three categories. CERT has also addressed an Espionage category though the work is classified [1]. The miscellaneous category is a clear indicator that their work is not complete and that more profiles may exist. An Espionage profile has been created from various sources but is not the direct work of CERT. The author’s previous work concerning the Espionage profile will be included in this research because we are examining national infrastructure [40]. As discussed in 2.2, for nations Espionage is a reality they must endure.

CERT also identifies a number of complexities that spanned the major profiles. They are environmental factors that can provide an opportunity which may precipitate an incident. Table 2-1 is taken in its entirety from [1] and offers structure to complexities that influence an insider event. The information provided concerning CERT Insider Threat profiles is introduced in their simplest form to provide a framework to work from when considering the Estonia’s national infrastructure.

Table 1 - The CERT Guide to Insider Threats, 2014 pg. 6

Collusion with outsiders	Insiders can be recruited by or work for outsiders, including organized crime and foreign organizations or governments.
Business partners	It is important to control and monitor access to your information and systems by “trusted” business partners.
Mergers and acquisitions	Consider heightened risk of insider threats when organizations are merged or acquired.
Cultural differences	Behavioral indicators exhibited by malicious insiders who were born in different countries may differ.
Foreign allegiances	Organizations operating branches outside their own country must consider the insider threats posed by employees with allegiance to another country.
Internet underground	Some insiders seek technical assistance from the Internet underground. The internet underground is a collection of individuals with shared goals where there is some degree of hierarchical structure and primary communication mechanism or agent of electronic crime involves the internet. Further, it may demonstrate some degree of pseudo anonymity and/or secrecy, which may be useful for organizing and carrying out electric crimes.

2.8. IT sabotage

Insider IT sabotage: insider incident in which the insider uses IT to direct specific harm at an organization or an individual. [1]

This type of attack requires some degree of technical sophistication. The more technically adapt the person is the great potential for damage. As companies compete to hire the most technically savvy personnel available, they also are hiring those most capable of crippling their infrastructure. Not hiring the most talented people also has business risks. The technical skill sets most often seen in this type of attack are system administrators, database administrators, and programmers. [1] When privileged accounts are given and not managed well, the organization has created an invitation for disaster.

In a 2005 report by Dawn Cappelli of CERT indicated that the majority of insiders who perpetrate an IT sabotage attack are males, ages 17-60, half are married, 57% where disgruntled, and 70% had no previous criminal history. The primary motives for these attacks were revenge (84%) and response to a negative event (92%). Interestingly none of these incidents where motivated by money, but 81% of targeted organizations experienced financial loss. Of those detected prior to the event, 94% were detected due to system failures or irregularities. Normal events such as log monitor or audits of employees provided no indicators. [1]

2.8.1. Personal predisposition

100% of the CERT database insiders who committed IT Sabotage exhibited at least one behavior classified as a personal predisposition. These observable behaviors indicate dispositions which offers an insight into why one employee may conduct a malicious act while another tolerates the same situation. [1] Personal predispositions provide behavior indicators that can alert and organization that intervention is required. How an organization responds is dependent on how the program is developed.

2.8.2. Managing expectations

Disgruntlement and unmet expectations have also been identified as a common traits seen across the IT Sabotage research profiles. Simply, unmet expectations lead to an employee's disgruntlement which in turn leads to an eventual incident. An example given by CERT was a new employee requires strict adherence to long relaxed security rules.

Unmet expectation may surface for a variety of legitimate reasons and may have precipitating events which can act as indicators to management that special attention should be paid to the situation. [1]

2.8.3. Behavioral Precursors

Behavioral Precursors are an individual action, event, or condition that involves personal or interpersonal behaviors and that precedes and is associated with malicious insider activity [1]. This will often be the first sign of disgruntlement. Noticing these behaviors presents an opportunity to identify a problem and address the underlying issue before an event takes place. Such action returns the individual to lower risk profile and perhaps removes the risk all together. Noticing is the key factor. This can be done by fellow employees or management, but is most often just not recognized.

2.9. Theft of intellectual property

Insider theft of intellectual property (IP): an insider's use of IT to steal proprietary information from the organization. This category includes industrial espionage involving insiders [1].

Intellectual property: intangible assets created and owned by an organization that are critical to achieving its mission [1].

In the cases studied, the people who perpetrated this crime were normally technically adept, though not your system administrators or technical maintainers. Insiders included employees who are scientist, engineers, programmers, and sales people. Only a small percentage stole the IP with intent to sell it. Normally one of three scenarios compliment this crime; taking the IP to a new job, using it to start their own company, or taking it to a foreign government or organization. [1]

The most difficult aspect of this threat vector is that these insiders are stealing information they normally access every day. It is their job to access this information. Discerning between normal or nefarious accesses is a challenge that cannot be totally solved by technical means alone.

There are two closely related patterns that were identified during the research.

Entitled independent*:* an insider acting primarily alone to steal information to take to a new job or to his own side business. [1]

Ambitious leader*:* a leader of an insider crime who recruits insiders to steal information for some larger purpose. [1]

In both cases the insiders felt a sense of entitlement or ownership toward the IP. This sense of entitlement in effect changes their decision making behavior. When dissatisfaction is added to the equation, the risk level rises and is often not noticed.

2.10. IT fraud

Insider fraud: an insider's use of IT for the unauthorized modification, addition, or deletion of an organization's data (not programs or systems) for personal gain, or the theft of information that leads to an identity crime (identity theft, credit card fraud) [1].

Incidents of insider fraud are distinctly different than the previous two profiles. These incidents are not normally technical in nature, in fact they are usually perpetrated by low level employees. Examples that where given included administrative people such as help desk, customer service, and data entry [1]. Because these people are lower level employees they usually have financial need that is different from the other two profiles. Success only encourages that bad behavior which makes the timelines much longer, years in most cases. Another complication is that if there are cohorts in crime it is likely to go on for a longer period of time and be more successful, especially if low or mid-level management is involved. This profile is also the most likely to be connected to organized crime. In cases where there are insiders and outsiders working together it is likely that the insider will only be involved in the theft of personally identifiable information (PII). The outsider will then use the PII to commit fraud.

2.11. Espionage

Though the espionage profile has not been disclosed by CERT a considerable amount of information can be pulled from "Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis" [41]. This exercise was completed in a NATO CCDCOE "Insider Threat Detection Study" and a comparison is available in Table 2-2 [40]. The CERT assessment made some very interesting and useful associations between IT

Sabotage and Espionage. By using systems dynamic modeling, phycologist and technical experts realized that individual cases from both categories could be modeled as a single concept [41]. Initially two models where developed, only after the modeling process was complete where correlations found and focused on. The aspects where parallels were drawn from included: [41]

1. The prevalence of both behavioral and technical rule violations prior to attacks.
2. The important consequences of whether the rule violations were detected.
3. When they were detected, the critical nature of the manner in which they were handled by management.
4. The impact of auditing and monitoring, both technical and non-technical, on discovery and handling of behavioral and technical indicators.

Follow on research lead to another model that identified six issues that required further investigation. This included following observations: [41]

1. Most saboteurs and spies had common personal predispositions that contributed to their risk of committing malicious acts.
2. In most cases, stressful events, including organizational sanctions, contributed to the likelihood of insider IT sabotage and espionage.
3. Concerning behaviors were often observable before and during insider IT sabotage and espionage.
4. Technical actions by many insiders could have alerted the organization to planned, or ongoing malicious acts.
5. In many cases, organizations ignored or failed to detect rule violations.
6. Lack of physical and electronic access controls facilitated both insider IT sabotage and espionage.

What makes this research so useful is not that Espionage and IT Sabotage can be lumped in the same category. Quite many of their other traits and motivations are very

different, but similarities between behavioral predispositions is convincing. Simply, their personal predispositions escalteted to conflict that precipitated an event. Sanctions to the individual and the perception of benefit without consequences acted as enablers for increased rule violations [41]. Their behaviors' precursors are observable, often what is lacking is the training to understand what was observed, a mechanism of reporting, and a plan of action once concerning behavior is identified.

There are also noticeable differences between Espionage and IT Sabotage. IT Sabotage is often an act of revenge, in response to negative or stressful events, and unmotivated by money [41]. Espionage has more complex motivators. In some cases revenge is a motivator but akin to IT Fraud there is often a financial element attached to their actions. The need for more resources once they have become accustomed to living beyond their means precipitates repeat occurrences [41]. The second similarity that can be drawn is that of acting with outside agents. From the perspective of a company, the outside agent and their actions are criminal no matter if the recipient is a criminal organization or a foreign government, drawing parallels to IT Fraud. Lastly espionage shares similarities to IP Theft with regard to the means in which they exfiltrate data. There have been cases of sabotage used to cover their tracks.

Table 2 - Adapted from NATO CCDCOE "Insider Threat Detection Study" 2015

Profile	IT Sabotage	Insider Theft of IP	Insider Fraud	Espionage
Who	Technical Employees - System Admins, Network Admins, Developers, Programmers	Scientist, Engineers, Programmers, Sales, for example.	Low level employees Help Desk Customer Service Data entry *Low/Mid-Level* Management	Technical or non-technical in nature.
When	Set up while employed. Executed after/or if suspected termination. Frequently within +/- 30 days of termination.	Usually within +/-30 days of leaving the organization.	Happens over a long period of time.	After the initial incident long period may pass before a follow on event. Happens over a long period of time.
Motivation	Revenge	Start their own business, new job, foreign government or organization.	Financial need or greed.	Financial need or greed Dissatisfaction with status
How	Access/Ability/Motive	Data exfiltration Email/USB/ Physical Documents	Corruption of organizational procedures. Inadequate auditing of Critical and Irregular Processes. Excessive access/privileges.	Methods spans all profiles.
What	Systems they worked on.	Steal info they worked on.	Personal Identifiable Information * With some form of management involved the fraud happens over a longer period of time and has a great monetary impact	Steal information and destruction of information if necessary to cover their tracks.

2.13. Summary of profiles

The CERT profiles provide clear indicators of what to look for with regards to insiders. This does not imply that this knowledge is complete. Only that it has been developed using rigorous methods by top researcher and is supported by over 1000 insider threat cases. These profiles allow organization to have a more focused understanding of the insider threat they may be up against. Now they can determine what methods of prevention, detection, and response are appropriate for the identified threat. Lastly they allow organizations the opportunity to plan a response.

3. Information security management systems vs insider threat programs

A comparison will be made between the ISKE and InTP to determine if the gap identified in 1.1 warrants further investigation, or if ISKE is a suitable for addressing this growing threat. IS programs are well established in IT. Insider Threat Programs are a relatively new concept that builds on an organizations existing infrastructure to provide an additional set of indicators that can be used to prevent, detect, and respond to insider events. The InTP is designed to specifically address the insider threat vector, an area of IS that has not received the attention that it deserves.

The only exception is that of NIST, who provides an ISMS's for U.S. government agencies and commercial entities alike. In an attempt to address the growing concerns posed by insider threats, NIST SP 800-53 rev4 introduces new controls specific to the problem [42]. These recommendations are general in nature but do compliment and reference existing controls that already exist in the ISMS. These updates were published in 2013 and represent the U.S. government's efforts to learn from expensive mistakes. In this case NIST has identified the need for this program, actions to take, though it lacks a framework for implementation. The drawback to what is offered by NIST is that it is new and unrefined, and as everything else associate with the U.S. government, expensive. In time this will change, but there is a cost associated with waiting as much as with beginning.

3.1. ISKE for Estonia

The first challenge when researching ISKE was accessing the document. ISKE is over 3000 pages long and only available in Estonian [42]. For this reason research is limited to documents about the program rather than the program documents themselves. This situation is not a deterrent to the finding of this thesis as ISKE is admittedly heavily influenced by IT Grundschutz. The IT Grundschutz methodology presented by the German Federal Office for IS (BSI) as a 'how-to' document for setting up a security information management system [43]. BSI has interpreted the general ISO 2700X requirements and created a publication that has a practical application focus [43]. As presented in 1.1 ISKE is an IS framework and therefore focuses on technical rather than behavior indicators.

3.2. What is the ISKE standard and what does it provide?

When developing the ISKE standard a number of considerations were taken into account. Estonia was looking for a program that was appropriate to their security goals and security level, was updated frequently, and was available free of charge or at a very low cost [42]. BSI was the closest existing standard that met these needs and was adapted accordingly. ISKE provides an ongoing process that addressed questions of confidentiality, integrity and availability of data and assets [42]. RIA lists a simplification of activities the ISKE process addresses [44]:

1. Mapping databases
2. Mapping information systems and other information assets
3. Identifying links between databases, information systems and other information assets
4. Identifying the required security class and level for databases
5. Identifying the required security class and level for information systems and other information assets
6. Identifying the typical modules, which comply with information systems, and other information assets
7. Identifying the required security measures for information systems and other information assets.

The process of implementation is continuous and there are challenges. IT systems continue to become more complicated, human behavior, the large number of e-services and development projects, and the growing costs have been identified as areas of concern [45]. Except for the number of e-services and development projects, these are the same concerns shared by virtually every organization using information technology.

3.3. How does the current ISKE standard protect from the insider threat vector?

As mentioned in 3.1 this part of the research is dependent on the publications offered by the BSI in English to conduct an assessment. The Supplement to BSI – Standard 100-3, Version 2.5 lists 46 threats [46], of which eight can be considered directly insider threat (intentional and unintentional) related:

1. T 0.14 Interception of Information / Espionage
2. T 0.16 Theft of Devices, Storage Media and Documents
3. T 0.17 Loss of Devices, Storage Media and Documents
4. T 0.19 Disclosure of Sensitive Information
5. T 0.32 Abuse of Authorizations
6. T 0.35 Coercion, Extortion or Corruption
7. T 0.41 Sabotage
8. T 0.42 Social Engineering

A number of others from this list may be the threat vector an insider uses but are not necessarily insider threat related. Additionally listed in the IT Baseline Protection Catalog G5 Deliberate Acts [47] are 195 deliberate abuses that are also explained. Of this list the act of theft is described five different times, sabotage once, fraud once, and spying once (though not espionage). The resultant combination of both sources is listed below with the applicable insider threat profile

IT sabotage

1. T 0.41 Sabotage
2. G 5,102 Sabotage (supporting documentation correlates to T 0.41)

IT fraud

1. G 5:14 toll fraud

Insider theft of IP

1. G 5.4 Theft
2. G 5:22 theft in mobile use of the IT system
3. G 5.69 higher risk of theft in the home workplace
4. G 5,125 data theft using mobile devices
5. G 5141 data theft via removable media
6. T 0.16 Theft of Devices, Storage Media and Documents

Espionage

1. T 0.14 Interception of Information / Espionage
2. G 5.104 spying information

The difference between profiles based on CERT research and the threats or acts based on BSI becomes immediately apparent. BSI is answering two characteristics of the profiles listed in Table 2.1, how and what. Sabotage and Espionage profiles will be compared to the associated threats.

3.3.1. T 0.14 Interception of Information / Espionage

Espionage is defined as attacks aimed at collecting, evaluating and presenting information about companies, people, products or other target objects. The presented information may then be used, for example, to provide certain competitive advantages to another company, blackmail people or build a copy of a product. In addition to a variety of technically complex attacks, there are often also much simpler methods for gaining valuable information, for example by bringing together information from several publicly accessible sources, which looks like harmless information in isolation, but can be compromising in other contexts. Since confidential data is frequently not sufficiently protected, this can often be intercepted using visual, acoustic or electronic ways.

Examples:

1. Many IT systems are protected against unauthorized access by identification and authentication mechanisms, e. g. in the form of user name and password verification. If the password is transmitted over the wire in an unencrypted form, it is under certain circumstances possible for an attacker to retrieve it.
2. To be able to withdraw money out of an automatic teller machine, the correct PIN for the used electronic cash card or credit card must be entered. Unfortunately, the visual protection available for this equipment is frequently insufficient, so that an attacker can look over the shoulder of a customer entering the pin without much effort. If the attacker steals the card afterwards, he can plunder the account this way.
3. To receive access rights to a PC or to otherwise manipulate it, an attacker can send the user a Trojan horse which he has enclosed within an email as a supposedly useful program.
4. In many offices, workplaces are not sufficiently protected in terms of acoustics. As a consequence, colleagues and also visitors could possibly

listen to conversations and come to know information which is not meant for them or is even confidential. [46]

T0.14 attempts explains the act of espionage. The first point to notice is that “presented information may then be used, for example, to provide certain competitive advantages to another company” and “build a copy of a product” are actually activities covered in the CERT profile IP Theft. Also “blackmail people” is used, and activity that may be criminal in nature and surely a tool of espionage, but also criminal organizations. In comparison to what has been presented in the cert profiles this information is less precise. The examples are also presented in a way to allow a practitioner to have rudimentary knowledge of threat, but not a detailed understanding of what you are looking for. More to the point, what the agent may be looking for. The threat profile is simply not as refined as the CERT profile.

3.3.2. T 0.41 sabotage

Sabotage is the deliberate manipulation of or damage to objects or processes with the aim of inflicting damage to the victim by acting this way. Particularly attractive targets can be data centers and the communication connections of public bodies or companies, since there a great effect can be achieved with relatively few resources.

Selective manipulation

The complex infrastructure of a computer center can be affected by selective manipulation, when possibly external perpetrators but also primarily intruders from inside actively influence important components to provoke operational disruptions. In this regard, insufficiently protected technical building systems and communication infrastructure as well as central supply points are particularly threatened if they are left unobserved in organizational and technical terms and can be easily accessed by externals without being noticed.

Examples:

1. Power supply - In a mainframe computer center, a manipulation of the uninterrupted power supply led to a temporary total failure. The perpetrator had repeatedly manually switched the uninterrupted power supply to bypass mode and then manipulated the main power supply of the building.

Altogether there were four failures within three years. Even hardware was partially damaged. The disruption took between 40 and 130 minutes.

2. Flooding - Sanitary facilities were also located within a data center. Due to blockage of the drains and the simultaneous opening of the water supply, water penetrated into central technology components. Damage caused this way resulted in interruptions of operation in the production system.
3. Electronic archives - Electronic archives present a particular risk of sabotage, since there, many sensitive documents are kept on a small floor space. Because of this aspect, by targeted unsophisticated manipulation a great deal of damage can be incurred under certain circumstances. [46]

T 0.41 Sabotage also presents a definition and examples. In comparison to the CERT IT Sabotage the definition is less precise and the examples are too focused. This description identifies ‘what and how’. The cert profiles offer who, how, when, and why and empirical evidence that supports it. Now that a clear understanding of what ISKE is and what it provides, a closer look at the gap that exists between the two programs will be explained.

3.4. What gaps exist between the ISKE standard and the InTP foundations?

Estonia has a high standard of IS as proven earlier in this chapter. From the two examples it is clear that the foundational information provided by CERT and that provided by BSI, and presumably ISKE greatly differs in its granularity. CERT profiles offers more data to address the insider threat.

What is not addressed is how the ISKE standard is implemented. It is very possible that an IS program may have used these examples and added a great deal more controls to address the many scenarios that can be imagined. Even if this is the case it still falls short of what an InTP has to offer. The work done in IS may only be found in siloes through the organization. Data fusion is not taking place to address the issue at all levels of the organization. Sales, HR, legal, management are all expecting IS and IT to handle this issue.

Insider threats are managed in accordance with ISKE standard with specific threats and risks being addressed directly in the form of a control. Controls are implemented to address risk and are resource-dependent. Due to this limitation, controls remain technical

in nature. Behavior science indicators and management techniques are not as easy to quantify and qualify, technically or monetarily in comparison. They simply are not seen as a cost effective solution, and would not fit into the function of an IS program.

Insider Threat Programs in contrast are programs that span the entire organization, include employee monitoring solutions that are technical and nontechnical in nature, are integrated with the training program, and have the authority to conduct inquiries and investigations when indicators suggest a higher degree of risk [30]. Where an IS program is myopic in nature, InTP's require partnerships that include representatives from IS, IT, human resources (HR), public relations, legal, physical security, and executive management involvement and support [30]. The tools required to have a successful InTP must be behavior in nature, which is neglected by IS programs [30], and require technical indicators enabled by IT and managed by IS programs like ISKE. The insider threat strategy will then move from deterrence (ISKE) to prevention, detection, and response which is what an insider threat program offers.

3.5. Research questions and propositions

To address RQ1, the BSI examples show a clear pattern. Threats and acts tell the practitioner what to put in place to prevent an incident. In doing so they address a problem directly but leave a great deal of possibilities associated with the threat unaddressed. The examples answer the questions 'what and how' that are associated with the threat or act. Insider threat profiles provide general information regarding the 'what and how' questions, but provide specific answers to the actors possible identity, motivation, and when they might act. Even partial use of this information short of implementation of behavioral indicator is useful when developing controls.

RP1.0 is then answered in the affirmative. Insider threat profiles are more precise. Short of implementing an insider threat program, improved controls could be devised with better information to address insider threats.

3.6. Tentative Hypothesis

The insider threat profiles provide better information to detect insider activities in comparison to what is offered by BSI.

3.7. Summary

In this chapter it was determined that the origins and motivations for the ISKE baseline was to build a program that fit the Estonian situation, rather than adopting an existing standard. It is decided that ISKE is strongly influenced the development of BSI, and that BSI was available in English. ISKE and BSI are found to be technical in nature and lack the application of behavior science to their methods.

From this point a focused search of threats that are addressed in the BSI standard were pulled. BSI threats are explanatory in nature but lack real knowledge that would allow the organization to identify an agent, only controls to prevent an incident. It was also found that CERT profiles are more precise definitions and provide information on what you are looking for, not just suggestions on what to protect. It is determined that a noticeable gap exists between the possibilities that are offered by each program.

Finally a comparison was done of the programs themselves. Due to their purpose, IS programs offer less in the way of finding insider threats. Even with their capabilities built up in a very robust way (as they apparently have been in Estonia due to its success) IS programs are not designed to span an organization. Nor are they designed to include members of other departments when designing and implementing their solutions. InTP offer new capabilities to address the insider threat vector that are not considered in an IS program. It is also worth noting an InTP is likely dependent on the indicators provided by IS programs.

3.8. Conclusion

This research proposes that insider threats have long been dealt with in somewhat less than holistic approach. The application of insider profiles and the implementation of an InTP offer a means of managing this problem directly, rather than addressing symptoms. Such a capability has been the desire of many organizations, but without clarity of the problem, measurable success has not been accomplished. The insider threat profiles are useful additions to an existing information security program in addressing the insider threat issue.

In the next chapter the insider threat profiles are examined to determine if these profiles would be a useful addition to RIA’s already existing information security program.

4. Application of profiles

The insider threat profiles will be examined individually to determine what characteristics of the profile fit to RIA's operational profile. This is a simple experiment allows to decide which profiles are of interest. Once the profiles are narrowed down priorities can be addressed as to which profile to address first. This decision is dependent on what the critical assets are and is beyond the scope of this investigation. From figure 2.1 each profile will be looked at individually and the rational presented.

4.1. RIA

Riigi Infosüsteemi Amet (RIA) - Estonia's Information System Authority has a number of responsibilities. The data exchange layer (X-Road) that enables secure information sharing between the e-government services is the reason RIA has been chosen for examination. Their work is central to Estonia's government success and the continued health of Estonia's information society. RIA is highly regarded at home and aborad. A survey published by the International Telecommunication Union (ITU) in 2014 places Estonia in the 5th position in the global cybersecurity index on par with Germany, U.K., Japan and South Korea [48]. Such an accolade is a good indication that the trust the Estonian people have is well earned. This was also reflected in RIA's annual report where surveys indicated that citizens have a high degree of cyber awareness and trust in their efforts and services [49].

On this infrastructure the government offers over 600 e-services to citizens and 2400 to businesses [50] [51]. E-governance services were first introduced in 2000, and are five to ten years ahead of other systems [50]. The two key ingredients that make these services possible are the X-Road (introduced in 2001) and a universal electronic ID card (introduced in 2002, PKI enabled) [50]. Though other countries may be more technologically advanced, they may not have these two ingredients. An even more fundamental ingredient is that of trust. Trust in Estonia's e-governance was built on the X-Road and ID card system [49]. The Estonian people trust the services deployed on the X-Road and the use of common ID numbers [50]. Even if a country was to have a solution for the two technical ingredients it is no guarantee that people will trust it. This was fantastically demonstrated when the United Kingdom failed to introduce a national identity card system in 2010 [50], costing the nation 370 million dollars [51]. These

achievements currently put Estonia five to ten years ahead of the nearest followers [52] of their e-governance model.

4.2. IT sabotage

IT sabotage is normally conducted by technical employees. As RIA provides the information security to the data exchange layer that is the X-Road, they do have a large number of technical employees, to include research and development, and Estonia's CERT team. Technical employees include system administrator, network administrators, developers and programmer, all of which RIA employees. These employees have access and ability. This is clear from their international cybersecurity ranking.

Though questions of motivation cannot be addressed directly, disgruntled employees happen everywhere. This disgruntlement, for whatever reason in the catalyst for the motive of revenge. IT sabotage is a profile for further consideration.

4.3. Insider theft of IP

CERT describes the people who commit IP theft are often the same people that develop the software or technology. They develop an emotional attachment to their work and actually feel entitled to it, rationalizing away their actions of theft [1]. Titles held by this profile are scientist, engineer, programmer, and in some cases sales. The motivation is normally to start their own company, take it to a new job, take it to another country, or another organization. What is most difficult about detecting this is that the information they are stealing is the same information they are working with every day.

RIA employees carry all of these titles short of sales. E-governance is a market that is growing rapidly and there is not enough expertise in the world. These employees are a valued international commodity even if they are unaware and hidden away in Estonia. This profile also deserves further consideration.

4.4. Insider fraud

Though RIA does have a help desk and customer service, they are lacking low level employees. These people are specialists with some level of education. This aside, it is unclear how their administrative and custodial services are run, so the possibility does

exist. As the information on the X-Road is encrypted it is unlikely that easy access to PII information of the general public could be harvested from the facilities without being noticed. Another possibility is how the PII of employees is handled. This aspect of how their administration is organized and managed would determine the level of risk associated.

More information is required before a determination can be made. This profile represents low risk.

4.5. Espionage

Espionage was covered in chapter 2.2.

As state in chapter 2.2, espionage is a reality nations must endure. The author sees no reason to exclude Estonia from this activity. Behaviorally espionage is identifiable to IT sabotage, but shares characteristics with all profiles. This profile merits further consideration.

4.6. Research questions and propositions

RIA's operational profile does match IT sabotage and insider theft of IP. Because RIA is an Estonian government organization the possibility for espionage cannot be ruled out and is therefore also a matching profile. It has been determined that the insider fraud profile cannot be determined at this time, but cannot be disregarded.

As discussed in the previous chapter ISMS provide information for deterring insiders but little to no information on how to detect them. Considering that three of four profiles do compliment RIA's personnel profile and capabilities profile further investigation is warranted.

4.7. Tentative hypothesis

RIA can provide greater protection against insider with an InTP.

4.8. Summary

Three profiles are of immediate interest. IT sabotage, insider theft of IP, and espionage. Though the possibility of insider fraud does exist, there was not enough information about the organzation's inner-workings to draw a conclusion. The risk associated with insider fraud is lower than the risk associated with the other three profiles.

4.9. Conclusion

RIA provides a critical service for the Estonian government operation and Estonia's information society. This makes the organization a likely target for espionage. Additioally the profiles for IT sabotage and insider theft of IP match the organization's personnel profiles and capabilities profile. It is reasonable to believe that RIA could be a victim of either crime. These finding indicate that the further research is merited to better access the risks posed by insider threats.

5. Estonian examples of insider incidents

The primary challenge to this research is navigation of the Estonian language. A considerable amount of information regarding the Estonian government agencies are on line and in English. Not always the information required for this research. For example researching actual case law has been difficult. Consideration of reviewing actual cases with the extensive investigative format used by CERT would provide more conclusive results.

In 2007 the personal data protection act (PDPA) was made law and entered into force in 2008 [53]. Seven years after Estonia had established the X-Road and e-governance had its first service available. Estonia established the Estonian Data Protection Inspectorate (EDPI) to address issues of PII abuses intentionally or unintentionally on the X-Road or the users there of. Once the personal data protection act came into force the EDPI assumed to role of enforcement for the country. Data from their annual reports will be examined.

Kaitsepolitseiamet (KAPO), Estonia's Internal Intelligence Agency also published information on espionage cases. These cases will be examined to determine if indicators where present that would have been detected by an InTP.

5.1. Estonian Data Protection Inspectorate

EDPI annual reports do not have a standard format. As the agency (in its current form) is relatively new and this is understandable. From their annual reports the following information was of value; complaints and challenges to use of PII by users of the X-Road, misdemeanors, and imposing of a penalty payment or misdemeanor penalty. Complaints are the sign of a free and open society. This is an indication that people are informed and feel empowered to take part in the government process. Table 3 offers seven years' worth of data. It is apparent that after the PDPA was put into force, awareness and reporting increased. The increase in reports does not directly correlate to misdemeanors or penalties. Trends may become more apparent in the years to come.

Table 3. Estonian Data Protection Inspectorate statistice from Annual reports

Selected criteria of reports from the Annual Reports of the Estonian Data Protection Inspectorate	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014
Complaints, challenges, misdemeanour notices (submitted)	*	*	*	110	358	306	592	818	404	550	413
Misdemeanors	5	8	15	4	23	46	35	34	43	29	11
Imposition of penalty payment or misdemeanour penalty	*	*	*	2	14	12	15	38	39	22	8
	Derived from data published in the Estonian Data Protection Inspectorate http://www.aki.ee/en/inspectorate/annual-reports										

Misdemeanor responsibility is only stipulated in the instance where information prescribed for internal use is released or disclosed [55]. Misdemeanors indicate that wrong doing was assessed though not necessarily severe enough for a monetary fine. In either case unintentional, through neglect or ignorance, may have been the cause rather than malicious intent. Issuing a fine is a subjective act beyond the scope of this research. The data is only presented to imply there is a degree of severity between incidents that was not captured by this research. A closer examination is required.

5.1.1. EDPI annual report assessments

The following exerts are from the annual reports in support of the data in Table 3.

2005 - In conjunction with the increase in budget for 2005, the Inspectorate planned for five new employees, but during the report year three employees left for other state authorities. The situation is problematic, as instead of hiring new staff according to the initial plan, the inspectorate has to deal with replacing staff. The positions of the officials who left the inspectorate must be filled. As the officials of the inspectorate are suitable for other state authorities thanks to their acquired know-how, the acquiring of staff by other state authorities has become increasingly frequent (three times by other state authorities during 2005) [55].

Though experience is not intellectual property it is an indicator that the personnel are a commodity in high demand. An issue that may lead to a shortage of personnel who are capable of supporting the infrastructure along the X-Road in the years to come. High turnover also leads to management challenges and is disruptive to efforts of maintaining consistent organization performance.

2006 – A number of cases where addressed specifically. The reports indicate that the violation was unintentional, considerable doubt of this lead to assessment of penalties [55].

Three cases indicated corruption of processes that lead to data protection violations. Corruption of processes is indicative of insider fraud.

2007 – This was none standard report introducing previous years statistics without explanation of activities of interest.

2008 – This report listed widespread problems experienced while enforcing the Public Information Act. Based on requests for explanations, complaints and challenges, the problems related to the public information may be collectively summed up as follows:

a) negligence and laziness of holders of information – requests for information are not answered within the prescribed term, the obligation of maintaining the documents register or publishing the information on webpage is not performed correctly;

b) disputes between persons making a request for information and holders of information regarding the legality of bases for access restrictions;

c) incorrect understanding that each letter to a holder of information is request for information and it shall be answered within 5 working days – many inquiries submitted as requests for information are actually requests for explanations,

d) webpages of holders of information are constructed not in user-centered but in institution centered manner [55].

The above observations indicate growing pains and society adjusts to new organization realities and raises public awareness. Negligence in the support of handling of information is not a malicious insider but an unintentional insider.

2009 - This was none standard report introducing previous years statistics without explanation of activities of interest.

2010 - Zero tolerance was established with regard to persons who misuse the police database, and anyone doing so is punished with disciplinary as well as misdemeanor procedures. There is regular information exchange between the police and ourselves for

this purpose. This has brought about a noticeable change for the better within the organization. Once the problem of archiving and deleting outdated data finds a satisfactory solution, we will be able to say that the biggest risks relating to the police database have been minimized [55].

This is a noticeable achievement, and also a clear indicator that abuses of PII do take place. The police and boarder guard are mentioned here but this does not mean there are no other problem areas not being mentioned. Standard granular reporting would be more helpful in identifying problems.

2011 - Information exchange with the Police and Border Guard Board and the Ministry of the Interior for surveillance of the misuse of police databases and the Population Register, respectively, is on firm grounds. Misuse of the Population Register was increasing, so we discussed the problem in media and implemented a stricter fine policy [55].

2012 – Misuse of the Population Register is the most common reason of misdemeanour proceedings (30 of 43 completed proceedings). Misuse of the police database has decreased (four misdemeanour cases). Our primary goal is to end breaches, not to punish. The majority of breaches end immediately when supervision starts or when a recommendation/proposal is received. **Comparative monitoring of the disclosure of debt data of natural persons** in November 2012 covered the websites of 66 debt collection companies. 12 of them had disclosed the names and often also the dates of birth or personal identification codes of private persons on public websites. Seven of these companies terminated the breaches voluntarily, five did it after we had issued them with precepts [55].

This is a unique case. Though not a profile insiders used information for the purpose of coercion or shaming. Clearly an abuse of power and PII, which is not in the spirit of an information society. It is concerning that organization feel entitled to abuse personal information rather than using the legal system to resolve disputes.

2013 – The punitive response (misdemeanor proceedings) volume has decreased and it mainly includes misuse of professional access rights to sensitive records. Since the violation has already taken place, supervision by making proposals-precepts is no longer

relevant, which is why the Inspectorate always responds by initiating misdemeanor proceedings in these cases [55].

Misuse it now becoming directly associated with intent.

2014 – The Inspectorate finds that in practice, everything is not as it seems. A simple example: a large number of institutions have ignored the obligation to commission a regular data protection audit upon maintaining databases. Required notes are not entered in the administration system for the state information system, which makes it more difficult to get an overview. In the event of large and complex systems, without an impartial external assessment, the management board of the institution cannot ensure that information security and data protection risks, particularly the institution's own personnel risk, are hedged. I would like to remind the management boards of all institutions that in this digital age, poor information security is just as dangerous as a badly protected state border, broken door lock or unattended wallet. The manager is liable for ensuring information security as much as for, say, organizing the accounting [55].

Estonia is a well-developed information society and clearly still evolving. Without proper oversight there will be laggards and abuses in various forms. Commercial organizations are simply weighing the risk to their organizations from its monetary impact with no regard for the greater good. These organizations are well placed insiders (Figure 2, business partners) who are developing a culture of "compliance of convenience". Such a culture provides and environment of risk taking with information that is not theirs, indicating they are not responsible actors. Again this does not fall into a CERT profile but there is a culture of concern as the Director-General has pointed out.

As observed by Rull, Täks, and Norta; cases of misuse of personal information require the expertise of highly qualified prosecutors and attorneys to argue a case. Evidence has to be collected before that. And, most importantly, there is no case without a victim. A person who has learnt about the misuse of personal data may initiate the case or the violation may be discovered by internal audits. No one knows how many violations have taken place, which victims do not know about, nor have internal audits discovered them [56]. There is clearly an issue and it is being handled by technical means and self-reporting by the victims.

5.2. Kaitsepolitseiamet

The following espionage cases where taken from KAPO's annual reports. These are the reports they have chosen to make public.

2005 – KAPO reports a noticeable increase in attempts by Russian agents to recruit Estonian citizens [57].

2007 – Reet Kuntus was found guilty of losing classified materials. This was done by means of corrupting processes associated with handling of classified materials [57].

2008 – Herman Simm deputy advisor to the Ministry of Defence was convicted of treason. His motives included discontent with the Estonian nation as it took a new direction towards western integration. Additionally he expressed frustration with loss of status and the desire/need for greater financial resources. Simm was notorious for corrupting processes. Due to his high charisma and status in various organizations he was never challenged [57].

2009 – Increase support of Russia to extremist groups in Estonia [57].

2010 – Noticeable increase of influence operations in Estonia by Russian interests [57].

2011 – Uno Puusepp retired from the KAPO in 2011 where he immediately moved to Moscow. It was reviled on a Russian television documentary "Our Man in Tallinn" that he was a double agent since 1996. During the interview he claimed that everything that landed on the desk of the KAPO directors ended up in Moscow. Puusepp's motivations were reported to be disgruntlement with the Estonian establishment and not motivated by money [58].

2012 – Aleksei Dressen worked at the Internal Security Service and his wife Viktoria Dressen conducted a long running operation for the Russian Federal Security Service (FSB). The details of his case are still classified. Both the Aleksei Dressen case as well as the one involving Herman Simm demonstrate that Russian special services are ready to carry out complicated and costly operations in order to recruit Estonian informants in important positions [57].

2013 – Vladimir Veitman was convicted of treason for providing information to Federal Security Service of the Russian Federation. He was a leading specialist in the Internal Security Service [59].

The above excerpts from KAPO's annual review indicate plainly that Russia represents a grave adversary in every aspect of intelligence collection. From government agencies to the civilian population, their actions are nothing less than aggressive.

5.3. Research questions and propositions

From the EDPI findings, Estonia has insider behavior, but nothing that conclusively fit the insider threat profiles. KAPO's annual reports covered a number of cases that fit the espionage profile.

RP3 does not hold up under the close examination. Though insider PII abuses do take place there is no indication of sabotage, theft or fraud. In fact it cannot be determined what the motivation or outcome of their actions were. In the case of KAPO, it is clear that this organizations counter intelligence resources are fully employed. The cases examined in the annual reports compliment the espionage profile. Due to Russia's large scale investment in influence operations and subversion InTP appear to be a useful set of tools that are not currently employed that can address this problem.

5.4. Tentative hypothesis

Estonia has insider threat behavior that is not fully understood and InTP is useful to address insider incidents, whether unintentional, intentional, or state sponsored.

5.5. Summary

EDPI annual reviews and posted statistics make a clear case that insider behavior is present. Corruption of processes and negligence are the two most common themes. Cases of organizations and individuals knowingly disregarding policy and procedures is prevalent. Though these acts are all violations of PDPA, malicious intent was not determined even if penalties were awarded. The EDPI identifies a pattern of neglect in the 2014 annual report.

The espionage insider threat profiles fits nicely with the information offered by KAPO. Reet Kuntus and Herman Simm both utilized corruption of processes that allowed the information to become compromised. Puusepp and Simm both admitted to being dissatisfied with their status. All of the cases mentioned were long term relationships with the exception of Reet Kuntus. Aspects of the Dressen and Veitman case have not been released and therefore enough information to determine if the profiles have relevance is not available.

5.6. Conclusion

The EDPI has considerable technical capabilities to investigate abuses of personal data. The methods they search are in support of the PDPA and do not provide granular detail that would be more helpful in this investigation. This aside there is evidence that abuses of information do take place. After seven years these problem have not entirely disappeared.

The Estonian Police and Boarder Guard seem to have the greatest share of violations. Though there are abuses of power and authority granted to them by the people of Estonia, the only criminal activity at this point is the act of violating the PDPA. The details of the debt collection companies that used the data in an illegal way also does not fit the profiles, but is a clear indication that personal data will be abused if it suits the companies' purposes. There are no commonly accepted norms or information specific moral-codes established that will protect personal data beyond enforceable laws. EDPI also states in their most recent annual report that poor information security practices in organizations is becoming a concern. Though Estonia has developed an impressive information society, they have yet to develop a security culture to compliment it.

Espionage was not the primary profile of concern in this research. After considering everything that has been presented in the KAPO annual reports, the espionage profile does fit. Espionage activities are active in many areas of Estonian society sponsored by Russia. The CERT expanded complexities of insider threats also fit the espionage cases that were covered; collusion with others, cultural differences, foreign allegiances, and the internet underground are all general concerns.

6. Summary

The motivation of this study was to determine how well defended the Estonian infrastructure and information society was from insider threats. This was done by examining the country's ISMS, RIA, and historical data regarding insider threats. Sampling was selected from open source information from EDPI, KAPO, and RIA. The methodology for this research was inductive reasoning using triangulation methodology and qualitative comparisons. Research questions where proposed with propositions with the intent of developing tentative hypothesis which would contribute to conclusive theory.

In chapter 3 BSI threat catalog and baseline catalog deliberate acts where used to compare against the insider threat profiles. It was determined that BSI was technical in nature and did not address the behavior science indicators that would be helpful in identifying the increased risk of a person before an incident. ISMS are focused on deterrence by implementation of controls to prevent an incident, rather than identifying the risk associated with an individual. The difference in the two programs focus leads to a gap in capabilities. It was determined that insider threat profile provides more useful information than threats or acts offer by BSI, and therefore should be consider for improving current ISMS.

The second examination was RIA. RIA's importance in defending the X-Road was the primary reason for this organization's selection. If it has to do with e-governance, all roads lead to RIA. If it was determined that RIA's protection could be improved, then it is likely the improvements could be made all along the X-Road and drastically reducing Estonia's risk to insider threats. Insider fraud appeared to be the least interesting profile with regard to RIA, though further study is needed for a conclusive answer. IT sabotage, insider theft of IP, and espionage are considered profiles of interest for this organization. Even with RIA's elite implementation of the ISKE there is room for improvement when looking at the insider threat vector through the InTP lens. InTP span an organization and provide robust capabilities that are built on top of ISMS's. RIA's risk from insider threat would decrease after the implementation of an InTP.

The last comparison was reported abuse case to the insider threat profiles. EDPI and KAPO provided the largest contribution for comparison. EDPI provided statistics and some historical data of the organizations challenges over the years. KAPO reported a

number of cases the treason, espionage, and criminal neglect of classified materials. Additionally they painted a picture of aggressive espionage activity by Russia. EDPI has identified that a culture of abuse exists, however small, across many organization. These organizations include both government and private companies. Intent and behavior that fit the CERT profiles was not readily apparent, but PII abuses are clearly taking place. Corruption of processes and negligence are the two most common themes. All of these organizations have ISKE implemented and therefore have some degree of insider threat protection. What appears to be lacking is a security culture. Though not directly the intent of InTP's managing and developing an organization security culture is one of the functions.

The espionage cases examined from the KAPO documents clearly fit the espionage profile in form and fashion. Though the profile characteristics are general in nature they do indicate that a deeper look is warranted. KAPO's CI activities are clearly hard at work and not capable of conducting similar operations along the entire X-Road. As stated in chapter 2.3 InTP's address this issue specifically for organizations that traditionally do not have CI capabilities. Though Estonia does have insider threat behavior, it is not fully understood if InTP are a useful means to address insiders, whether unintentional, intentional, or state sponsored. Research from EDPI raises doubts while reports from KAPO confirm a real need.

Based on the data derived from this research Estonia can improve its protection from insider threats with the use of the insider threat profiles alone, but also by implementing insider threat programs in critical government agencies. A more in-depth study is warranted to provide clarity to EDPA findings and to expand what can be learned from Russian activities in both private and public sectors.

6.1. Study limitations

Evidence has been collected from open source documents. To reproduce this research it is recommended to conduct extensive surveys, based on those used to populate the CERT database. Investigation of the cases statistically reported by EDPI and KAPO would be classified in nature, similar to what has been done in the US, by CERT. Completing this research and creating such a database will provide Estonia with new tools for combatting the same old threats.

The Estonian language proved to be difficult hurdle to overcome also. Future works should attempt to look at ISKE directly rather than the ISMS that it was modeled after.

7. Conclusion

Insider threats are a growing concern worldwide. CERT has packaged over a 1000 incidents into profiles that allow organizations to better understand the individuals who perpetrate these crimes. This body of research intended to determine if an insider threat program would improve the security posture of the Estonia against insiders if adopted.

The examination of BSI is flawed in the respect that it should be a comparison with ISKE, the Estonian standard. This aside, it is clear that insider threat profiles have more to offer than descript statements concerning insider events or methods used in BSI. By design InTP's are more robust than ISMS and entail more capabilities. Estonia has an extremely high standard of information security, but no experience with implementing InTPs. Their success with ISKE indicates Estonia is entirely capable of building an InTP effectively and at a lower cost than those currently in operation. With this in mind, a closer study specifically addressing ISKE needs to be conducted to provide clarity on the value of the program to Estonia. It has been established that InTP do lower the risk associated with the insider threat vector by managing various capabilities that exist in most organizations.

RIA's operational profile does match three of the four profiles convincingly. The insider fraud profile requires a more in-depth look into RIA's operations before it can be validated. IT sabotage seems to be the greatest risk as such an event of scale could bring down the countries many services and functions. Second to this is espionage. Due to the aggressive nature of Estonia's largest neighbor, the possibility of espionage cannot be ignored. As reported in 2.2 the behavioral characteristics of this profile are shared with the IT sabotage profile. When RIA decides to implement a program this is a logical and complimentary place to start.

The historical cases pulled from EDPI proved to be the most curious data. This data set requires a more in-depth look. Clearly there are insider activity leading to the abuse of PII but no real use of the data for fraud, which is the profile most likely to abuse PII. Why this is the case cannot be determined at this point, but it is an interesting phenomena worth further investigation. CERT openly admits that the three profiles presented are not a complete work and that there are a number of cases that fall under miscellaneous. Where activity on which this data is built does highlight concerns, it does not indicate that these events match the insider threat profiles.

The comparison of the espionage cases fit the profiles well. Though the number of cases is limited, the perpetrators behaviors would have been identifiable to an insider threat program as risky. Therefore drawing the InTPs attention toward this individual at an earlier time and hence reducing the impact of their actions.

Estonia is well protected by ISKE and all that an ISMS has to offer. That was necessary yesterday, today requires additionally capabilities. InTP are a means of managing the insider threat specifically with the technologies and personnel that likely already exist in the organization. These capabilities are new to most organizations and have the potential to define the organizations security culture, raise awareness, and prevent, detect, and respond to insider incident when they occur. Because Estonia has chosen to make themselves so dependent on information technology, they must address insider threats directly and immediately. Though InTP are relatively new in nature, it has been established they address a gap that currently exists in ISMS's with regard to insider threats of all kinds. The noted exception is NIST Special Publication 800-53 Revision 4 which provides guidance or where to start, but is by no means a definitive instruction on the subject. With this in mind, the following recommendations are made based on the research and the belief that Estonia cannot afford to be a latecomer to this particular field of security.

7.1. Recommendations

The first recommendation is for RIA to examine insider threat programs and profiles. Internal knowledge is required to make a credible strategic recommendations. Many of the organizations presented during the current research, work with confidential information. Having an un-cleared outsider conducting such activities may be uncomfortable if not impossible. For this reason it is recommended RIA to initiates a study to assess Insider Threat Program's value, not only for RIA, but all organizations providing services on the X-Road. These organizations are nothing less than trusted business partners and must hold similar standards currently being delineated by ISKE. Due to RIA's technical expertise no other organization is more capable of preforming such an evaluation. As RIA is already fully employed, it is further recommended that a feasibility study should be completed by a government appointed independent consultancy with the appropriate clearances. Ideally such consultants should be familiar with the interworking of RIA and educated by CERT CMU.

This research was completed from the BSI standard in which ISKE was derived. Initial research indicates a gap with regard to the protection afforded by an InTP vice an ISMS, which BSI is. As ISKE is not available in English, direct research of ISKE's protection was not completed. It is recommended that RIA examines the ISKE's current protection for insider threats profiles offered by CERT to determine exactly what the risks are. Insider threat profiles do provide extensive data regarding three types of insider threat profiles. Amending ISKE to address CERT profiles rather than more general materials offered by BSI provides enhanced protection. It also lays the foundation for insider threat programs to be put into place with established controls. Should the aforementioned research determine InTP are of value, it is recommended ISKE to be immediately updated with due consideration for NIST Special Publication 800-53 Revision 4, focusing on insider threat amendments.

Furthermore, it is recommended that the Estonian Data Protection Inspectorate provides standard reporting methods from year to year. Current reporting by this agency was the only source of data concerning security violations. More granular data concerning misdemeanors and fines would not have only been helpful in current research, but would aid in maintaining transparency. While publishing violations do in fact happen is helpful, telling the story of why they are happening so people understand the mechanism that directly impact their lives, is more informative and raises awareness. Transparency of violation by those who are entrusted with access to privileged information is a fundamental necessity in maintaining the trust that has been built and thus far maintained by Estonia along the X-Road. This trust is the foundation on which Estonia's e-governance and information society rests, and in the future millions of e-residences may reside.

It is also recommended that violations will be made more public and kept in a central public registry. Once again, this is a matter of building trust and transparency. Making the information difficult to find serves no purpose except to bring into question what is not being reported, and why. This act acknowledges a problem and provides Estonia the opportunity to show the world Estonia is acknowledging the issue and dealing with it. It also allows Estonia to build a security culture to compliment the established information society.

The fifth recommendation addresses where to establish an InTP. Each organization will need to manage their own program. A centralized program, much like ISKE, in Estonia is a possibility considering the effectiveness of EDPI and requirements placed on those who provide services on the X-Road. Their capabilities already show promise with attribution of data violations. Similar capabilities will also be required by an InTP, with a different focus. The focus will be specific to the threat profile which poses the highest risk to the organization. As discussed in chapter 1.1 established intelligence or police agency are not a good choice as their mandates may conflict with that of an InTP. These agencies have specialized knowledge and skill-craft. This is helpful especially in investigations, but fall short in the scope of other activities InTP are required to attend to. The knowledge that is held in RIA and the EDPI are both key ingredients in developing and implementing InTP along the X-Road. RIA for the technical expertise and EDPI for their already existing capabilities and proximity to the Ministry of Justice. These organizations provide a logical proving ground before dissemination and implementing InTP's on a wider scale.

The former recommendations are all specific to Estonia and address current situation. Though there is research concerning insider threats outside of the United States, nothing has been offered that is supported by as much empirical data or that address strategic, governance, and policy issues when establishing these programs. Estonia is a nimble nation which allows it to lead where other European nations can only follow. The U.S. is responsible for the majority of insider threat research. Though Europe and the U.S. share strong ties, there are differences in these societies that will manifest themselves behaviorally. For this reason similar research should be conducted here in Europe. Insider threat programs are simply a genesis of information security programs into the realm of behavioral sciences. These programs will be adopted *en masse* in the future. First by the largest and richest, as they develop and become more affordable, to virtually all organizations. In Europe, currently no one is offering what CERT has presented to U.S. organizations; public and private. For this reason it is recommended that a research center be established in Estonia. The NATO Counter Intelligence Centre of Excellence in Krakow has been established, but as discussed, their capabilities do not fully address insider threats. The Cooperative Cyber Defence Centre of Excellence in Tallinn has already published their first paper on insider threat programs. This organization could legitimately conduct research throughout Europe, and in time, provide empirical data for

both to Europe as a whole and individual nations who participate. Becoming a partner to CERT is a straightforward process and the possibilities should be explored. Estonia has lead the way in e-governance, is a thought leader concerning the possibilities of an information society, has taken the initiative defining NATO's Cyber Security research, and should now take this opportunity to lead again.

In closing, insider threats pose a neglected and grave risk to any nation whose economy would be adversely effected by a disruption of information technology infrastructure. In the case of a country that is embracing e-governance, the risks posed by insiders may even be dire. It is doubtful that any single incident will bring down a nation. The events of 2007 visibly demonstrated the possibilities of a well-organized hacktivist youth group. Estonia has clear examples of insider behavior in its society and espionage in its most secure government institutions. Since 2007 the nation and its institutions have bolstered their defenses so that similar attacks can be dealt with. Nevertheless, in its current state, the nation and its economy have not directly addressed insider threats. It is recommended to take immediate steps to educate key decision makers and stakeholders on the potential of these programs and the vulnerability that currently exists. The nation's security depends on it.

8. References

[1] D. Cappelli, A. Moore and R. Trzecia, The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud), Upper Saddle River, NJ: Addison-Wesley Professional, 2012.

[2] The United States Department of Justice, "Identity Theft," The United States Department of Justice, 2 Nov 2015. [Online]. Available: http://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud. [Accessed 7 Dec 2015].

[3] E. McCallister, T. Grance and K. Scarfone, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," National Institute of Standards and Technology, April 2010. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf. [Accessed 8 Dec 2015].

[4] J. Bughin, M. Chui and J. Manyika, "Clouds, big data, and smart assets: Ten tech-enabled business trends to watch," *McKinsey Quarterly*, no. August, pp. 1-14, 2010.

[5] M. Sawhney and D. Parikh, "Where Value Lives in a Networked World," *Harvard Business Review,* vol. Reprint R0101E, no. January , pp. 79-86, 2001.

[6] D. D. Remenyi, "Analysis of the 2007 cyber attacks against Estonia from the information warefare perspective," in *Proceedings of the 7th European Conference on Information Warfare and Security*, Plymouth, UK, 2008.

[7] J. Manyike and C. Roxburgh, "The great transformer: The impact of the internet on economic growth and prosperity," October 2011. [Online]. Available: file:///C:/Users/Jeson/Downloads/MGI_Impact_of_Internet_on_economic_growth.pdf. [Accessed 2 November 2015].

[8] P. Paganini, "2013 - The Impact of Cybercrime," 1 Nov 2013. [Online]. Available: http://resources.infosecinstitute.com/2013-impact-cybercrime/. [Accessed 2 Nov 2015].

[9] PWC 18th Annual Global CEO Survey, "A marketplace without boundaries? Responding to disruption," Jan 2015. [Online]. Available:

http://www.pwc.com/gx/en/ceo-survey/2015/assets/pwc-18th-annual-global-ceo-survey-jan-2015.pdf. [Accessed 25 Nov 2015].

[10] PWC Global Economic Crime Survey 2014, "Global Economic Crime Survey 2014," 2014. [Online]. Available: http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey.html. [Accessed 25 Nov 2015].

[11] KPMG, "Cybercrime survey report 2014," 2014. [Online]. Available: https://www.kpmg.com/IN/en/IssuesAndInsights/ArticlesPublications/Documents/KPMG_Cyber_Crime_survey_report_2014.pdf. [Accessed 25 Nov 2015].

[12] Ernst and Young, "Global Information Security Survey 2014 Get ahead of cybercrime," Ernst and Young, Oct 2014. [Online]. Available: http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf. [Accessed 25 Nov 2015].

[13] National Institute of Standards and Technology, "Guide for Assessing the Security Controls in Federal Information Systems and Organizations," June 2010. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf. [Accessed 25 Nov 2015].

[14] ISO/IEC, "ISO/IEC 27001 - Information security management," 2013. [Online]. Available: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm. [Accessed 25 Nov 2015].

[15] ISACA, "COBIT 4.1," 2015. [Online]. Available: http://www.isaca.org/. [Accessed 25 Nov 2015].

[16] SANS, "CIS Critical Security Controls," 2015. [Online]. Available: https://www.sans.org/critical-security-controls. [Accessed 25 Nov 2015].

[17] National Security Agency, "Defense in Depth," National Security Agency Information Assurance Solutions Group – STE 6737, Fort Meade, 2010.

[18] C. Strohm, "Cybercrime Remains Growth Industry With $445 Billion Lost," 9 June 2014. [Online]. Available: http://www.bloomberg.com/news/articles/2014-06-09/cybercrime-remains-growth-industry-with-445-billion-lost. [Accessed 2 Nov 2015].

[19] D. Paletta, D. Yadron and J. Valentino-Devries, "Cyberwar Ignites a New Arms Race," The Wall Street Journal, 11 Oct 2015. [Online]. Available: http://www.wsj.com/articles/cyberwar-ignites-a-new-arms-race-1444611128. [Accessed 28 Oct 2015].

[20] M. Taves, "How fear and self-preservation are driving a cyber arms race," c|net, 2 May 2015. [Online]. Available: http://www.cnet.com/news/how-fear-and-self-preservation-are-driving-a-cyber-arms-race/. [Accessed 28 Oct 2015].

[21] SafeNet, "Breach Level Index," Gemalto, 27 Oct 2015. [Online]. Available: http://breachlevelindex.com/#sthash.b4DX6ito.l29MW1Wu.dpbs. [Accessed 27 Oct 2015].

[22] J. Menn, "Exclusive: Hacked companies still not telling investors," Reuters, 2 Feb 2012. [Online]. Available: http://www.reuters.com/article/2012/02/02/us-hacking-disclosures-idUSTRE8110YW20120202. [Accessed 28 Oct 2015].

[23] J. Mutch, "Beware The Coming SEC Regulations On Cybersecurity," Forbes, 15 May 2013. [Online]. Available: http://www.forbes.com/sites/ciocentral/2013/05/15/how-to-prepare-for-when-the-sec-comes-asking-about-cybersecurity-risk/. [Accessed 28 Oct 2015].

[24] D. Drinkwater, "Reporting cyber attacks should be "a legal requirement"," SC Magazine, 24 March 2014. [Online]. Available: http://www.scmagazineuk.com/reporting-cyber-attacks-should-be-a-legal-requirement/article/339433/. [Accessed 28 Oct 2015].

[25] D. Cappelli, A. P. Moore and T. J. Shimeall, "Protecting Against Insider Threat," 1 Feb 2007. [Online]. Available: http://www.sei.cmu.edu/library/abstracts/news-at-sei/securitymatters200702.cfm. [Accessed 2 Nov 2015].

[26] R. Trzeciak, "InTP Series: Establishing an Insider Threat Program (Part 1 of 18)," 4 March 2015. [Online]. Available: https://insights.sei.cmu.edu/insider-threat/2015/03/intp-series-establishing-an-insider-threat-program-part-1-of-18.html. [Accessed 2015 2 Nov].

[27] E. Cole, "Insider Threats and the Need for Fast and Directed," SANS Institute / SpectorSoft, April 2015. [Online]. Available: https://www.sans.org/reading-room/whitepapers/analyst/insider-threats-fast-directed-response-35892. [Accessed 28 Oct 2015].

[28] G. Ropohl, "Philosophy of Socio-Technical Systems," Society for Philosophy and Technology, 1999. [Online]. Available: http://scholar.lib.vt.edu/ejournals/SPT/v4_n3html/ROPOHL.html. [Accessed 15 Nov 2015].

[29] P. Runeson, M. Host, A. Rainer and B. Regnell, Case Study Research in Software Engineering Guidelines and Examples, Hoboken, Jew Jersey: John Wiley & Sons, Inc, 2012.

[30] Cyber council: Insider Threat Task Force, "A Preliminary Examination of Insider Threat Programs in the U.S. Private Sector," September 2013. [Online]. Available: file:///C:/Users/Jeson/Downloads/A%20Preliminary%20Examination%20of%20Insider%20Threat%20programs%20in%20the%20U.S.%20Private%20Sector%20(2).pdf. [Accessed 6 Nov 2015].

[31] Biblica, The NIV Bible, Grand Rapids Michigan: Zondervan, 2011.

[32] Chairman of the Joint Chiefs of Staff, "Joint Intelligence, Joint Publication 2-0," 2013. [Online]. Available: http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf. [Accessed 15 Sept 2015].

[33] Carnegie Mellon University, "Insider Threat Program Manager (ITPM) Certificate," [Online]. Available: http://www.cert.org/insiderthreat/insider-threat-program-manageritpm-certificate.cfm. [Accessed 15 September 2015].

[34] T. R. Peltier, Information Security Risk Analysis, Boca Raton: Auerbach, 2001.

[35] B. Akhgar and S. Yates , We Have Met the Enemy and They Are Us: Insider Threat and Its Challenge to National Security, Waltham, MA: Elsevier Inc, 2013.

[36] E. Cole and S. Ring, Insider Threat Protecting the Enterprise from Sabotage, Spying, and Theft, Rockland, MA: Syngress Publishing Inc., 2006.

[37] C. Colwill, "Human factors in information security: The insider threat - Who can you trust these days?," Information Security Technical Report 14 / Elsevier Ltd., 2010. [Online]. Available: http://ac.els-cdn.com/S1363412710000051/1-s2.0-S1363412710000051-main.pdf?_tid=41614d44-8942-11e5-b837-

00000aab0f6c&acdnat=1447335516_9c1c44bdb138f9047fc288ac26d29292. [Accessed 14 Nov 2014].

[38] D. L. Charney, "True Psychology of the Insider Spy," National Counterintelligence and Security Center, Fall/Winter 2010. [Online]. Available: http://www.ncsc.gov/issues/docs/Charney-PsychologyofInsiderSpyAFIO-INTEL_Fall-Winter2010.pdf. [Accessed 6 Nov 2015].

[39] CERT Insider Threat Center in Insider Threat , "Insider Threat Blog," CERT Software Engineering Institute Carnegie Mellon University, 17 Oct 2013. [Online]. Available: https://insights.sei.cmu.edu/insider-threat/2013/10/-analyzing-insider-threat-data-in-the-merit-database.html. [Accessed 29 Oct 2015].

[40] M. Kont, M. Pihelgas, J. Wojtkowiak, L. Trinberg and A.-M. Osula, "NATO Cooperative Cyber Defence Centre of Excellence," NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia, 20 Dec 2015. [Online]. Available: https://ccdcoe.org/sites/default/files/multimedia/pdf/Insider_Threat_Study_CCDCOE.pdf. [Accessed 21 Dec 2015].

[41] S. Band, D. Cappelli, L. F. Fischer, A. P. Moore, E. D. Shaw and R. F. Trzeciak, "Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis," Dec 2006. [Online]. Available: http://resources.sei.cmu.edu/asset_files/TechnicalReport/2006_005_001_14798.pdf. [Accessed 29 Oct 2015].

[42] National Institute of Standards and Technology, "NIST Special Publication 800-53," National Institute of Standards and Technology, April 2013. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. [Accessed 24 Dec 2015].

[43] A. Raintamm, "Estonian Security System Overview," Riigi Infosüsteemi Amet RIA, 2012. [Online]. Available: https://www.ria.ee/public/ISKE/ISKE_english_2012.pdf. [Accessed 15 Nov 2015].

[44] Federal Office for Information Security, "BSI-Standards," Bundesamt für Sicherheit in derInformationstechnik, 2015. [Online]. Available: https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html. [Accessed 23 Nov 2015].

[45] Estonian Information System's Authority, "Three-level IT baseline security system ISKE," Estonian Information System's Authority, 10 5 2012. [Online]. Available: http://archive-ee.com/page/711796/2012-11-20/https://www.ria.ee/iske-en. [Accessed 23 Nov 2015].

[46] T. Viira, "ISKE: IT Grundschutz in Estonia," Estonian Informatics Centre, 2010. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/Grundschutz/3GS_Tag_2010/ISKE.pdf?__blob=publicationFile. [Accessed 23 Nov 2015].

[47] Ferderal Office for Information Security, "Supplement to BSI-Standard 100-3, Version 2.5," Ferderal Office for Information Security, 03 August 2011. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/supplement_to_100-3.pdf?__blob=publicationFile&v=1. [Accessed 23 Nov 2015].

[48] Bundesamt für Sicherheit in der Informationstechnik, "G 5 Deliberate Acts," Federal Office for Information Security, 2015. [Online]. Available: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05.html. [Accessed 20 Dec 2015].

[49] International Telecommunication Union, "Estonia ranks fifth in the global cybersecurity index," International Telecommunication Union, 2015. [Online]. Available: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Estonia-ranks-fifth-in-the-global-cybersecurity-index.aspx. [Accessed 15 Nov 2015].

[50] Estonian Information System Authority, "2014 Annual Report Cyber Security Branch Of the Estonian Information System Authority," Estonian Information System Authority, 15 Apr 2014. [Online]. Available: https://www.ria.ee/public/Kuberturvalisus/RIA-Kyberturbe-aruanne-2014_ENG.pdf. [Accessed 3 Dec 2015].

[51] G. Anthes, "Estonia: A Model for e-Government," *Communications of the ACM*, vol. 58, no. 6, pp. 18-20, June 2015.

[52] The Economist, "Estonia takes the plunge," 28 Jun 2014. [Online]. Available: http://www.economist.com/news/international/21605923-national-identity-scheme-goes-global-estonia-takes-plunge. [Accessed 15 Nov 2015].

[53] G. Anthes, "Estonia: A Model for e-Government," *Communications of the ACM*, vol. 58, no. June, pp. 18-20, 2015.

[54] Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, "Personal Data Protection Act," Riigikantselei 2010, 2007. [Online]. Available: https://www.riigiteataja.ee/en/eli/509072014018/consolide. [Accessed 21 Dec 2015].

[55] Data Protection Inspectorate, "Report concerning the performance of the personal data protection act and the public information act 2006," Data Protection Inspectorate, 2006. [Online]. Available: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/2006_English%20version.pdf. [Accessed 21 Dec 2015].

[56] Estonian Data Protection Inspectorate, "Annual Reports," Estonian Data Protection Inspectorate, 2015. [Online]. Available: http://www.aki.ee/en/inspectorate/annual-reports. [Accessed 21 Dec 2015].

[57] A. Rull, E. Täks and A. Norta, "Towards Software-Agent Enhanced Privacy Protection," Springer International Publishing Switzerland, Tallinn , 2014.

[58] Estonian Security Police, "Annual reviews," Estonian Security Police, 2015. [Online]. Available: https://www.kapo.ee/en/content/annual-reviews.html. [Accessed 21 Dec 2015].

[59] J. FITSANAKIS, "Estonian intel officer comes out as Russian spy in TV interview," IntelNews.ORG, 17 DECEMBER 2014. [Online]. Available: http://intelnews.org/tag/kapo-estonia/. [Accessed 13 Dec 2015].

[60] Kaitsepolitseiamet, "Judicial decisions Treason," Kaitsepolitseiamet, 2015. [Online]. Available: https://www.kapo.ee/en/content/judicial-decisions.html. [Accessed 2 Dec 2015].

[61] J. J. I. B. G. Rumbaugh, The Unified Modeling Language User Guide, Addison-Wesley, 2005.