CCDCOE

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

Markus Kont, Mauno Pihelgas, Jesse Wojtkowiak,

Lorena Trinberg, Anna-Maria Osula

Insider Threat Detection Study

www.ccdcoe.org
publications@ccdcoe.org

Executive Summary

This study focuses on the threat to information security posed by insiders (i.e., *insider threat*) as the recent cases of Edward Snowden, Chelsea Manning, and Herman Simm have highlighted the significant risks of *"good guys gone bad"* within a defence structure. Insider threat has to, in particular, be explored as most security frameworks focus on intrusions by external actors. But what happens if the malicious user is able utilise internal channels to access your systems? What if the perpetrator is someone who you trust? How do you detect and deal with a destructive and hostile insider with a security clearance?

Our work provides a comprehensive overview of insider threat, examines a selection of high-profile incidents and existing research. The analysis takes an interdisciplinary approach, discussing insider threat from technical, legal, and behavioural perspectives.

The authors outline the key components of an Insider Threat Programme and propose guidelines to assist organisations that are planning to implement their own programme. Additionally, the study provides legal analysis of seven scenarios that combine the questions and concerns that surfaced during the study.

In order to understand what drives different insiders to malicious deeds, it is essential to establish profile types. We analyse five distinct insider profiles:

- Sabotage;
- Theft (of intellectual property);
- Fraud;
- Espionage;
- Unintentional insiders.

An Insider Threat Programme is not a product that can be bought off the shelf, but rather a continuous process. The programme offers the organization the ability to identify and prevent changing risks, detect an incident as it occurs, and once an incident has occurred, respond to the incident in an efficient manner. The analysis and lessons learned from incidents will feed information back into the planning phase, allowing to continuously develop and improve the programme.

The main idea is to notice various technical and non-technical detection indicators that can lead to incidents. We propose six different categories of detection indicators – three are related to behavioural aspects, while the remaining three are more technical. For every indicator, we assess its relevance to each of the insider profiles. Most importantly, when analysed and handled properly, these indicators act as precursors that accompany different threats. Early or timely detection allows to minimise the damage, or in best case prevent the incident altogether.

This research topic was brought forward by the German Armed Forces within a Request for Support to the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) dated 25 March 2014. The request was submitted through the NATO CCD COE Steering Committee and was approved for implementation.

About the NATO CCD COE

The NATO Cooperative Cyber Defence Centre of Excellence is an international military organisation accredited in 2008 by NATO's North Atlantic Council as a 'Centre of Excellence'. Located in Tallinn, Estonia, the Centre is currently supported by the Czech Republic, Estonia, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, Turkey, the United Kingdom, and the United States of America as Sponsoring Nations and Austria, and Finland as a Contributing Participants. The Centre is neither part of NATO's command or force structure, nor is it funded by NATO. However, it is part of a wider framework supporting NATO Command Arrangements.

NATO CCD COE's mission is to enhance capability, cooperation and information sharing between NATO, NATO member states and NATO's partner countries in the area of cyber defence by virtue of research, education and consultation. The Centre has taken a NATO-oriented interdisciplinary approach to its key activities, including academic research on selected topics relevant to the cyber domain from the legal, policy, strategic, doctrinal and/or technical perspectives, providing education and training, organising conferences, workshops and cyber defence exercises, and offering consultations upon request.

For more information on NATO CCD COE, visit the Centre's website at http://www.ccdcoe.org.

Table of Contents

1. Introduction 7
   1.1. Scope 8
   1.2. Motivation 8
   1.3. Outline 8
   1.4. Acknowledgements 8
2. High-profile Examples 9
   2.1. Edward Snowden 9
   2.2. Chelsea Manning 9
   2.3. Daniel Ellsberg 9
   2.4. Herman Simm 10
   2.5. Nidal Malik Hasan 10
   2.6. Summary 10
3. Introducing the Insider Threat Programme 12
   3.1. Insider Threat Definition 12
   3.2. Insider Threat Programme in Comparison to Counter-Intelligence 13
   3.3. Insider Threat Profiles 14
      3.3.1. Sabotage 15
      3.3.2. Theft of Intellectual Property 16
      3.3.3. Insider Fraud 16
      3.3.4. Espionage 17
      3.3.5. Unintentional Insider 18
   3.4. Complexity of Insider Threats 18
   3.5. Threat Timeline and Detection 19
   3.6. Key Components of Insider Threat Programmes 20
   3.7. Summary 22
4. Creating an Insider Threat Programme 23
   4.1. Insider Threat Programme Roadmap and Life Cycle 23
      4.1.1. Initial Planning and Identifying Stakeholders 24
      4.1.2. Achieving Leadership Buy-in 24
      4.1.3. Ensuring Sustained Buy-in From Leadership 25
      4.1.4. Completing the InTP Life Cycle 26
   4.2. Exploring the Road Less Travelled 26
   4.3. Detection Indicators 28
      4.3.1. Personal Indicators 29

4.3.2. Behaviour Indicators 30
4.3.3. Background Indicators 31
4.3.4. Computer Networks Indicators 33
4.3.5. Client-side Indicators 34
4.3.6. Service Indicators 36
4.4. Summary 36
5. Legal Analysis 38
5.1. Immediate Termination of the Employment Contract and Revocation of All Access Rights 38
5.1.1. Legal Assessment 38
5.1.2. Recommendation 39
5.2. Hand-picking Users for Data Stream Monitoring 39
5.2.1. Legal Assessment 40
5.2.2. Necessity to Make a Decision and the Existence of Concrete Suspicion 41
5.2.3. Recommendation 41
5.3. An Automated Monitoring System Requires Human Intervention in Interpreting Data 41
5.3.1. Legal Assessment 42
5.3.2. Means of Automated Monitoring 42
5.3.3. Devices and Accounts Provided by the Employer 43
5.3.4. Monitoring Employee's Internet Traffic 45
5.3.5. Notification of Monitoring Activity 46
5.3.6. Recommendations 46
5.4. Requiring Essential Personnel to Relinquish Their Private Cryptographic Keys 46
5.4.1. Differentiation between Private and Work-only Use 47
5.4.2. Recommendation 47
5.5. Requiring Essential Personnel to Relinquish Their Communication Devices for Inspection. 47
5.5.1. Return of the Device Provided by the Employer 48
5.5.2. Handing Out the Private Device 49
5.5.3. Recommendation 49
5.6. Conducting Forensic Activities on Any Devices which are Provided by Contractors 49
5.6.1. Conditions Subject to Service Contract 50
5.6.2. Recommendation 50
5.7. Setting Up Decoy Targets 50
5.7.1. Legal Assessment 50
5.7.2. Recommendation 51
6. Future Work 52
7. Project Summary 53

1. Introduction

The world has gone through immense changes in recent decades. While this statement applies to several domains, the field of Information Technology must be mentioned specifically. We now have an immense capability to store, process and transmit data, to an extent that traditional paper documents are being replaced by or converted to digital media. As an example, in Estonia digital and handwritten signatures are considered equal.

When the concept of interconnected computer systems was originally envisioned, it was assumed that every member was to be trusted. Popularisation of interconnected computers has proven that it is not the case, and therefore security in cyberspace has received significant attention in recent years. Often, the security framework focuses on perimeter defence, with the main question being *'Is this a valid user?'* But what happens if the perpetrator uses internal channels to access the systems? What if it is someone who you trust? An insider with a security clearance?

In recent years, several high-profile cases have emerged where a trusted individual inflicted great harm on an organisation. For example, Stuxnet attacks stalled the Iranian nuclear programme by sabotaging the *programmable logic computers* (PLC), which controlled centrifuges for nuclear material separation [1]. Such facilities commonly use private networks with no uplink and strict access policies: thus, the most logical conclusion is malware infiltration by an insider. It is unclear whether that person committed the sabotage willingly, but the payload only activated upon very specific criteria. Therefore, it is feasible that initial infections occurred outside the facility, with technicians responsible for maintenance of PLCs being the primary target. The technician would then unknowingly carry an infected media drive into the secure facility, where the payload activated on the PLC maintenance computers. Note that contractors are often used to develop or maintain critical systems, which was also the case with Edward Snowden [2]. He was a system administrator within the Central Intelligence Agency (CIA), and later a contractor for Dell and Booz Allen Hamilton, where he was assigned to manage (and design) systems for one of their largest clients, the National Security Agency (NSA). As a result, he had access to highly classified data, which he collected over several years. He disclosed all the documents to journalists in 2013, who in turn publicised them in high profile media outlets such as *The Guardian, Der Spiegel, The Washington Post* and *The New York Times*. Before the Snowden incident, in 2010, Chelsea Elizabeth Manning (formerly known as Bradley Edward Manning) released Iraq and Afghan war logs to Wikileaks, a site dedicated to releasing classified information [3] [4]. Among the material was the controversial *'Collateral Murder'* video, documenting a friendly fire incident where an Apache attack helicopter attacked journalists in Baghdad.

Insider threat is not a novel concept, nor has it emerged with digital media. Snowden and Manning can be compared to Daniel Ellsberg, who released 'the Pentagon Papers', a top secret study of US political and military involvement in Vietnam [5] [6]. Ellsberg was involved in writing the study but came to oppose the war. Furthermore, Herman Simm, a former chief of the Estonian Ministry of Defence's security department, was accused of spying for a foreign nation [7]. He pleaded guilty and was sentenced in 2009 [8]. A stark example is Nidal Malik Hassan, who was a US Army psychiatrist and responsible for murdering 13 people. He had exchanged e-mails with a known al-Qaeda member prior to the mass shooting, and had been investigated by the FBI [9]. No pre-emptive action was taken, however, and concerns over his behaviour were dismissed.

Therefore, in today's organisational networks, malicious insider actions are a prominent threat which could have serious consequences, and a comprehensive Insider Threat Programme (InTP) must be implemented. The threat is often not properly addressed, as a certain level of trust has already been established with an insider. Better understanding of the problem background must be formulated, which has to be integrated with modern incident mitigation techniques, both technical and organisational. Additionally, the legality and feasibility of the techniques must be considered.

1.1. Scope

The purpose of this study is to provide a comprehensive overview of the insider threat concept and possible mitigation methods. An assessment of the effectiveness of each method will be conducted, along with analysis from the legal perspective.

1.2. Motivation

The threat posed by insiders is frequently reported to be one of the most important reasons in cases of successful data exfiltration. While this threat is presumably widely known in IT security circles, it does not seem to have received the same attention from senior decision-makers. Also, most IT security efforts and available technologies seem to focus on detecting incoming malicious cyber activities, while, in contrast, methods or technologies to detect malicious insiders and to prevent their actions seem raw. Privacy laws and regulations seem to introduce an additional layer of complexity while dealing with this issue.

The potentially high threat posed by insider attacks is probably shared among NATO and its Allies and it might be safe to assume that many of the NATO Nations' military organisations also struggle with finding means and methods to counter this threat while respecting privacy law, especially on an operational level. This study should help to start discussions and further actions, on different levels, on how to face and in the end mitigate the threat posed by insiders.

1.3. Outline

Chapter 2 provides an overview of insider threat, based on case studies and existing research. In Chapter 3, a more elaborate introduction to the insider threat will be provided. We will also describe different insider profile types and outline the key components of an Insider Threat Programme (InTP). Then, in Chapter 4, creation of an InTP will be discussed in more detail. We will also provide some example detection indicators to assist organisations that are planning to implement their own programme. Chapter 5 provides legal analysis of seven scenarios that combine the questions that surfaced during the study. Future work will be presented in Chapter 6, and the primary ideas of the study will be summarised in Chapter 7.

1.4. Acknowledgements

The authors would like to thank everyone for their ideas and support to develop this study. Special gratitude goes to MAJ Dr Christian Czosseck, Hillar Aarelaid, Johannes Tammekänd, LT Raik Jakschis, and Teemu Uolevi Väisanen.

2. High-profile Examples

This chapter provides a concise overview of insider threat cases. Access to such information is often restricted, therefore we do not aim to cover all incidents but only the most publicly prevalent. Additionally, several cases are not related to cyberspace, but provide valuable considerations for anyone interested in implementing an InTP.

2.1. Edward Snowden

Edward Joseph Snowden's youth was spent online – tinkering with computers, being vocal in chat rooms, and immersing himself in Japanese popular culture. He did drop out of high school at age 15 but, as his later career proved, his years before employment were not idle. It is agreed that significant self-education occurred during that period. He left the army after a training accident in Georgia when he broke both his legs, and was hired in 2006 as a computer engineer by the Central Intelligence Agency (CIA). There he was responsible for maintaining network security, a position which requires top-secret security clearance. Nothing in his background indicated malicious intent. [2] [10]

Snowden later stated that he first contemplated leaking confidential information in 2008, after being assigned to Geneva. He departed the CIA in 2009, details of this are unclear, he allegedly clashed with his supervisors. His next employer, Dell, served as an outsourcing contractor for the National Security Agency (NSA). Snowden had a successful career at Dell designing IT infrastructure solutions, initially in the NSA facility in Yakota Air Base, Japan. The final months before the now well-known incident were spent as a high-level system administrator to NSA's Kunia Regional Security Operations Centre, now working for the Booz Allen Hamilton consulting company. [2] [11]

The first illegal downloads of classified documents were conducted in the summer of 2012. On December 1, 2012, Snowden made his first contact with Glenn Greenwald, a lawyer and a journalist, requiring his PGP[1] key to establish a secure connection. They finally met in Hong Kong, where Snowden disclosed an unknown number of digital documents. [2] [12]

2.2. Chelsea Manning

Bradley Edward Manning, who was later legally recognised as Chelsea Elizabeth Manning, was born in 1987. Gender identification issues led to a life of bullying and isolation, which also transferred into her service in the US Army, which she joined in 2007 with hope to resolve her personal questions. The military environment proved unsuitable to Manning, who, being restricted by the US military's *'don't ask, don't tell'* policy, became an anonymous gay rights activist. Despite being noted by her supervisors for instability and being sent for mental health counselling, Manning was deployed to Iraq where she had access to classified information. [3]

In April, 2010, a classified video of a friendly fire incident was released in WikiLeaks, after which Manning's behaviour became increasingly erratic. This manifested in her sending a picture of herself wearing a wig to her supervisors, and making public statements in social media about her crisis. She allegedly approached Adrian Lamo, a former hacker, with a confession, and he reported Manning to the authorities. [4]

2.3. Daniel Ellsberg

Daniel Ellsberg, born in 1931, was a strategic analyst for RAND Corporation[2] from 1959 to 1971, and an Anti-War activist. He graduated Harvard *summa cum laude* in 1952, received a Woodrow Wilson Scholarship and studied economics for a year at Cambridge, and then served in the US Marine Corps between 1954 and 1957 (extending his service to serve in the US 6th Fleet during the Suez Crisis in 1956), before completing his PhD in

[1] Pretty Good Privacy - Program often used for signing and encrypting texts, emails and files. PGP relies upon a 'web of trust', which means that public key can be signed by a third user to attest to validity of key ownership.
[2] RAND Corporation, which was formed in 1948, is a non-profit organization that advised US government on strategy and decision-making.

Economics in 1962. He popularised the 'Ellsberg Paradox', whereby in some situations people's choices violate the expected utility. [5]

In 1964, he worked as a researcher under the direction of Secretary of Defence on secret plans to escalate the war in Vietnam, despite personal objections and increasing resentment for the conflict (witnessing the war first-hand between 1965 and 1967). The 7000 page study dubbed 'the Pentagon Papers' was completed later that year. Having read the entire document, and convinced of governmental wrongdoings, Ellsberg began photocopying it in 1969. Much time in 1970 was spent on unsuccessful attempts to convince Senators to publicise the papers, and in 1971 Ellsberg presented the papers to *The New York Times*. Despite being initially accused of 12 federal felony counts, with a possible sentence of 115 years in prison, all charges were dismissed in 1973. [6]

2.4. Herman Simm

Herman Simm, born in 1947, was a former Estonian police officer, chief of police, and the head of the Estonian National Security Authority in Ministry of Defence (MoD). He is also one of the most damaging spies in NATO history, and is currently serving a 12-year prison sentence for disclosing national and international classified information to a foreign government. [7]

He joined the police and the Communist Party in the 1970s, and had reached the rank of colonel when the Soviet Union disintegrated. Former ties were often ignored during the turbulence of forming Republic of Estonia. Additionally, Simm was hailed a hero for organising the defence of parliament when Soviet hardliners attempted to seize it in May 1990.

In 1995, after allegedly being recruited by KGB successors during a trip to Tunisia, Simm was appointed Director of the Analysis Division in the Estonian MoD. He started making photocopies or photographs of documents, which he would then place in empty drinking cartons and leave in designated garbage cans. [13]

His security clearance was raised to international status when Estonia entered NATO in 2004. He was cleared by multiple countries due to his service record, allowing Simm to expose NATO inner workings to Russia. Documents entrusted to him were often noted for improper handling, but with Simm being a trusted high-level official who had a say in making the rules, no concerns were raised. He was finally caught in 2008, after being placed under surveillance when a handler unwittingly exposed Simm as an asset. [13]

2.5. Nidal Malik Hasan

Nidal Malik Hasan, born in 1970, was a US Army psychiatrist. He is currently on death row for the Fort Hood mass shooting on November 5, 2009. He obtained a BSc degree in Biochemistry in 1997 and a medical degree in 2001, followed by an internship and fellowship at the Walter Reed Army Medical Centre in 2003. In 2009 Hasan was an active member of the Dar al-Hirjah Mosque and Islamic Centre, which was known for facilitating radical followers of Islam, including several September 11 hijackers. He also had made numerous statements regarding his religious beliefs, including a statement that *'nonbelievers should be beheaded'*, and warnings about his instability were issued two years prior to the incident. Warning signs, including an e-mail exchange with known extremist Anwar al-Awaki which was investigated by the Federal Bureau of Investigations (FBI), were not acted upon. Therefore, Hasan was allowed to continue on a path which culminated in the massacre. The alleged catalyst was his upcoming deployment to Afghanistan, and his fear of possible combat with fellow Muslims. [9]

2.6. Summary

These examples range from social criticism (Ellsberg and Manning) to terrorism (Hasan), but what they all share are clear preliminary warning signs. Ellsberg actively campaigned for releasing the Pentagon Papers, Manning and Snowden had confrontations with their superiors, Simm handled classified documents improperly, and Hasan was not silent about his radical convictions. Alarming indicators were available, but they were not properly monitored nor managed.

It should be noted that charges against Ellsberg were dismissed, while Simm, Manning and Hasan are serving prison sentences, the latter on death row. Only after Ellsberg's concerns were ignored by the official channels did he decide to leak the material. Snowden can be seen as a modern-day Ellsberg, but it is unclear if he attempted to report his concerns. By comparison, Manning and Hasan were clearly disturbed individuals. Manning performed cyber espionage and displayed behavioural indicators. Hasan performed non-cyber sabotage, and displayed behavioural and technical indicators. Therefore, an InTP should provide a framework for early detection and intervention without simultaneously creating a constrictive working environment. These concepts are discussed in subsequent sections.

One prominent organisation which maintains a database of insider threat incidents is the CERT Division of the Software Engineering Institute (SEI) at Carnegie Mellon University (CMU). With the information gathered from this database, the CERT Division has published a number of best practices and technical papers (available from [14]) on various aspects of insider threat detection. The empirical data is confidential, and only an anonymised overview is publically available. Thus they lack what public cases provide – an insight into the chain of events which culminate in an insider incident.

We shall now proceed with introducing the Insider Threat Programme (InTP).

3. Introducing the Insider Threat Programme

During a recent survey of more than 500 security professionals from US corporations and government institutions, 44% of participants cited insider threats [15]. Another survey of nearly 700 IT professionals revealed that 88% of the respondents recognise insider threat as a cause for alarm but have difficulty in identifying specific threatening actions they should be monitoring [16]. For this reason, insider threat detection has received a lot of attention during the last decade, and a number of research papers have been published in this field. The purpose of this section is to provide more in-depth discussion on definitions, various insider profiles, and finally building up to describe the key concepts of an InTP.

3.1. Insider Threat Definition

The terms *insider* and *insider threat* can seem intuitive, but according to several articles [17] [18] and [19], lack a clear definition. An *insider* can be a member of an organisation, an associate (contractor, business partner or guest), anyone with authorisation[3] to perform certain activities, anyone who is authenticated[4] by the system (including unauthorised users using valid credentials), or an unwilling or coerced accomplice to an external actor. A person who has stopped being an associate or member of a certain organisation can still be considered as an insider if that person's credentials have not been properly revoked or the person is (mis)using previously acquired knowledge. As argued in [20], the definitions can be divided into three categories – based on knowledge, access and trust.

According to the first argument in [20], a system may be compromised through *knowledge*, or defensive measures can be bypassed if the person is aware of their placement. This is common when system security is achieved by obscurity. For example, an insider who is responsible for software development may possess knowledge of several zero-day[5] vulnerabilities in the product. Exploitation of those vulnerabilities may not be dependent on affiliation or assigned privileges. Therefore any person with privileged knowledge of internal systems can be considered an insider. By following this logic, an outside threat agent can be become an insider if they acquire such knowledge.

From the technical perspective, as discussed in [20], an IT system simply verifies that provided credentials are valid, and the authenticated user is allowed to access a resource. Therefore any person who were to acquire valid system credentials could be considered an insider, again including external threat agents. As discussed in [17], employees sometimes bypass established procedures to simplify their tasks. While manifestation is clearly a security breach, and its result can be an incident, the motivation is generally not malicious. If existing policies do not allow employees to accomplish their tasks then these workarounds may improve efficiency, or prove to be the only viable solution. Example 1 in [20] presented a scenario where an employee needed to prepare for a Monday meeting over weekend. As there were no viable options for working remotely, she chose to remove the hard drive from her computer. Upon returning to work on Monday, with the intention to return the device, her actions had been discovered and she no longer had access to the facility.

CERT Division defines malicious insider as *'a current or former employee, contractor, or business partner'* [21]. Additionally, the insider *'has or had authorised access to organisation's network, system, or data'*, and *'has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability of the organisation's information or information systems'* [21]. This definition shares similarities with third argument in [20], which proposes that an insider be defined as a person who is empowered with *trust* from an organisation to access internal resources, to carry out actions in its name, and to be affiliated with it. The technicalities which would allow external agents to be included within the *insider* definition can be neglected without ruling out the possibility of outside influence. Control methods for

[3] Authorisation is the verification that connection attempt is allowed.
[4] Authentication is the verification of the credentials of the connection attempt.
[5] Zero-day vulnerability is a flaw in a computer system which is unknown to the vendor, therefore it can be exploited before control methods exist.

protecting confidentiality of privileged knowledge[6] and verification of system credentials[7] should be in place regardless of InTP implementation. E.g. an InTP should aim to prevent valid users from giving privileged knowledge or access to the third party.

An insider could be unknowingly used as an attack vector to achieve this result. This conforms to the *trust* concept in [20] but conflicts with [21]. Regardless of intent, an InTP should protect assets against trusted individuals. The definition and scope of an Unintentional Insider will be presented in section 3.3.5.

3.2. Insider Threat Programme in Comparison to Counter-Intelligence

An Insider Threat Programme (InTP) is not the same as a Counter Intelligence (CI) Programme. Counter Intelligence, as defined by the Joint Publication 2-0, Joint Intelligence (2013) in [22] 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 organisations, or foreign persons, or international terrorist activities'.*

CI is focused on agents of a foreign government operating inside the organisation or country. This definition overlaps only a sliver with the scope that InTP will cover. CI has traditionally been associated with intelligence agencies or security services which are exclusively government funded and sponsored. InTPs include government organisations 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 organisations' security requirements [23].

InTPs are operated to prevent incidents caused by their employees, no matter their country of origin. This is not to say that espionage against a nation's businesses is not of interest to governments' CI operations; only that the chances of defending against and prosecuting such activity have a greater chance of success if an InTP is instituted inside the targeted organisation. National CI operations were fully employed before the information age, but they do not have the resources to take care of national infrastructure, and the non-government organisations that operate under it.

InTPs require a multidisciplinary approach in order to be successful. Expertise from the CI community has been identified by CERT of Carnegie Mellon as a key ingredient to the programme's success [23]. Successful programmes have also included: legal input; Human Resources (HR); top Level support from the organisation's leadership (a champion); financial specialists; law enforcement; behaviour specialists; technical support from records management; data architects; system network architecture specialists; information assurance; and senior technologists. There are many questions that must be answered with all of these members in a room. Their knowledge and leadership is required to ensure that a programme is developed that has addressed their area of expertise. Questions will need answered that span the breadth of the specialties that are represented; ensuring that Information Assurance policies do not violate the organisation's HR or legal policies, for example. After understanding legal and HR issues, technically inclined members of the InTP can determine how best to implement a new practice. InTP are intended to span an organisation. Understanding and protecting critical assets, while maintaining the integrity of the organisational culture, is the ultimate goal [24]. Considerations (technical, legal, or otherwise) must be answered before implementation is started. Each organisation has specific critical infrastructure and culture. These factors will influence how a programme is designed and implemented. Standardised InTPs risk creating vulnerabilities by not addressing the key components identified by your specialist.

[6] Role Based Access Management (RBAC) is commonly used. Each system user is assigned into roles. Each resource is assigned roles, along with permissions for each role; e.g. workers can only read files while managers can also create new.
[7] Two-factor authentication is often used to verify weather access request is made by valid user. Randomly generated confirmation code is sent to user via alternative channel, usually via Short Message Service (SMS), which user would then enter during second stage. Access is granted if both stages are validated.

3.3. Insider Threat Profiles

The need to establish insider threat profiles was indicated by the United States Department of Defense (US DoD) in 2000, which is also when the research by the CERT Division was initiated [21]. Since that time a number of other US government agencies have also initiated studies, and used the research material to better understand this problem. These agencies include the Secret Service, Department of Homeland Security, Department of the Treasury, and later the US banking and financial sector. [14] [25]

Before introducing the individual insider threat profiles, the constraints of this research will be presented to provide a better understanding of what value this research offers in terms of the benefits of an Insider Threat Programme for an organisation.

Organisations are reluctant to report incidents (as stated in [26]). For government agencies and contractors, this is due to the nature of classified information. In the case of companies not associated with classified information, public embarrassment impacts customer confidence in the brand or credibility of the organisation, institution, or agency. Due to the reluctance in reporting insider incidents, the number of actual cases could be significantly higher [23]. Insider threat programmes offer procedures and policies that allow an organisation to execute a pre-defined course of action, to include:

- Inquiries – internal investigations to determine the nature of the offence and how to proceed; and
- Investigations – when an inquiry has determined that the course of action should include legal prosecution of the individual for the incident.

Most comprehensive insider threat profiles were developed by CERT Division of the CMU [14]. Although these insider profiles are exclusively pulled from US cases, no greater body of knowledge regarding case studies currently exists on real insider incidents [27]. Their research extensively dissected over 700 cases that produced 4 clear profiles in [28] and [29]. This data is entirely based on convicted insiders who had malicious intent. It does not reflect unintentional insider activities and the risk they pose to an organisation. IT Sabotage (134 cases), fraud (235 cases), theft of Intellectual Property (IP) (90 cases), and espionage (120 cases). Espionage is not explored publicly by CERT as the information is classified and not available for public examination. The four profiles presented in Table 1 were constructed mainly from [30] and [31]. CERT has created a miscellaneous category that constituted 52 insider threat cases. This is an indicator that other profiles and motivations exist but require more data before they can be clearly defined. An insider can also carry out multiple crimes simultaneously. The following chapters describe the profiles in-depth and also bring in the fifth profile – the *unintentional insider* – which does not fit with the four traditional profiles listed in Table 1.

Profile	IT Sabotage	Insider Theft of IP	Insider Fraud	Espionage
Who	Technical employees (e.g., System or Network Administrators, Developers, Programmers)	Most often Scientists, Engineers, Programmers, Sales personnel	Lower level employees (e.g., positions at help-desk, customer service, data entry)	Both technical and non-technical employees
	Employees with privileged access		Low/mid-level management	
When	Set up while employed	Usually within the period of 60 days before or after leaving the organisation	Happens over a long period of time	Happens over a long period of time
	Execute after termination			After the initial incident, a long period may pass before a following event
Motivation	Revenge	Start their own business	Financial need or greed	Financial need or greed
		New job position		Dissatisfaction with status
		Foreign government or organisation		
How	Access, ability, and motivation	Data exfiltration: E-mail, USB drives, physical documents, etc.	Corruption of organisational procedures	Methods span all profiles
			Inadequate auditing of critical and irregular processes	
What	Affects systems they worked on	Steal information they worked on	Personally identifiable information (PII)	Theft of information
			In some cases, fraud happens over a longer period of time and has great monetary impact.	Destruction of information to cover their tracks

Table 1: Insider Threat Vector Profile

3.3.1. Sabotage

IT Sabotage presents risks that may be the least appreciated by organisations. According to empirical research, these people tend to be technically savvy [26] [32]. In [32], it was stated that 86 per cent of offenders in the CERT database were employed in technical positions. Furthermore, 90 per cent had privileged access to the systems, databases, and networks they worked with every day [32]. These are the people trusted to keep an operation running day to day. Should the individual find the motivation, they can carry out attacks and conceal them with relative ease.

The primary motivation across the IT Sabotage profile was revenge [32]. For whatever reason, these employees' expectations were not met and they decided to take malicious action. According to [33], access after termination of contract occurred in 67 per cent of cases, and in 57 per cent incidents started within 60 days before or after termination. In some cases, *'backdoors'*[8] are installed right after being hired to make their legitimate job duties easier [34]. Scripted[9] automation is required to maintain large scale networks and computer systems. The technical means for achieving that are commonly the same as those used for creating malicious backdoors.[10] Subsequently, if a person were to become disgruntled with the organisation, those tools can be used for exacting revenge. One possibility is the use of a logic bomb,[11] which is designed to disrupt service integrity, availability, or both. Logic bombs can be placed during the employment, and activated after termination (as presented in [21], Practice 1, 10 and 11).

[8] A backdoor is a method for bypassing mandated authentication mechanisms.

[9] 'Scripting' refers to a process of automating repeated or highly complex tasks, to save time, reduce human errors, or increase efficiency. This is usually achieved via programming languages.

[10] For example, SSH public key authentication is commonly used for managing Linux/UNIX systems. It is easy for a person with super-user privileges to attach her personal public key to any user account. She can then access that account without entering the password.

[11] For example, a file filled with zeroes can be compressed exponentially. An unsuspecting user might deflate the file, and become a victim of DoS attack as deflated data can easily fill computer memory. This is commonly referred to as a 'zip bomb'.

3.3.2. Theft of Intellectual Property

Theft of intellectual property (IP) is the biggest fear for many companies. The amount of information that can be taken out of an organisation via electronic media in a short time span, and in most cases without attribution, is astounding. Victims include every major US defence contractor [35] [36] and the US Department of Energy [37], and there are many examples in Silicon Valley where competition for people is just as high as it is for customers. Apple and Samsung have provided years of media entertainment with their law suits of both copyright infringement as well as theft of intellectual property [38]. Larger organisations may survive the loss of IP and perhaps learn some lessons. Medium and small organisations, however, can be wiped out by a single incident [39].

CERT research in [26] has identified scientists, engineers, programmers and sales people who work with the IP as the most likely candidates for stealing it. Normally they steal information they work on and helped to create. Because of their personal investment, some emotional attachment or a sense of entitlement might be established to the IP. Their actions will most likely take place within 60 days of leaving an organisation, before or after [29] [40]. Data exfiltration is accomplished in a number of ways, and is not limited to email, USB, or physical documents.

These insiders are specialists who work on the IP every day as a part of their normal routine. The motivations for stealing the IP have been to start their own business, taking the information to a new job, and giving it to a foreign government [26]. It is uncommon for the stolen IP to be sold, possibly due to the emotional attachment an insider may have to his or her contribution. When reviewing the research for the profile of theft of IP, two distinct patterns were identified [26]:

- Entitled Independent; and
- Ambitious Leader.

The Entitled Independents are motivated to take the IP (creation of which they have contributed to) to their new job or to form their own companies. The actual theft is commonly committed 60 days before resigning (as discussed in [26]). The Ambitious Leaders recruit people inside the organisation to steal the IP [26]. Though the outcome of their actions is the same – the loss of IP – the roles they play and positions they fill in the organisation have different risks associated with them. The offenders in the latter category can be considered a subset of former, as they inherit most characteristics but are not content with only the IP which they personally created [26].

3.3.3. Insider Fraud

Insider Fraud cases represented the largest group that was profiled by CERT (discussed in [21]). One noticeable difference between fraud and other threat profiles is financial need [41]. Nearly half were low level employees, none professional or technical in nature, and were on the lower end of the pay scale. Due to the financial need or greed of the perpetrators, the crime normally happens over an extended period of time. In cases where there was a group of people working together, having a low or mid-level manager involved ensured the success for a greater length of time.

Insider Fraud is accomplished by corrupting existing corporate processes [41], which are critical to the organisation or irregular. Even if these processes are not carried out correctly, management can accept this behaviour because the results are needed for the organisation's continued success. As a result, opportunities for poor oversight and possibilities for bypassing audits are created. Whether this is done by the management knowingly or not is not relevant. Additionally, employees with excessive privileges were also cited as a threat vector (insider trust trap, in [41]).

As discussed in [41], a common target in an Insider Fraud case is personally identifiable information (PII), and the purpose is to copy or alter the data. The PII is then used by the individual or members of the group who are outside the organisation to commit fraud. For example, a list of e-mail addresses can be sold to online marketers. PII is targeted due to the fact that it is easier to access and liquidate than regular currency. A list of clients that an insider uses to conduct daily tasks can easily be copied, whereas a transfer of funds would have a clear transaction history. Therefore, malicious use of PII has inherently lower risk associated with it. Additionally, organised crime involvement was noted in cases with the greatest monetary losses.

3.3.4. Espionage

The Espionage profile has not been released by CERT. The research done in this area has been for agencies such as the Secret Service, Department of Homeland security, and the Federal Bureau of Investigation. The results of their studies have not been declassified or released to the public thus far. In [30], comparisons were made between espionage and sabotage profiles. From those comparisons we derived an Espionage profile included in Table 1. This is not presented as a definitive work but as a starting point when developing technical and behavioural indicators for an InTP. As observed in [30], saboteurs and spies had common predispositions, incidents were influenced by stressful events, concerning behaviour could be observed by co-workers, and an incident was facilitated by lack of proper detection and control methods.

David L. Charney, a psychiatrist with first-hand experience in consulting for the FBI, has written a two-part white paper in [31] and [42] on psychological motivations for malicious insiders. Based on interviews with convicted spies, and a decade of insight in consulting intelligence operatives, he proposed ten life stages for an insider spy [31]:

1. Sensitising;
2. Stress/Spiral;
3. Crisis/Climax/Resolution;
4. Post-Recruitment;
5. Remorse;
6. Active Spy;
7. Dormancy;
8. Pre-Arrest;
9. Arrest and Post-Arrest;
10. Brooding in Jail.

He argued that insider motivations can be traced back to difficulties in childhood. When combined with the stress of growing up, unexpected life crises and feelings of inadequacy, a person might become determined to seek possibilities for damaging their employer. Such insiders can manifest in institutions with a restrictive or secretive atmosphere. Initial feelings of excitement and righteousness can be replaced with regret, but feeling that the point-of-no-return has been reached, the insider continues on the selected path, especially when coerced by an external threat agent. The majority of covert malicious actions are then conducted, in some cases over a time frame of several years. Eventually, the pressure can prove overwhelming, and the insider may be genuinely glad when repercussions finally arrive. Therefore, a concept of *reconciliation* was proposed to encourage insider spies to voluntarily turn themselves in before reaching the most damaging periods of the cycle [42].

While a sabotage case is overwhelmingly motivated by revenge [30], agents preforming espionage have a wider range of motives. Dissatisfaction with their career, dissatisfaction with status or opportunities, and of course financial problems are all common among those cases [42] [30]. The financial need and dependence exhibited by espionage cases has greater similarity to fraud cases with respect to motive. Espionage only shares the methods of exfiltration with the IP Theft profile, with one possible exception being that both profiles are very

specific regarding their targets. Furthermore, the espionage timetable is distinct. As presented in Sections 3.3.1 and 3.3.2, IT sabotage commonly occurs within 30 days of being terminated, and IP theft 60 days before resignation. As presented in Section 3.3.3, insider fraud is conducted continuously once a method has been established. In the case of espionage the agent may choose to be active and then sleep for years before deciding to risk another action [31].

3.3.5. Unintentional Insider

To this point the focus has been on Intentional Insiders, those with malicious intent. Unintentional Insider Threats (UIT) may lack malicious motivation but their actions can provide access for any number of cyber threats, negatively impacting an organisations security posture. A definition of UIT was offered in [43], as:

> *'a current or former employee, contractor, or business partner who has or had authorised access to an organisation's network, system, or data and who, through action or inaction without malicious intent, causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organisation's information or information systems'.*

The threats are: accidental disclosure; use of malicious code to conduct an attack in coordination with social engineering; improper or accidental disposal of a physical media or medium; and the loss of portable equipment. The Foundation study also identified organisational factors and human factors that contributed to increased UIT incidents [44]. The focus of this body of research is to raise awareness and provide a roadmap for organisations to follow when standing up their own programmes. Many of the activities of an InTP that will be covered compliment the identification of UIT as well as implementing organisational changes to address UIT-specific problems. For example, the ability to identify an incident, analysis of behavioural changes preceding an incident, and education of the organisation to raise awareness and accountability [21]. As an InTP becomes more mature (and measures are in place) the organisation will develop the capability to determine where resources need to be spent. Should the UIT vector risk demand greater attention, then resources can be diverted as required.

3.4. Complexity of Insider Threats

In addition to specific insider profiles, CERT has identified several complexities that had been consistently seen throughout their work [26]. These six complexities are seen across all insider profiles, and in some cases they are even compounded. Each complexity presents challenges and increases the risk associated with a specific insider profile.

1. **Collusion with Outsiders**. The insiders can be recruited to work for interests outside the organisation to include foreign governments and organised crime. Bunn and Sagan also observed this in their data sets though all insider cases were from nuclear facilities or organisations. [45]
2. **Business Partners**. Trusted business partners hold a substantial amount of information about an organisation and their employees may even have access to critical information.
3. **Mergers and Acquisitions**. Mergers and acquisitions are turbulent times for organisations. Motivations and expectations of many employees will change in an unpredictable and possibly unmanageable way.[12] For government and military organisations, downsizing and restructuring also present similar challenges. The expectations of employees of the organisation will change and it is unlikely that those expectations will meet in the same place.
4. **Cultural Differences**. Behavioural indicators exhibited by malicious insiders can vary from culture to culture, country to country. Consideration of cross cultural communication and social norming may prevent unmet expectations and disappointment.

[12] Though Mergers and Acquisitions is a term used in large business transactions, the same organisation changes take place in government. Notably during transitions between cycles of centralisation and decentralisation that follow increases in spending and times of austerity.

5. **Foreign Allegiances**. National identity is yet another variable that can prove difficult to manage. Allegiances can also transcend national boarders to changing belief systems and identity, ethnicity, and cultural differences. All have the potential create conative dissidence that may impair predictable, ethical, and acceptable behaviour.
6. **Internet Underground**. Active involvement in the internet underground may be an area of concern. These activities provide insiders with access to technical assistance, criminals who have experience in electronic crimes, and some degree of secrecy. Active involvement raises the risk that the individual will be compromised unintentionally, and is fertile ground for recruitment. In most cases espionage agents are self-recruiting. [31] Activity on the internet underground indicates at a minimum curiosity and excitement. For outsiders it represents a potential way in.

3.5. Threat Timeline and Detection

Insider Threats can share common characteristics, which may emerge in access logs, audit logs, network streams, file system changes, or other forensic trails. Those characteristics can overlap with audit trails for benign activities, as discussed in section 3.3.2, making false positives an aspect of InTPs that must be managed well. Figure 1 illustrates the lifecycle of an insider and their theory on how to prevent an incident.

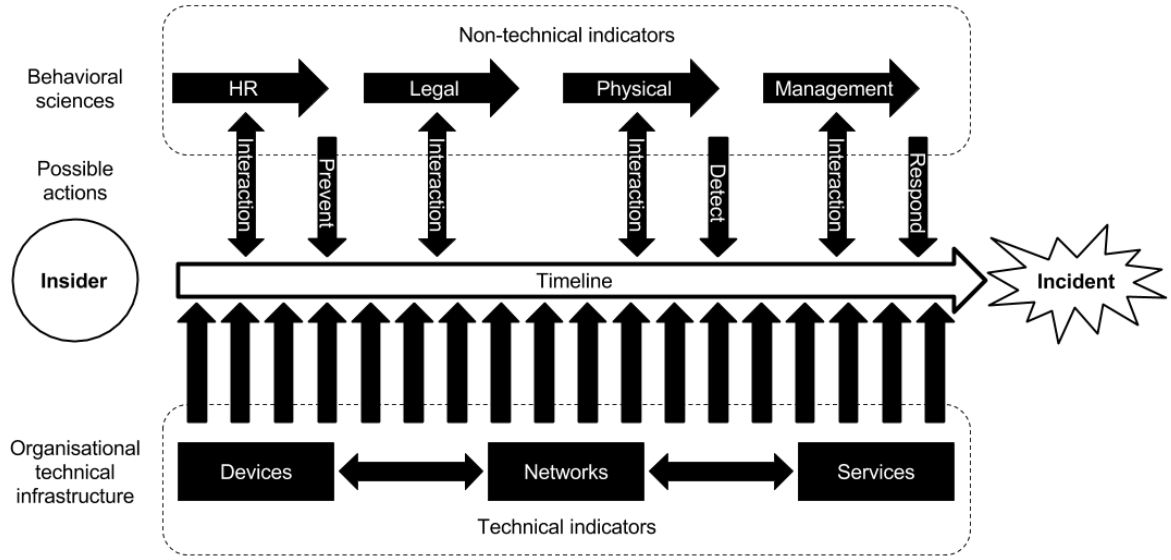

Figure 1: Insider Threat Timeline

Note, that multiple indicators are scattered across the timeline, as, due to the complexity of modern information systems, actionable information is commonly fragmented. Data fragments must be combined and interpreted in proper context in a process which is referred to as *Data Fusion* [46]. Technical indicators are complicated, take time to implement and require constant calibration, and their success depends on the talent of operations personnel, the quality of the system architecture, and proper implementation.

By comparison, human metrics can be quite simple in design, as one simply needs to be mindful of co-workers' behaviour; but several pitfalls must be avoided. Firstly, organisations must avoid the *'trust trap'* whereby inexcusable actions are ignored on account of seniority, as discussed in section 2.4. Secondly, obvious concerns for the mental well-being of employees must not be de-prioritised, as presented in sections 2.2 and 2.5. This is difficult to achieve in high pressure work environments, for example during final stages of a project with a looming deadline. Therefore, human metrics must be fully supported by the leadership and enforced by dedicated personnel. Thirdly, a human problem requires humane response which aims to understand and help rather than to condemn and punish. Superficial measurement of human metrics can be perceived as unneeded

bureaucracy, while an overly invasive approach can induce and enhance paranoia. InTP must not evoke disillusionment in loyal employees.

Insiders are people. This simple statement implies a great deal of complexity. Each person perceives the world slightly differently, has different beliefs, principals, morals, and culture. Through the daily intercourse of communication, people resolve problems, do their work and accomplish the mission of their organisation. These relationships are all different and must be managed individually, including the relationship with the organisation. Understanding personal predispositions, expectations, and motivation are all the responsibilities of management and Human Resources. Changes in any of these characteristics are behavioural in nature. When technical indicators suggest a change has taken place, intervention at the personal level is required to ensure the individual is still a dependable member of the team. Thus, combining technical and non-technical indicators increases the probability of preventing, detecting, and responding to an insider threat.

Insiders who commit IT Sabotage, IP Theft, and Fraud all have a different timeline on which they act. Knowing this allows the organisation to better understand when the individual's motivations have changed and when increased monitoring is required. A well designed and managed InTP will allow the organisation to move an individual back on the timeline that ends in an incident.

3.6. Key Components of Insider Threat Programmes

As stated in [47], no mandates, standards, or benchmarks exist for Insider Threat programmes. Information technology is a relatively immature and volatile field, and it is a well-known fact that the trial-and-error approach is unavoidable when pioneering new methodologies. Thus, organisations in the private sector who have implemented an InTP have done so of their own volition, using resources already available to them, and out of necessity. Their efforts and lessons learned laid the groundwork for the researchers of Carnegie Mellon University's CERT and Intelligence and National Security Alliance (INSA).

INSA Insider Threat Task Force was formed to *'engage with Intelligence Community and DoD thought leaders, CIOs, and representatives from private sector to examine best practices'* [47], and delivered a thirteen-step roadmap in [24] which provides essential elements as a structured process for implementing a successful InTP. This roadmap is presented in Figure 2. Additionally, INSA has provided a spreadsheet on insider threat publications in [48], and mapped them to each element in the InTP design process. Documents presented within this spreadsheet were used as a starting point when developing and classifying the proposed indicators in Section 4.3.

Figure 2: Insider Threat Programme Roadmap [24]

By comparison, the CERT team has defined key components for creating a successful InTP in [28]. These components are presented in the following list:

- Formalised and defined programme;
- Integration with Enterprise Risk Management;
- Insider threat practices related to trusted business partners;
- Prevention, detection, and response infrastructure;
- Insider threat training and awareness;
- Data collection and analysis tools, techniques, and practices;
- Policies, procedures, and practices to support the InTP;
- Protection of employee civil liberties and privacy rights;
- Communication of insider threat events;
- Insider threat incident response plan;
- Confidential reporting procedures and mechanisms;
- Oversight of programme compliance and effectiveness; and
- Organisation-wide participation.

In addition, the German Federal Office for Information Security (BSI) has developed the *IT baseline protection* (‘*IT-Grundschutz*’) methodology [49]. Although it is not directly linked to dealing with insider threats, it is meant to provide a foundation for organisations who strive to achieve a high level of information assurance and security. This methodology provides a thorough *how-to* for practitioners from various-sized organisations. Still, IT baseline protection standard recommendations must be scrutinized and implemented with consideration to the particularities of the organisation – meaning that it does not always provide a one-size-fits-all solution.

Nevertheless, standardisation in methodology, and reusable procedure is offered to reduce the expense of the information security program.

The lack of a community-accepted standard for InTPs was also exemplified in [50], which outlined InTP ingredients for organisations who are considering such implementation. This work exemplifies the scientific immaturity behind the creation of InTPs. Every supporting research material highlights the need to integrate an InTP with existing risk management processes, multi-disciplinary involvement of key personnel, and development of indicators (human and technical) and controls specific to the target organisation.

3.7. Summary

The principal profiles compiled by CERT (sabotage, theft and fraud) with additional profiles derived by us (espionage, unintentional) form the basis for understanding the insider threat problem. Whereas sabotage is usually motivated by revenge, theft and fraud are motivated by greed. Whereas sabotage aims to cripple with maximum impact (usually 30 days after termination of contract), stealth is key for theft (usually 60 days before leaving) and for fraud (conducted on an ongoing basis). On the other hand, espionage can manifest as a combination of other profiles with overwhelming behaviour similarities to sabotage.

It is apparent, that each organisation which intends to implement an InTP must conduct an internal risk assessment (which should already exist to some extent), and define a set of indicators and control mechanisms specific to their unique environment. At the time of writing, the roadmap presented in Figure 2 provided the most concise starting point for doing that. With this in mind, we are left to ask ourselves *'where to start?'*.

The framework in Figure 2 provides a roadmap. This roadmap probably already has many elements in place in your current operation. Risk management, information security, security operations, network, systems, and database administration, and of course physical security are part of everyday life in most organisations. InTPs add a new paradigm that expands the organisation's security culture and capabilities for defending itself.

4. Creating an Insider Threat Programme

This chapter will describe creating an InTP by first describing the primary steps in the programme life cycle. We will also look at an alternative approach that explores which mistakes to avoid when creating an InTP. Finally, we will discuss what types of detection indicators would be worthwhile to implement within an InTP.

4.1. Insider Threat Programme Roadmap and Life Cycle

Research sponsored by INSA in partnership with the United States Department of Homeland Security, FBI, and the Office of the Director of National Intelligence provides a roadmap for implementing an Insider Threat Programme. Their research, published as an extensive table in [48], reviewed more than 200 insider threat publications and provides a 13 step model that represents those actions that have been taken by current successful programmes in both business and government. Each action serves a specific purpose and adds value at an appropriate time. Some organisations have taken more steps to implement their programmes, some less. If during the review of the chosen materials it is decided that additional processes are required, the INSA research review in [48] provides a good starting point to deviate from. The thirteen step model was collected from programmes that have already been established and researched. At this time it would be premature to even consider them best practices. Insider Threat Programme research and practice are still in their infancy and there exists a lack of real knowledge and experience in this field. This being said, Insider Threat Programmes and the research thereof are the result of a real need in the Information Security field focusing on the insider threat vector.

> *Aufschub bringt Gefahr – 'Procrastination leads to disaster'*
>
> *German Proverb*

InTPs, as with CI programmes, have to this point been the projects of large corporations and governments. In the Report to Congress on Foreign Economic Collection and Industrial Espionage 2009-2011, *Foreign Spies Stealing US Economic Secrets in Cyberspace*, it was noted that a number of advanced industrial countries agree that China and Russia are continually using traditional human and technical collection methods against small and medium sized companies [51]. This report went on to say that Germany's Federal Office for the Protection of the Constitution (BfV) estimates that German companies lose $28 billion-$71 billion and 30,000-70,000 jobs per year from foreign economic espionage. Approximately 70 per cent of all cases involve insiders [51]. Similar numbers were reflected in statistics from the Republic of South Korea and Japan. The same report also brings up concerns about spying between friendly nations and competing corporations in friendly nations, a phenomenon which increased after the fall of the Soviet Union. Where some nations see spying as a dishonourable undertaking, most see it as a necessity beyond good or evil and temper their known activities with appropriate public relations for their populations. Snowden's revelations surprised the world. It was not just the masses that learned how invasive networked media can be, but also governments who also learned how vulnerable their apparatuses for intelligence are. Though most of the people of the world would consider espionage unsavoury, there is an undefined percentage of the world's population who will commit these acts in the right circumstances. These circumstances are directly addressed by CERT's insider profiles in the form of behavioural indicators. An information security programme that chooses not to have an insider threat programme has just accepted a known risk that cannot be measured.

Clearly, an InTP is a broad programme that requires participation from many stakeholders in order to be successful. We previously mentioned that organisations that have implemented the BSI's IT baseline protection standard have a considerable foundation on which to build their InTP. To support this, BSI's IT baseline protection recommendations list many indicators which are applicable for both unintentional and malicious insiders [49]. However, having solutions instituted to address these indicators does not constitute an InTP, but it can prove helpful nevertheless. Additionally, an organisation that has implemented BSI will not be unfamiliar with what is expected and required of their people to successfully implement an InTP. Simply, there is a large

gap between the security provided by a mature BSI programme instituted in a large organisation, and a fully implemented InTP.

The creation of an Insider Threat Programme compliments an organisation's already well-established information assurance programme. It is assumed that enterprise risk assessment have been completed. From this point setting a roadmap of where an organisation is on the Capability Maturity Model from previous audits will allow more realistic goals to be set, establishing a clear way ahead for the InTP programme manager. Though an InTP does compliment the Information Assurance Programme, it is recommended that this programme remains a separate operation for two reasons.

4.1.1. Initial Planning and Identifying Stakeholders

First, information assurance and risk management activities have specialised roles with specialised people inside of both organisational functions. The subculture or bias that exists in these departments would influence the InTP. Even in organisations with Counterintelligence and Internal Investigations functions the InTP would conflict with their mandates. What is legal for an agency with a CI mandate might not be legal for a private organisation, or even other divisions inside the same agency. An InTP spans the organisation to include a team that consist of HR, legal, physical and IT security, as well as behavioural science members and management. Having the InTP under a member of management with decision making authority and access to the executive (Commanding Officer or Chief Executive Officer) reduces the time required for course correction as the programme develops.

Secondly, this programme will change the culture of the organisation and requires senior level support and involvement to ensure these changes happen successfully. Questions like 'who is watching the watchers?' must be addressed to ensure inquiries (many of which will be initiated by false positives) and investigations (procedures that end with legal proceeding) are handled at an appropriate level. The damage done by publically chasing false positives will negatively affect the morale of the organisation and if it persists, the corporate culture. In this respect, an InTP does not want to create a persona that is held by CI or Internal Investigations. Where these departments serve a specific purpose, and in many cases their actions are shrouded in secrecy, an InTP must become a mechanism for self-reporting of organisational security shortcomings and a tool for framing events to benefit the continued improvement of the security culture inside the organisation. If it becomes an organisation shrouded in mystery, there are a number of behaviours that may develop that will negatively impact on the health of the organisation. Total transparency is not possible, but trust must be managed. Additionally a governance mechanism must be in place to ensure that the watchers are indeed being watched. As various personnel throughout the organisation may be flagged for more intensive monitoring for any number of changes in behaviour or activity, watchers should be under continuous heightened scrutiny as well. Due to their privileged and trusted positions they are in a unique position to corrupt security processes and abuse the trust trap.

4.1.2. Achieving Leadership Buy-in

After the initial planning and identification of the stakeholders, leadership buy-in becomes a real challenge. One of the first questions that might arise is the availability of resources, especially people and time. Simply pushing new assignments down the chain of command might not be very wise. Instead, the availability of existing and potentially new resources should be considered before making any decisions. Otherwise, if the personnel resources are already stretched thin, they could be stretched even thinner or reassigned and lost altogether. The impact is a mediocre response that puts the programme in jeopardy from its inception. A failed programme negatively affects the morale, culture, and wellbeing of an entire organisation and its partner agencies. Whether your insiders are criminals, competitors, enemies of the state, or just simply unaware, in the end uncovering their nefarious activities could be compared to having a good enough '*net*' to catch anything

harmful. The more buy-in from the personnel, the finer the mesh and the better informed and trained the personnel, the stronger the net.

4.1.3. Ensuring Sustained Buy-in From Leadership

Leadership from the top of an organisation sets the tone for short term behaviours that will eventually become long-term corporate cultural norm. The idea of changing the culture is overwhelming, but no less imperative. A shining example of cultural change is that of safety. Safety slowly became a concern during the industrial age. Poor factory conditions damaged the health and safety of workers, as well as the facilities and equipment. Today safety programmes are institutionalised in government and fully embraced by industry in the western world. Liability is not the sole reason for this change in culture, although it was the motivation for business. Healthier and safer workers perform better for longer, and so it is good business. The science of safety especially took off in the last half century. Even Deming's view that being unsafe is a waste and should be removed from the process indirectly speaks to a change in today's culture. Modern society takes for granted the benefits that a safety culture provides; they are institutions that we have come to expect. It is only reminders seen on TV or during trips to the undeveloped world that we can begin to appreciate, though hardly measure, how far safety cultures have come. They permeate every aspect of our lives.

In 2015 we cannot wait another 200 years for the security movement to really kick off before addressing the issues of security and changing our culture to accommodate it. Security in IT is well-developed when compared to the first days of the internet, but somehow falls short of a good night's sleep for an informed Corporate Information Officer. Today, security operation centres work around the clock to protect systems and people from an ever-growing number of threats. These capabilities are already in place and continually improved. An InTP compliments those existing capabilities and provides a system to address insiders, both intentional and unintentional. The best indicators are behavioural in nature. This requires an educated and aware management team and employee base with committed resources, and people who are working to solve these specific problems.

Military organisations already have a culture of security. From day one new recruits are indoctrinated in some form as to the realities of physical security. From getting onto a base, to understanding how an armoury works, and eventually receiving an ID card that allows access to the infrastructure. Interestingly, unauthorised access to an armoury has a limit to the amount of damage that can be done. Damage caused by access to critical infrastructure and networks in a case of espionage is often not measurable. To an adversary, access is priceless and is often unknowingly sold by an insider very cheaply.

> *A German insider was convicted of economic espionage in 2008 for passing helicopter technology to the Russian SVR in exchange for $10,000. The insider communicated with his Russian handler through anonymous e-mail addresses.* [51] *(B-2)*
>
> *German authorities would like more corporate feedback and say that most enterprises either do not know when they are victims of cyber espionage or do not want to publicly admit their weaknesses. Most countries engage in some form of corporate outreach.* [51] *(B-3)*

During the Cold War, espionage was practised by virtually every country, famously by the US and Russia. Spying among allies was also a common occurrence. During the Cold War, the US was reluctant to discuss friendly spies. '*We tended to look the other way*,' says Herb Meyer, a former special assistant to the Director of Central Intelligence, '*they were taking advantage of us while we felt we had a larger interest*'. But that attitude is changing [52]. Perhaps due to the US being preoccupied with its Cold War adversaries, proper attention was not given to what has become a growing problem. Among the countries most often cited by US intelligence agencies as seeking technological and financial secrets are France, Germany, Japan, South Korea and Israel [52].

During the summer of 1991, IBM accused the German intelligence service of eavesdropping on its telecommunications and passing stolen information to German companies. IBM lost several important bids in Europe around this time, possibly because of inside knowledge obtained by its German competitors [52]. Between 1987 and 1989, French intelligence planted moles in several US companies, including IBM. In the autumn of 1991, a French intelligence team attempted to steal 'stealth' technology from Lockheed. Only the Federal Bureau of Investigation's persistence ended these operations [52]. This is not to say that the US has been the only victim of industrial espionage by state sponsored intelligence operations. Germany and South Korea judge that China, in particular, increasingly uses cyber tools to steal trade secrets and achieve plausible deniability, according to press reporting [51](B-2). German officials have also noted that business travellers' laptops are often stolen during trips to China. The Germans in 2009 highlighted an insider case in which a Chinese citizen downloaded highly sensitive product data from an unidentified German company where he worked to 170 CDs [51](B-2). According to a 2010 press report, the Germans view France and the United States as the primary perpetrators of economic espionage 'among friends'. France's Central Directorate for Domestic Intelligence has called China and the United States the leading 'hackers' of French businesses, according to a 2011 press report [51](B-2). Clearly there are no guiltless parties when it comes to the world's second oldest profession.

4.1.4. Completing the InTP Life Cycle

Today's State Counter Intelligence agencies simply cannot defend the State infrastructure, let alone being responsible for business entities in their society. Efforts by governments to engage the private sector have met with varying degrees of success, but all have room for improvement. Thus, insider threat programmes fill the gap that currently exists. The argument could be made to delay establishing a programme until better techniques, programs, and practices are available. However, in the meantime, insider incidents will be happening, your organisation is losing its critical assets, and no one knows how to effectively respond to an incident.

In order to complete the Insider Threat Programme life-cycle organisations must have the following basics:

- Policies and procedures to deal with at-risk employees, and means of identify them and evaluating them.
- A mechanism for professionals across the enterprise to voice the interests of their business unit concerning incidents.
- The ability to make an assessment of insider threat vulnerabilities.
- Training and exercises to raise the awareness of the organisation.
- Established procedures for initiating and conducting investigations. Established contacts with the various law enforcement agencies that would be helpful in the event of an insider incident.
- A method of recording incidents and integrating lessons learned back into the organisations operations.

Any one of these capabilities represents a strategic goal that where an organisation can initiate their InTP from.

4.2. Exploring the Road Less Travelled

Sadly there is no road map better than what has already been offered in Figure 2. Considerations and lessons learned do not offer a sure-fire path to success, but they do offer wisdom on how move forward. Of particular interest was *A Worst Practice Guide to Insider Threats: Lessons from Past Mistakes* by Matthew Bunn and Scott D. Sagan [45]. Otto von Bismarck once said that only a fool learns from his mistakes; a wise man learns from the mistakes of others. Their paper is intended to help nuclear security operators learn from the mistakes of others in protecting against insider threats. They draw on episodes involving intelligence agencies, the professional military, bodyguards for political leaders, banking and finance, the gambling industry, and pharmaceutical manufacturing [45]. Where CERT and INSA focus on those things that have worked, *Lessons from Past Mistakes* pulls morsels of wisdom from specific incidents that have not.

Lesson #1: Don't assume that serious insider problems are NIMO (Not In My Organisation)

Most organisation try to build trust with their employees. Doing so may lead to the assumption that our organisation is different and not susceptible to Insider Perpetrated Incidents (IPI). The natural assumption when such an event does occur is to believe that it was not intentional. Motivations and beliefs change. At the time of this writing there is not a technical solution that detects these changes specifically.

Lesson #2: Don't assume that background checks will solve the insider problem

Background checks are a precaution that is normally taken by an entity outside of the organisation in question. The process is opaque and trusted, once again making the organisation susceptible to the Trust Trap. This is not to say that they are not effective, but they have not been effective against people who entered the organisation 'cleared' only later to reveal themselves as an insider, Robert Hansen and Edward Snowden being two prime examples. Background checks are also static. Once completed the file is shelved for some period of time. This begs the question of whether this system is outmoded. A method of Continuous Personnel Risk Management (CPRM) has yet to be clearly defined but merits future development.

Lesson #3: Don't assume that red flags will be read properly

This lesson cites the previously mentioned Hasan case in which red flags where ignored, and in fact suppressed to transfer the individual with good evaluations to another command. They identify several reasons for this. First of all, the hassle involved in removing an officer from their post, and additionally the negative image it might give of the command and its commanders should there be political fallout from making such accusations against a Muslim in the current political environment. Even when erratic behaviour had been identified, it did not follow Hasan to his new command, as local records and career service records had two different destinations. There are a number of lessons to be learned when designing an InTP. The first is that individual and group interests may not align with organisational objectives such as compartmentalisation and information sharing. Having an organisational structure and policies to confront red flag events when they occur strengthens a security culture and the integrity of the organisation.

Lesson #4: Don't assume that insider conspiracies are impossible

As shown by the CERT expanding complexities, conspiracies indeed happen and are most likely conducted by organised crime or espionage. Conspiracies are more difficult to detect and referencing a Rand study *Insider Crime*, conspiracies account for approximately 10% of the crimes in their database. [53]

Lesson #5: Don't rely on single protection measures

Relying on just one protection method is not a deterrent, no matter how good you may believe the measure is. Once a method of defeating the chosen protection is discovered you are defenceless. Defence in depth is a common practice in Information Assurance to increase complexity for attackers trying to get into systems, thereby mitigating risk. Managing multiple deterrence, though cumbersome, ensures that the risk level is less binary.

Lesson #6: Don't assume that organisational culture and employee disgruntlement don't matter

Both culture and employee disgruntlement are topics addressed by the presented CERT materials, both in the profiles and the expanding complexities that have been recognised. Employee disgruntlement can be an indicator of culture, but also a function of the size of the organisation; the more people in the organisation, the greater number of relationships, and the greater chance for an employee to become less than happy with their environment. In both cases there is not a technical solution, although possibly there are technical indicators. Addressing these issues requires both management and employees to understand the risks and have the tools to take action when concerning behaviours are identified.

Lesson #7: Don't forget that insiders may know about security measures and how to work around them

Bunn and Sagan [45] raise the point that systems, once in place, become static. For most organisations which are trying to reduce uncertainty in their processes to have a predictable result (product or service), the ability

to address a reactive adversary has not been developed. Privileged users in IT as well as 'trusted' insiders will have the specialised knowledge required to be a reactive adversary. The best case to illustrate this point is that of Robert Hanssen, the senior FBI analyst convicted in 2001 of fifteen counts of espionage in what the FBI has called 'possibly the worst intelligence disaster in US history'. [45] [54] Hanssen's ability to access CI watch lists, avoid lie detectors, and control his contact with outsiders allowed him to be so 'successful'. When developing an insider threat programme these issues must be addressed when developing governance for the programme. Who will watch the watcher?

Lesson #8: Don't assume that security rules are followed

Rules that make sense and that are understood by employees have the greatest chance of being adhered to. That being said, Bunn and Sagan also point out that competing motivations are inevitable with security programmes. Security is a secondary mission for any organisation; the primary mission is adding or creating value for the organisation by generating revenue in the private sector and accomplishing a mission or fulfilling a mandate in the public sector. This can be done in a variety of ways but all require input from employees. Every security procedure that must be followed detracts from productivity – time that could have been used on the mission. If two departments (blue and green) where all things being equal (the work, management, resources, people, training, etc.) are competing to produce widgets (bullets, security reports, software, whatever), and blue follows the security protocols but green ignores them once a week, green's productivity will be noticeably higher so long as no security incidents are noticed. A gamble to be sure, but it could very well pay off at the expense of those who follow the rules, and at the expense of the company's security culture. Your poor performers are perceived to be more productive and will be rewarded. The point is that incentives must be carefully placed, both to accomplish the mission and to support the security culture.

Reviewing rules to ensure they are appropriate is also necessary. If rules are perceived as needless, ridiculous, or lead to unproductivity by wasting time and resources, the security processes will be viewed with contempt leading to unwanted behaviours that undermine the organisation's security culture. If rules are broken, a method for self-reporting the violation and improving the process should be implemented, but this cannot work without incentives. If no changes need to be made it is an opportunity to educate employees so they understand the importance of the rule that they violated. If the rule is indeed cumbersome for no apparent reason, removing it will send a powerful and empowering message.

Lesson #9: Don't assume that only consciously malicious insider actions matter

Unintentional insiders are more common that malicious insiders. The damage they wreak is far less than the damaged caused by focused intent. Random acts, whether with good intent or the random act of ignorance, still have an impact. In many cases they are just not professional and affect morale and culture in that way. Raising the awareness of the people in the organisation can both humble them to the effects of their actions and reinforce the security culture mind-set. Additionally training and required reading are useful methods of holding people responsible and accountable for their future actions.

Lesson #10: Don't focus only on prevention and miss opportunities for mitigation

Bunn and Sagan refer to the Fukushima Nuclear accident when discussing prevention versus mitigation. Prevention represents the latest preventative measure; do this so that will not happen. This offers solutions for a static environment. Though no one would recommend going without a signature based antivirus software, there is also no one who is going to tell you that it will work. Mitigation is a response to a dynamic world that is largely out of the control of IT professionals. Preventing malware is not as important as knowing what to do once it impacts your operations. Having a plan, via governance and policies, and an operation that can respond to the incident with those policies presents the least risk for the way ahead.

4.3. Detection Indicators

This section presents assessments on the relevance of detection indicators regarding the profiles established within section 3.3. Note that indicators should be developed by each organisation to suit their particular

requirements. Therefore, we do not attempt to compile a definitive list, but rather to propose a structure that can be customised for creation of an InTP, and for profiling one's employees within an InTP framework. Overlap in sensor data is desirable, especially if sensor data from multiple disciplines are effectively fused together, as no single indicator provides comprehensive situational awareness.

Whatever the event that precipitates the desire for revenge, technical and behavioural indicators can notify the members of your insider threat team that special attention and care needs to be paid to this employee. Preventative actions can move the employee backwards on the time continuum (see Figure 1 above), away from actually damaging the company's assets.

If an insider possesses all the privileges for the IP, then detection of wrongdoing is very difficult. For example, working overtime on a project an employee is passionate about is an indicator found in these types of incidents. However, this behaviour is very common in the IT sector, especially when a deadline is near, and in any case engineers are known for passion toward their speciality. Discouraging overtime can be perceived by an employee as an attempt to suppress passion projects, which might lead to unmet expectations. As a result, a loyal employee might leave or become disillusioned and thus become a threat. Technical indicators can provide actionable evidence only if detected in a timely manner, and in the correct context. Intervention from co-workers and management provides the best path to preventing an incident, but this approach requires vigilance which can often be neglected in a familiar working environment. Therefore, technical indicators and countermeasures should be used in conjunction with context provided by human assessment.

Though clear similarities exist between espionage and the other CERT profiles, common personal predispositions and behavioural indicators of IT sabotage provide a good place to start when spies are considered a risk to your organisation. The one similarity that all threat profiles share in is their malicious intent toward the organisation, and that this malicious behaviour is a criminal act.

4.3.1. Personal Indicators

Root causes for insider incidents can often be found within the troubled personal lives of perpetrators, as evidenced by the high-profile examples in chapter 2 and in the empirical research conducted by CERT. Thus, it is imperative to build the first tier of indicators on this knowledge. People can and will withhold personal information, even if disclosing such information is mandated by existing CI procedures (and of course a restrictive environment can motivate an insider incident), yet co-workers might have suspicions over the personal wellbeing of their peers. It is important that such delicate issues are handled by dedicated personnel specialists or counsellors, to avoid so-called 'witch hunt'. Furthermore, the expert opinions of that specialist must not be ignored by management or security officers.

Indicator	Sabotage	Theft	Fraud	Espionage	Unintentional
Depression	High	Low	Low	Medium	High
Financial obligations	Low	High	High	Medium	Low
Address change (moving)	Low	High	High	Medium	Medium
Death among family or friends	Medium	Medium	Low	Medium	High
Feelings of inadequacy	High	Medium	Low	High	Medium
Break-up or divorce	Medium	Low	Low	Medium	High
Impending termination of contract	High	High	Low	Medium	Medium

Table 2: Personal indicators

Each example in Table 2 can contribute to, if not directly motivate, an insider incident. What these examples share, besides being in the domain of a personnel specialist, is that they may not be transparent on the employee's personal records. For example, one's official place of residence does not necessarily translate to the physical location which that person might consider home. If a house where a person grew up is being demolished, that person might suffer depression as a direct result. As a result, that person may be prone to making mistakes (unintentional profile), or he might unload his frustrations in the working environment (sabotage). If the insider has simply been evicted from a previous residence and is forced to relocate on short notice, then the worries become more practical. Maybe the rental prices of apartments are too high and the alternative is becoming homeless. These indicators place the insider firmly in profiles with potential for financial gain (theft, fraud and espionage). They also reduce the likelihood of committing sabotage, as that would directly conflict with self-preservation. While institutions with established CI and clearance procedures might require employees to notify the employee (or intelligence services) of such occurrences, stealth is a key factor in theft, fraud and espionage profiles. The insider may withhold the information or, if the information is reported periodically, present the relevant information after the damage has been inflicted. Furthermore, a new or broken relationship might mean changed financial obligations or may upset a person's mental state. If the insider truly harbours malicious intent or is mentally unbalanced, then he is unlikely to present this information voluntarily. However, co-workers and HR specialists might detect some early warning signs.

Another sensitive event is termination of employment which brings along overwhelming motivation for committing sabotage, as presented in section 3.3.1. It also exposes the employer to theft of intellectual property (e.g., carrying IP over to new job), as presented in section 3.3.2. Fraud, however, is unlikely to be the result of termination as it is usually conducted on an ongoing basis over an extended period of time. Espionage activities fall under the scope of sabotage (e.g., expose secrets for revenge) if termination was initiated by the employer. As also noted earlier, leaving employees should be monitored more closely for any such activity.

4.3.2. Behaviour Indicators

Data regarding behaviour must be formulated over time, based on the way the employee acts within the working environment. These indicators are directly observable by co-workers, HR personnel and managers, unlike subtle personal predispositions in Table 2 which require assessment. Table 3 was compiled using the information in [55] and [56]. Only behavioural indicators which must be formulated over time were chosen, while indicators requiring background checks are presented in Table 4 in the next subsection. Technical indicators are also omitted, as those must be monitored by IT system operations personnel, and will be discussed in sections 4.3.4 to 4.3.6.

Indicator	Sabotage	Theft	Fraud	Espionage	Unintentional
Unwillingness to comply with established rules and procedures	High	Medium	Low	Medium	High
Repeated breach of procedures	Medium	High	High	High	High
Excessive or unexplained use of data copy equipment (fax, copy, camera)	Low	High	Low	High	High
Excessive volunteering which would elevate access to sensitive data	Low	High	High	High	Medium
Excessive overtime work	Low	High	High	High	Low
Bringing personal equipment to high-security areas	Low	High	Medium	High	High
Carelessness	Low	Low	Low	Low	High
Concerning statements, jokes, or bragging	Medium	Low	Low	Medium	High
Impulsiveness	Medium	Medium	Low	Low	High
Poor social interaction	High	Medium	Low	Low	Medium
Aggression	High	Medium	Low	Low	Medium

Table 3: Behavioural indicators

It appears that several indicators can cover the same fields but are given different assessments; however, that is not the case, as there is a significant difference between unwillingness to comply with procedures, and simply failing to comply with them. The former exhibits the hallmarks of sabotage, as the attitude can be driven by emotion or personal beliefs (maybe even conflicting with self-preservation). The latter can be more subtle, to the point where it is only noticeable under direct observation. Thus, that person may be pursuing a personal agenda, exhibiting signs that are usually associated with theft, fraud and espionage profiles. It is also likely that this person is simply being careless, which would expose him to becoming an unintentional insider (e.g., compromise by accident or be exploited by external threat agent). Yet, carelessness is observable regardless if it results in a breach of procedure, and can be a by-product of an overly bureaucratic working environment.

Likewise, exhibition of poor social skills or aggression can be a precursor for sabotage incident. Fraud and espionage are carried out over an extended period of time which may span years, and depend upon avoiding detection. Therefore, the chances of a person who exhibits those indicators being involved with fraud or espionage are low. As strange as it may seem, 'excessive friendliness' or 'being too hardworking' could even be considered as indicators for malicious intent. Maintaining a low profile is meaningless if the insider has no access to whatever he is interested in stealing. This was discussed in sections 2.4 and 3.3.4.

Procedures for handling problematic behaviour may already be in place in HR or security departments, but they can potentially be evaded (or neglected) if they are not fused together with other indicator classes within an InTP framework. Note that assessing behaviour of any person always requires proper context.

4.3.3. Background Indicators

Whereas previous indicators were based on subjective assessments from co-workers, background screening should focus on objective historical records. Many organisations already have the building blocks in place as a

part of recruitment and CI procedures, which can be modified to fit the InTP profiles. Table 4 was also compiled using the information in [55] and [56]. Only indicators which can be verified using background screenings were chosen while behavioural indicators were presented in the previous sections in Table 3.

Indicator	Sabotage	Theft	Fraud	Espionage	Unintentional
Involvement with individuals or groups who oppose core beliefs of organisation	High	Medium	Medium	High	Medium
Criminal record	Medium	High	High	Medium	Low
Addiction (alcohol, drugs, gambling)	Medium	High	High	Medium	Medium
History of mental or emotional disorder	High	Medium	Low	Medium	Medium
Indebtedness	Low	High	High	Medium	Low
Sexual behaviour which indicates lack of judgement	Low	Medium	Medium	Medium	High
Engagement in activities which can cause a conflict of	Medium	High	High	High	Medium
Business dealings	Low	High	Medium	Medium	Low
Active presence in social media	Low	Low	Low	Low	High
Number of previous employers and average time of employment	High	High	Low	Low	High
Spending exceeds income	Low	High	High	High	Low

Table 4: Background indicators

Background checks, especially in positions which require clearance for classified information, are commonplace. However, that data can also provide insight into which threat profile an insider may belong, and which countermeasure to apply if warning signs are detected or an incident occurs. Debt may motivate an insider to steal intellectual property, commit fraud, or may make that person susceptible to coercion. A large number of previous employers with short average time spent with each may indicate unreliability, with theft being the highest concern. That insider may already be considering his options for his next employment, and be on a path for stealing intellectual property. Furthermore, a person with numerous business dealings may be interested in forming a new company, which is a prevalent motivation for committing intellectual property theft. If an insider exhibits other indicators within the theft profile, then he could be put under surveillance, or pre-emptive actions can be taken if the threat has already been correlated.

Business partners and contractors should be held to the same standards as official employees if working with sensitive information. An existing criminal record may mean termination of contract if that position requires security clearance, but contractors may not be held to the same standard. For example, personnel who perform routine maintenance of essential office equipment are not necessarily cleared. Additionally, troubling background can bar a new employee from being hired, but is that standard being followed when existing employee is being promoted or granted security clearance? As presented in section 2.4, Herman Simm, who had already displayed troubling behavioural indicators (i.e., breach of document handling procedures), had surprisingly little trouble gaining NATO security clearance.

4.3.4. Computer Networks Indicators

Network monitoring is essential for troubleshooting, and for intrusion detection. IDS (Intrusion Detection System), IF (Intelligence Framework) and PCAP (Packet CAPture) solutions are commonly used for perimeter defence (ingress), but outgoing (egress) and internal (LAN[13]) traffic must be monitored for insider threat detection. Network events are managed by technical NOC (Network Operations Centre) personnel.

Indicator	Sabotage	Theft	Fraud	Espionage	Unintentional
Correspondence with competitors	Low	High	High	Medium	Low
E-mail messages with abnormally large amount of data	Low	High	High	High	Low
DNS queries which indicate involvement with internet underground	Medium	High	Low	Medium	Low
Use of suspicious protocols (e.g. IRC)	Low	High	Low	Low	High
Use of suspicious services (e.g. VPN, Tor)	Low	High	Low	Low	Low
Execution of offensive tools	Medium	High	Low	Medium	Low
Execution of malware	Medium	Low	Low	Low	High
Anomalous peaks in outgoing connection count	Medium	High	Low	High	Low
An unauthorised device is connected to the network	Medium	High	Low	High	Medium
Download of blacklisted software	High	Medium	Low	Medium	Medium
Connections initiated from a workstation outside working hours	Medium	High	Low	Medium	High

Table 5: Network Indicators

Almost all entries in Table 5 are rated as high for theft and low for fraud. Empirical studies by CERT have shown that the former is usually conducted by technical personnel whereas the latter is carried out by non-technical employees. Furthermore, fraud is usually carried out during working hours, and the insider has access to stolen or modified data as part of his daily routine. Therefore, it is very difficult to differentiate this kind of malicious activity at the network level. However, precursors for fraud could be detected from communication traffic as significant number of insiders within the fraud profile were recruited by (or in collusion with) outsiders. Messages can likely be found within regular e-mail, chat, VOIP traffic and call records, but the legality of monitoring such data should be taken into consideration. CERT also advises targeted monitoring of any employee who is due for termination in [29], with explicit focus on possible theft of IP.

By comparison, those who commit Theft of IP are likely to use sophisticated exfiltration tools, and are likely to do it outside working hours. Egress filtering is not a new concept, and organisations have begun to adopt it for example by blocking outgoing ports which are insecure or could be used for data exfiltration. But some

[13] LAN - Local Area Network

protocols must be open for normal network operations, such as HTTP[14], HTTPS[15], DNS[16] and ICMP[17]. Special attention should be put on the outgoing traffic on those protocols, as they can be exploited for sending out confidential data. Some techniques, such as DNS tunnelling, split each file into queries (line-by-line). Thus they create a large amount of connections which should be noticeable in PCAP, IF or NetFlow[18] graphs. Creating a baseline for normal traffic allows monitoring personnel to identify abnormalities. For example, anomalous connections (e.g. outside working hours) from a single workstation can indicate malicious intent or a malware infection (which would fall under the unintentional insider profile). But it could also be a hardworking employee, so proper context should be applied. For example, this kind of anomaly is less likely to be malicious if the employee is involved in a project which is approaching its deadline. Another consideration is regarding the time window; the traffic might not be anomalous if compared to older data (such as one year instead of one month), implying routine activities. The same principle applies for handling situations when an employee goes on and returns from a vacation.

Another indicator which can be monitored on OSI[19] networking layers 2[20] and 3[21] (but is often overlooked) is connection of new devices. Networks in high-security areas should employ layer 2 filtering and access control, but unfortunately those can be easily bypassed by technically savvy insiders. Nevertheless, a list of authorised network devices that is kept in sync with information from the configuration management system can detect insider attacks and data exfiltration by the means of installing rogue devices (sabotage, and theft or espionage respectively).

4.3.5. Client-side Indicators

The term *client-side* refers to any action that occurs on the client portion of a client-server model. Within an InTP framework, this definition applies to an insider's workstation, mobile device, etc. Note that essential office devices such as printers, copiers and fax machines should functionally be defined as services in the client-server model, but as they are usually managed by the same technicians who support the workstations and are physically located in the same office space as the insider, we have decided to present them in this section. It is important to keep in mind that, since an insider has physical access to these client devices, they can potentially manipulate data (e.g., logs and other forensic evidence) on those devices, therefore centralised monitoring tools must collect indicator data before the user can tamper them. For example, centralised logging solutions should not poll log files (which can easily be overwritten), but clients should send the event data from memory during runtime.

Several indicators in Table 6 are based on recommendations by CERT [57]. It is feasible for technically savvy insiders to use pre-acquired knowledge along with specialised software tools for information system sabotage, identification of valuable or vulnerable systems (sabotage, theft), escalation of privileges (theft, espionage), or exfiltration of confidential data (theft, espionage). For example, offenders in sabotage cases have downloaded malware and disabled anti-malware software on their workstations to ensure success. The operational status of anti-malware software should therefore be monitored and logged at all times, and special attention should be directed toward users who have displayed indicators in IT sabotage profile (e.g. impending termination of contract, dissatisfaction or anger). Alternatively, if no correlation with sabotage or theft profiles are found, then the insider may be unintentionally involved in malware attack.

[14] Hypertext Transfer Protocol - used for data transfer for World Wide Web.
[15] HTTP over SSL or HTTP Secure - Encrypted HTTP.
[16] Domain Name System - associates human-readable domain names with numerical IP addresses.
[17] Internet Control Message Protocol - protocol for error detection in network devices.
[18] NetFlow - feature for measuring network traffic which was initially introduced by Cisco. NetFlow provides information, such as number of bytes transmitted, what protocol was used, source and destination addresses. NetFlow does not present the payload.
[19] OSI model - Open Systems Interconnection model.
[20] Data Link Layer - switch level where packets are delivered using unique hardware addresses.
[21] Network level - router level which enables packet forwarding between intermediate networks.

Indicator	Sabotage	Theft	Fraud	Espionage	Unintentional
Anti-malware alerts	High	Medium	Low	Medium	High
Blacklisted files detected ('hacker tools')	High	High	Low	High	Low
(Attempt of) disabling anti-malware tools	High	High	Low	Medium	High
Attempted escalation of privileges	High	High	Low	Medium	Low
User attempts to print or copy confidential documents	Low	High	Low	High	Medium
Abnormally large number of software errors	High	Medium	Low	Medium	High
Unidentified device is attached (USB, CD-ROM)	Medium	High	Low	High	Medium
Failed login attempts	Medium	High	Low	Low	Low
Different users (attempting to) log in from the same workstation	Medium	High	Medium	Low	Low
User logs into a desktop workstation outside working hours	Medium	High	Medium	Low	Medium
Lack of log messages or monitoring data	High	High	Low	Medium	Medium

Table 6: Client-side indicators

Data exfiltration can be carried out physically, by printing or copying files. Correlating printer logs with indicators from Table 4 can be used to foil theft of IP or espionage, while providing little value against sabotage. Insiders might be trying to escalate privileges or hide their tracks by logging in using their colleagues' credentials. A number of failed login attempts for a user could indicate password guessing, while even more alarming would be if a single workstation would be used to attempt authentication with several different user accounts. Even though some workstations inside an organisation (e.g., in conference rooms) could be shared by multiple employees, these would still be rare exceptions and under normal circumstances a single workstation would be used only by a single employee. Therefore, attention should be payed to all events when there is more than one user accessing or even attempting to access a workstation. Another threat indicator that is often mentioned is working outside of normal working hours. Just on its own, working extra hours is completely normal if this could be explained by the fact that the employee is trying to meet an approaching deadline, but if this event is accompanied by other indicators (e.g., copying files, anti-malware alerts, etc.), this could mean that the insider could be looking to harm the company while there is no one else is around.

It is apparent from Table 6 that client-side monitoring does not protect against IT fraud. Those users tend to be non-technical, and their workstation use does not differ from everyday activities. While they might attempt to probe the limits of their existing privileges, or attempt escalation by colluding with other insiders, modern systems rarely display relevant information of such events on the client portion of client-server architecture.

4.3.6. Service Indicators

Service is a common terminology in IT systems to describe the server part in client-server architecture. In reality, what is understood by an end-user as a 'service' can be a complex combination of interconnected servers. Each of these servers handles a specific role, and implements its own event logging and protection mechanisms. Therefore, it is especially important to tailor the indicators in this category to suit the infrastructure of an organisation. Table 7 outlines some of the indicators that could be observed from services.

Indicator	Sabotage	Theft	Fraud	Espionage	Unintentional
Modification of centrally stored log files	High	High	Low	Medium	Low
User copies a large number of documents to a local disk	Low	High	Low	High	Low
Authentication failures	Medium	Medium	High	Medium	Low
Configuration file changes	High	Medium	Low	Medium	Medium
Permission changes	Medium	High	Medium	High	Medium
Database content changes	Medium	Low	High	Medium	Medium
Employee attempts to access resources not associated with his role	Low	High	High	High	Medium
User account is used from multiple devices	Medium	High	High	Medium	High
User account is set to expire in 30 days or less	High	High	Low	Medium	Low
Multiple accounts per user	High	High	Medium	Medium	Low

Table 7: Service indicators

Even central logging solutions can be attacked in order to alter messages stored there. Any unexplained gaps could indicate possible tampering by insiders who are attempting to cover their tracks. To mitigate this, it is advised to consider digitally signing centrally stored log data that would allow to verify the integrity of the logs at any point in time.

In [29], CERT proposes automatic directory service queries to identify user accounts that are set to expire in 30 days or less (time when IP theft takes place). Furthermore, audit logs display information about the device used to access the service (in addition to information about credentials). If a single user account is used from several distinct devices, then the user may attempt to copy IP to a personal laptop (theft), the user could have given the credentials to another employee (fraud), or compromised credentials could be in use for lateral movement (unintentional).

Maintaining and auditing the integrity of database tables is a primary defence against fraud which aims to alter their content for personal benefit, but provides little defence against theft which simply aims to copy the data. The number of files copied could be used as an indicator for that. Most services should have the functionality to collect such information, but must be explicitly enabled.

4.4. Summary

We identified that when creating an InTP, it is essential to identify relevant stakeholders already in the initial planning phase. In order to be able to kick-off and also sustain the InTP, it is necessary to achieve and also sustain buy-in from the management level. Otherwise, the project will most likely not be able to make use of

the required resources (e.g., personnel, finances, and computational hardware), and will fail to meet the overall goals.

The various steps within InTP phases form a continuous life cycle. An InTP offers the organization the ability to identify and prevent changing risks, detect an incident as it occurs, and once an incident has occurred, respond to the incident in an efficient manner. The analysis and lessons learned from incidents will feed information back into the planning phase, allowing to continuously develop and improve the programme.

We also looked at several types of detection indicators. We did not attempt to compile a definitive list, but rather to propose a more generic structure that can be customised in each organisation for the creation of an InTP. Along with the list of indicators, we also provided an analysis of the relevance of each indicator to different insider threat profiles.

5. Legal Analysis

The study has proposed a number of different measures and detection indicators (section 4.3) that should be monitored when tackling threats posed by insiders, however the legality of such actions has not yet been discussed. The following sections will present a series of hypothetical scenarios which are inspired by the insider profiles (section 3.3) and the potential detection indicators. The legal assessment for the scenarios is an abstract account based on examples from German and Estonian law. The scenarios reflect only a small number of possible profile and indicator combinations, but the assessments put forward a selection of legal issues of general nature, whereas a more thorough legal analysis will have to take into account detailed conditions of the scenario together with relevant legislation and case law. Different legal regimes may have different approaches to regulating the described situations. In many cases, due to the legal rules not being detailed enough and case law being insufficient, the final legal assessment of the specific scenario would be at the discretion of domestic courts.

5.1. Immediate Termination of the Employment Contract and Revocation of All Access Rights

This scenario presents a case where an employee has caused a serious security incident and now might be trying to take additional steps to cover up the action by destroying evidence. Immediate action has to be taken by the organisation. This situation could occur for all insider threat profile types, but is more likely to happen for the fraud, espionage, and unintentional insider profiles.

Scenario 1

Following a recent security incident, the organisation has conducted an internal inquiry regarding the extreme violation of policies and employment contract concerning an employee. Since the organisation feels that they cannot take the risk of allowing the employee continued access to organisation's resources (e.g., workstation, e-mail, files), they have suspended all access for the employee, who will be escorted from the premises immediately. The organisation has decided that no further services are required from the employee and the contract will be terminated ASAP. All personal belongings will be handed over to the person in question.

Can the employer revoke all access to resources immediately (to avoid any further potential damage) without providing a grace period for the employee to finish any ongoing tasks?

5.1.1. Legal Assessment

The contractual relationship between an employer and employee is usually outlined in the employment contract governed by specific legal regime.[22] In certain circumstances, such as when employed by the government, the work relationship may also be governed by further regulations.[23]

In general, all rights and obligations of both the employer and the employee have to be exercised until the end of the contract termination deadline.[24] If the employer submits a notice of dismissal that will come into force after a certain period of time, the employee may still have the right to access the work email account and work-related devices, in particular if the employer still wants him to continue working until a certain day. However, once the employment contract is terminated, all the claims deriving from the employment

[22] E.g. the Estonian Employment Contracts Act RT I, 12.07.2014, 1 [84].

[23] E.g. the Estonian Civil Service Act RT I, 29.06.2014, 109 [85]; German Federal Civil Service Act, BBG, *Bundesbeamtengesetz* 5th of February 2009 (BGBl. I S. 160), last amended 6th of March 2015 (BGBl. I S. 250) [76].

[24] E.g. In Germany, regulations §§ 620 ff on the termination of the employer-employee relationship of the BGB, (German Civil Code, *Bürgerliches Gesetzbuch*, 2nd of January 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), last amended 29th June 2015 (BGBl. I S. 1042)) apply [80].

relationship (such as returning all the devices the employee used for fulfilling work tasks, or terminating access to work-related email accounts) need to be satisfied.[25] Accordingly, the employer may revoke access to all work related accounts.

Under certain circumstances such as inability to fulfil his or her work-related tasks due to committing a fraud or otherwise losing the trust of the employer, or causing serious damage, the employer has the right to extraordinarily terminate the employment contract.[26] A warning for such a termination is not always needed, for example in a situation where the employee has seriously breached his or her obligations.[27] The law provides therefore the option for the employer to terminate the contract without a period of notice if the circumstances show that the continuation of the employment until the agreed date of termination or until the end of the ordinary legal period of notice proves to be unacceptable.[28] The basis for such a termination can be different in different legal systems and courts might judge differently from case to case. But in general such circumstances can justify the immediate denial of all access.

5.1.2. Recommendation

The employer should review the employment contract in order to ensure that these include an agreement to, in case of a discovery of a breach or any data misuse, immediately revoke all access rights after announcing the termination of the employment contract. Depending on the nature of the tasks of the employee and on having access to relevant systems, the conditions for such access may be further elaborated in the employment contract. The employer, for example, may want to specify that revocation of all access rights applies from the moment of uncovering misbehaviour or even from the moment on when first suspicion aspects arise. This way, the employee would not have the right to access work-related systems even before the official employment contract is terminated.

5.2. Hand-picking Users for Data Stream Monitoring

The scenario is aimed at situations where non-technical detection indicators (i.e., personal, behavioural, and background indicators) suggest that an employee's risk level has elevated. This requires more thorough targeted monitoring than is normally undertaken. By the term targeted monitoring, we mean that the user's incoming and outgoing data streams (e.g., network traffic, e-mails, phone calls, database transactions, etc.) will be stored for inspection by the security analyst.

Scenario 2

An employee has submitted a resignation application to leave for a position in another organisation. The employment contract is set to end in 30 days. Meanwhile the employee will continue to fulfil his duties and has been instructed to hand over any unfinished work to a colleague that has been assigned as his replacement. InTP indicators (see 3.3.2 Theft of Intellectual Property) suggest that employees are most likely to steal any intellectual property or other valuable data within the last 30 days prior to leaving the organisation. The security team would like to monitor employees who are either leaving or displaying some other non-technical indicators.

Is the organisation's security officer allowed to hand-pick users for in-depth data stream monitoring?

[25] Estonian Employment Contracts Act RT I, 12.07.2014, 1., § 84 (1) [84]; § 611 ff. German Civil Code [80].
[26] Estonian Employment Contracts Act RT I, 12.07.2014, 1., § 88 (1) [84]; § 626 I German Civil Code [80].
[27] Estonian Employment Contracts Act RT I, 12.07.2014, 1., § 88 (3) [84]; § 626 I German Civil Code [80].
[28] § 626 I German Civil Code.

5.2.1. Legal Assessment

Scenario 2 refers to whether an employer can monitor its employees. The underlying principle here is that all monitoring options must be outlined in the employment contract or in further regulation provided by the employer, with the consent of the employee, or derive from law; without fulfilling these conditions, such monitoring may be illegal.

While the employer may have an eligible interest to control the fulfilment of the work-related tasks and for that purpose process employee's personal data,[29] he must respect the employee's privacy and control the fulfilment of work-related obligations in a way that does not breach the employee's fundamental rights such of privacy and secrecy of correspondence.[30] In Germany, for example, the basic right that may be breached with such monitoring is the employee's 'right to informational self-determination' deriving from the German Constitution.[31]

Different legal frameworks offer various levels of analysis regarding whether basic rights have been breached. Generally, it needs to be identified which basic rights may have been breached, whether such a breach has any legal bases or justification, and whether such a breach is proportionate. Proportionality must always be considered when analysing the possible breach of fundamental rights, meaning that the chosen measures must be first of all suitable for the fulfilment of their goal, secondly, necessary and finally, moderate.[32] The legal assessment will be done based on relevant legislation and case law.

Further data protection concerns are outlined in national legislation[33] that within the European Union will have to be in accordance with the EU regulation.[34] The EU framework ensures a certain level of harmonisation by outlining a number of principles such as the obligation to ensure that personal data must be (a) processed fairly and lawfully; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; (d) accurate and, where necessary, kept up to date; and (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.[35] The Directive also prescribes an exhaustive list of bases for such processing including, *inter alia*, unambiguous consent of the data subject; or being necessary for the performance of a contract to which the data subject is party; or being necessary for compliance with a legal obligation to which the controller is subject; or being necessary in order to protect the vital interests of the data subject.[36] Outside the EU, the approaches to data protection may differ considerably.

---

[29] Personal Data Protection Act (hereafter IKS), RT I, 29.06.2014, 109, IKS § 14 (1), p 4 [85].
[30] Estonian Employment Contracts Act RT I, 12.07.2014, 1., § 28 (2) p 11 [84].
[31] The Federal Constitutional Court deduced in the case '*Volkszählung*' (BVerfGE 65, 1) [88] the right to informational self-determination from Articles 2 I, 1 I of the German Constitution, *Grundgesetz*, 23rd of May 1949 (BGBl. S. 1), last amended on 23rd December 2014 (BGBl. I S. 2438) [78].
[32] Estonian Data Protection Inspectorate (AKI), *Isikuandmete töötlemine töösuhetes*, 2011, p 10-11 [72].
[33] For example, in Germany the Federal Data Protection Act (BDSG) serves as major basis for the legal assessment of the relationship between employer and employee with regard to data, *Bundesdatenschutzgesetz*, 14th of January 2003 (BGBl. I S. 66), last amended on 25th February 2015 (BGBl. I S. 162), hereafter BDSG [99]. In Estonia, the principles for data protection derive from the Constitution as well as Personal Data Protection Act RT I, 29.06.2014, 109 [85].
[34] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 281 , 23/11/1995 P. 0031 – 0050 [86]. Principles pertaining to personal data processing will be part of chapter II of the future General Data Protection Regulation which will replace the 95/46/EC Directive and is expected to be enacted by end of 2015 with a transition period of two years. The draft (Council of the European Union, 11th of June 2015, Interinstitutional file 2012/0011 (COD), 9565/15) can be accessed at [81].
[35] Directive 95/46/EC, Article 6 [86].
[36] Directive 95/46/EC, Article 7 [86].

5.2.2. Necessity to Make a Decision and the Existence of Concrete Suspicion

In hand-picking an employee for monitoring, a number of aspects deriving from domestic regulation need to be taken into account.

For example, Germany has established as a general rule that, in the context of an employment relationship, personal data can be collected and processed only if it is considered necessary for the purpose of the establishment, exercise or termination of the employment contract.[37] However, legal frameworks may differentiate between different types of data. In some cases the employer may not process 'delicate personal data' if the legal basis for such processing derives only from the employment contract; instead the legal basis must be clearly stipulated in law or be with the consent of the employee;[38] whereas such a restriction would not apply to general personal data.[39]

The law may also prescribe conditions under which the behaviour of the employee may give grounds for *ad hoc* monitoring such as if there is a concrete suspicion of an employee having committed a criminal act which is related to his work environment.[40] Domestic legislation may stipulate that the suspicion of having committed a minor breach of law such as an administrative offence would not suffice.[41]

In contrast, simple hand-picking of a user without a concrete suspicion for the purpose of further monitoring than foreseen in the employment contract without a reason is not allowed by German law.[42] Such data screenings must be always based on concrete suspicion and facts.

5.2.3. Recommendation

The employer must ensure that the employment contract or internal regulation includes the reasoning and conditions for possible *ad hoc* monitoring, and these must be in accordance with the law. Should such monitoring occur, it should be protocolled and the person who is being screened has to be specified. To avoid possible problems, a second person (if possible the Data Protection Officer) should be present when screening the employee's data.[43]

5.3. An Automated Monitoring System Requires Human Intervention in Interpreting Data

To some extent this scenario is similar to scenario 2, but in this case the automated monitoring system has already detected suspicious activity originating from an employee and generated some alerts. This information already provides a basis for suspicion that could warrant further investigation. Unfortunately, automated systems are not guaranteed to give definitive answers, so a human analyst is required to take a closer look to interpret the data. If the suspicion remains, more detailed targeted monitoring could be set up for this user to confirm the suspicion and gather supporting evidence.

[37] § 32 I 1 BDSG, German Federal Data Protection Act, (BDSG) [99].
[38] See for example § 4 I, II German Federal Data Protection Act, (BDSG) [99].
[39] Estonian Data Protection Inspectorate (AKI), *Isikuandmete töötlemine töösuhetes*, 2011, p 35 [72].
[40] The criminal act must fall under the scope of § 12 of the German Criminal Code: *Strafgesetzbuch* 'StGB', meaning the suspicion of a 'crime', German Criminal Code, *Strafgesetzbuch*, 13th November 1998 (BGBl. I S. 3322), last amended on 12th of June 2015 (BGBl. I S. 926), hereafter StGB [77]; see also Seifert, in Simitis, BDSG, § 32, Rn. 102 [100].
[41] § 32 I 2 BDSG [99].
[42] § 32 BDSG [99].
[43] See also for example Intersoft Consulting Services, *Darf der Arbeitgeber Emails der Mitarbeiter lesen?* [87].

Scenario 3

The automated security monitoring system has generated an alert for a workstation in response to an unusually high number of file retrievals from the organisation's file server. This was followed by an alert from the organisation's e-mail server that an e-mail including several large attachments was sent to an external address from the same workstation. This sequence of events could potentially indicate data exfiltration, but in order to investigate these alerts, the security officer would need to access the work mailbox and open the e-mail to verify the purpose and the legitimacy of the contents. There is a possibility that the alert may be a false positive, which might not be valid reason to invade a person's privacy.

This kind of automated monitoring systems often require human intervention in interpreting data. **Can the security officer invade a person's privacy based on suspicion that stems from alerts generated by the monitoring systems?**

5.3.1. Legal Assessment

In general, the same legal assessment applies as the response to scenario 2. Whereas *proportionality* is a principle relevant to all the scenarios under discussion, it should be explicitly underlined here since the German law emphasises the importance of the proportionality of the applied measures in automated monitoring. Accordingly, the employer first has to verify whether the intended measure is necessary or whether less intensive measures could be used instead (see also the reasoning under Scenario 2).

It is the obligation of the employer to verify that his interest to use personal data in order to discover a potential criminal act overweighs the right to informational self-determination of the employee.[44] The careful balancing of these rights should take into account a number of considerations. For example, if the employer already considers the alert to be a 'false positive', then it might be helpful to ask oneself certain questions before processing personal data, for example – *What facts does the alert reveal? Do the facts show high or low probability for a certain unacceptable behaviour? What impact would it have if it turns out to be a 'true-positive'?*

Under German law, preventive measures such as data mass screening for the purpose of finding out whether there might be a suspicious employee are not allowed.[45] Instead, the employer is first required to have concrete facts leading to suspicion. Preventive measures may only be allowed for the purpose of making a decision concerning one of three options: the establishment, exercise or termination of the employment.[46] So it is not possible to simply handpick one employee and monitor his data without any reason (see Scenario 2).

5.3.2. Means of Automated Monitoring

The employer must ensure that the employment contract or internal regulation include the reasoning and conditions for such monitoring, and these must be in accordance with the law.

The regulation for automated monitoring may also depend on the different means employed. Some legal frameworks allow for the use of surveillance technology without the consent of the individual, if this is to be done for the purposes of protecting individuals or assets in situations where this does not excessively damage the legitimate interests of the data subject and the collected data is used exclusively for the purpose for which

[44] Deriving from §32 I 2 BDSG [99].
[45] Seifert, in Simitis, BDSG, § 32, Rn. 103 (legal commentary) [100].
[46] § 32 I 1 BDSG [99].

it is collected.[47] This means that even though, for example, video monitoring of employees has been regarded by the courts as a very intensive intervention in the right to self-determination, some legal frameworks allow it as long as the individuals that may be monitored through such automated means are aware that such monitoring takes place, for what purposes it is implemented, and who is conducting the monitoring.[48] However, like in any example of monitoring, the monitoring must not disproportionally breach individuals' rights and requires, at least in Germany, a high level of justification.[49] GPS-monitoring measures (e.g. car or cell phone) are limited to cases where it serves the protection of the employee or when goods of high value are being transported (this might apply not only to bank transports,[50] but could as well apply to transport of computer equipment containing very sensitive information) or where such monitoring is needed to ensure the fulfilment of the employment contract. In the case of cell phone-tracking the employee needs to be notified about this monitoring measure.[51] In case of monitoring, it needs to be kept in mind that the processing of personal data is taking place even if the monitoring devices are merely storing personal data and no one will at a later stage get access to such data.[52]

5.3.3. Devices and Accounts Provided by the Employer

The conditions and legality of employers' monitoring of employees' telecommunications such as email traffic data and content as well as general internet use is a much debated issue.[53] The limits for such monitoring may vary in national frameworks, but there is a general differentiation between:

a) The private use of the business email account which has been provided by the employer;
b) The forbidden private use of the business email account which has been provided by the employer; and
c) Use of a private email account for business purposes.

a) An email account provided by the employer to be used only for business purposes

The specific regulation of monitoring may differ within domestic legal frameworks, but generally, the employer can prohibit the use of work-related devices for private purposes.[54] For the purposes of transparency, such a prohibition must be included in the employment contract or in internal regulations, consented to by the employee.[55] If the employer has allowed for the use of the email account only for business purposes, the employer's monitoring competences are usually wider than in situations where the dual use of the email account is allowed. In this case, the employer may check on the traffic data of the emails.[56] There still exist controversies regarding the type of data that can be monitored (traffic data or content data), but the prevalent opinion is that the employer may also control the content of the emails.[57] In some cases, there is no specific

[47] In such case, the consent of the data subject is substituted by sufficiently clear communication of the fact of the use of the surveillance equipment and of the name and contact details of the processor of the data. This requirement does not extend to the use of surveillance equipment by state agencies on the bases and pursuant to the procedure provided by law. See IKS § 14 lg 3 [85]; Seifert, in Simitis, BDSG, § 32 Rn 82 [100].
[48] Estonian Data Protection Inspectorate (AKI), *Isikuandmete töötlemine töösuhetes*, 2011, p 67 [72].
[49] For example: BAG (German Federal High Labour Court), *Urteil v. 21.06.2011*, Az.: 2 AZR 153/11 (video monitoring) [92].
[50] Seifert, in: Simitis, BDSG, § 32, Rn. 82 [100].
[51] Ibid, Rn 83; § 98 I 1 German Telecommunication Act, *Telekommunikationsgesetz*, 22nd June 2004 (BGBl. I S. 1190), last amended on 25th of July 2014 (BGBl. I S. 1266), hereafter TKG [75].
[52] Estonian Labour Inspectorate (Tööinspektsioon), *Isikuandmed töösuhetes ja reeglid töökorraldusele*, p 7 [73].
[53] For discussions in Estonia, please see the guidance documents provided by the Estonian Data Protection Inspectorate [95].
[54] Estonian Data Protection Inspectorate (AKI), *Töötajate arvutikasutuse privaatsus*, p 10 [94].
[55] Estonian Data Protection Inspectorate (AKI), *Töötajate arvutikasutuse privaatsus*, p 10 [94].
[56] Seifert, in Simitis, BDSG, § 32 Rn. 91 [100].
[57] Seifert, in: Simitis, BDSG, § 32, Rn. 91 [100]; Gola/Wronka, *Handbuch Arbeitnehmerdatenschutz*, Rn 787 [63]; Jofer/Wegerich, *Betriebliche Nutzung von E-Mail-Diensten: Kontrollbefugnisse des Arbeitgebers*, K&R 202, 235, 273 [62]; different opinion: Wedde, in: DKWW, legal commentary, BDSG § 32, Rn 15 [100]; Däubler, *Gläserne Belegschaften* Rn 351 [65]; see further for example *b*, in case the employer prohibits the private use, but does not control it and tolerates the private use by his employee.

regulation provided by law and the limits of the employer's monitoring are subject to the interpretation of the existing general laws (such as the BDSG in Germany) by the courts.[58]

b) An email account provided by the employer to be used for both private and business purposes

Generally, the right to process employees' personal data must derive from law[59] or be based on the consent of the employee. National frameworks may provide various legal grounds for such monitoring, for example 'suspicion regarding competition'[60] or 'possible breach of confidentiality'.[61] However, in both situations, the breach of the fundamental rights of the employee must be proportional.[62] The employee must be aware that his or her communication may be monitored and/or recorded and that these may be examined under the circumstances prescribed by law.[63]

In Germany the debates are ongoing. On the one hand, if the employer has allowed the private use of the email system, he may qualify as a 'telecommunications provider' and consequently not be allowed to analyse the content of the emails.[64] As telecommunications provider he has to comply with the requirement of secrecy of telecommunications[65] in order not to commit a criminal act.[66] The same applies to the situation when the employer prohibits the private use of the business device but does not control it on a regular basis and tolerates the known private use of the business email account by employees. This behaviour might lead after a certain period (six months or up to a year) to the employee's right to proceed this way.[67]

However, the legal assessment of such situations has been inconsistent. Some courts have not followed the view that the employer has to be regarded as telecommunications provider because the employer does not provide access to its email system for economic purposes.[68] It might therefore also be possible that even though the employer allows the private use of the email system, he is allowed to control the content of the emails. But there has not yet emerged any court sentence from the German Constitutional Court. In any case, the employer has to respect the right to informational self-determination of the employee, which could mean in some cases that if an employer has marked certain emails with the subject 'private', then the content may not be read.

c) Use of a private email account for work-related e-mails

Situations where a private email account is used for work-related communication and the data needs to be accessed by the employer have usually not been regulated by law. Neither in Estonia nor in Germany is there an explicit provision regulating the employer's right to the business-related data stored in employees' private accounts.[69] In Germany, it may be possible to get access to the stored business data by filing a suit as the

---

[58] In Germany, for example, a draft including more specified rules concerning data protection within the employer-employee relationship was elaborated in 2010 but negotiations have stopped until the EU finalises the data protection reform. Read more at [96] and [97].

[59] E.g. Estonian Personal Data Protection Act RT I, 29.06.2014, 109, § 14 lg 1 p 4 [85].

[60] E.g. Estonian Employment Contracts Act RT I, 12.07.21)014, 1, § 23 [84].

[61] E.g. Estonian Employment Contracts Act RT I, 12.07.2014, 1, § 22 [84].

[62] See the requirement for proportionality at Scenario 2 (in section 0).

[63] Estonian Data Protection Inspectorate (AKI), *Töötajate arvutikasutuse privaatsus*, p 10 [94].

[64] Seifert, in Simitis, BDSG, § 32, Rn 92 [100]; §§ 99 I 4 TKG (Telecommunication Act) [75] and; § 11 I Nr. 1 TMG (Telemedia Act), *Telemediengesetz*, 26th February 2007 (BGBl. I S. 179), last amended on 1st of April 2015 (BGBl. I S. 434) [74].

[65] § 88 TKG [75].

[66] § 206 StGB, German Criminal Code [77].

[67] Weitzmann, John H., *Was darf der Chef wann kontrollieren?*, 14 March 2013 [58].

[68] VGH Karlsruhe, *Urteil v. 27.05.2013*, 2 K 3249/12, Rn 63 (verdict of the Higher Administrative Court Karlsruhe) [66]; VGH Baden-Württemberg, *Urteil vom 30.07.2014* – 1 S 1352/13 [67]; LAG Berlin-Brandenburg, *Urteil vom 16.02.2011* – 4 Sa 2132/10 [71]; LAG Niedersachsen, *Urteil vom 31.5.2010* – 12 Sa 875/09 (last two are verdicts of labour courts of 2nd instance) [69].

[69] Apart from the general obligation according to which, once the employment contract is terminated, all the claims deriving from the employment relationship (such as returning all the devices and tools the employee used for fulfilling work tasks) need to be satisfied. This may be interpreted also to include data that is proven to be owned by the employer. See

employer has the right to information.[70] The court will usually also ask the employee to provide an affidavit.[71] The claim can be connected with a so-called 'action of trover',[72] meaning that the employee will most probably have to hand over the business data and delete business-related content from his private device.[73] There has been very little case law on this issue. A German Labour Court of first instance[74] discussed the question whether XING-contacts (a similar website as Linked-In) are part of business data[75] or whether they belong to the ex-employee with the result that under certain circumstances[76] the employer could have the right to claim the data.[77] In this specific case the contacts collected by the employee were not considered as business data as they were only added to the employee's contact list because of working in the same field or because they were colleagues. The court made clear that these contacts could only be considered as business data if they were collected from the very beginning for a specific business activity.

Furthermore, there may be a difference in whether the private email was used for work-purposes from the device provided by the employer or from another (private) device. In the former case, the employer may have more options to access the data, should the need for necessary legal grounds be satisfied (see Scenario 2).

Although the discussion of criminal proceedings is out of the scope of this paper, there may be grounds for law enforcement to access that data, in accordance with national legislation.

5.3.4. Monitoring Employee's Internet Traffic

If the employer wants to monitor an employee's internet traffic, monitoring must have specific goals such as to ensure the security of the computer system and the control of the fulfilment of the employee's work-related tasks.[78] Such monitoring may be based on the need to fulfil the employment contract,[79] with the consent of the employee or on other basis outlined in law.[80] Importantly, such monitoring must be necessary for ensuring the security of the computer systems and justified as a measure in addition to other preventative tools such as filtering access to certain pages or displaying automatic messages. The Estonian Data Protection Authority has concluded that given the existence of many other measures, automated monitoring and analyses of the employee's internet traffic may not be proportionate with the breach of employee's basic rights.[81] In Germany, monitoring internet traffic follows the same rules as monitoring email activity as to traffic and content (see sections 5.3.2 and 5.3.3).[82] If the employer has allowed the private use of the internet, it must be assessed to

---

Estonian Employment Contracts Act RT I, 12.07.2014, 1., § 84 (1) [84], together with relevant provisions from Law of Property Act RT I, 30.06.2015, 4 [83].

[70] § 242 BGB (German Civil Code), deriving from the principle of equity and good faith [80].

[71] An affidavit is a written, *ex parte* statement made or taken under oath before an officer of the court or a notary, public or other person who has been duly authorised so to act, Gifis, Steven H., Law Dictionary, 5th edition, p. 16 [64].

[72] § 985 BGB [80].

[73] This procedure is not regulated by the BDSG but by the Civic Code '§§ 242, 259 BGB' [80] and the general civil procedural law called – the code of civil procedure *Zivilprozessordnung,* 'ZPO', 5th December 2005, BGBl. I S. 3202; 2006 I S. 431; 2007 I S. 1781; last amended 31 August 2015 (BGBl. I S. 1474) [101].

[74] Arbeitsgericht Hamburg, *Urteil vom 24.01.2013*, Az. 29 Ga 2/13 (Labour Court sentence of first instance); Discussions also concerned the question on who is the owner of the account. The Court outlined that the answer depends on the answer to certain questions, for example 'what email address was used for the registration? If payment for the account is needed, who pays for it?' [93].

[75] Meaning secret business data under the competition Act 'UWG'; *Gesetz gegen den unlauteren Wettbewerb*, 3rd March 2010 (BGBl. I S. 254), last amended on 1st of October 2013 (BGBl. I S. 3714) [79].

[76] These circumstances can refer for example to the question whether the employee gained these contacts before or after the employment or whether he gained them due to work-related activities.

[77] Arbeitsgericht Hamburg, *Urteil vom 24.01.2013*, Az. 29 Ga 2/13 (Labour Court sentence of first instance) [93].

[78] Estonian Data Protection Inspectorate (AKI), *Isikuandmete töötlemine töösuhetes*, 2011, p 65 [72].

[79] IKS § 14 lg 1 p 4 [85].

[80] Estonian Data Protection Inspectorate (AKI), *Isikuandmete töötlemine töösuhetes*, 2011, p 65 [72].

[81] Estonian Data Protection Inspectorate (AKI), *Isikuandmete töötlemine töösuhetes*, 2011, p 65 [72].

[82] Seifert, in Simitis, BDSG, § 32, Rn. 93 [100].

what extent that private use during working can be accepted by the employer before considering it a breach of the employees' duties.[83]

5.3.5. Notification of Monitoring Activity

Some legal frameworks require the employer to notify the employee about such monitoring and also give the data subject the right to access the data that has been stored about him or her.[84]

5.3.6. Recommendations

The employer should not allow the private use of devices in order to take advantage of the wider scope on monitoring rights. This prohibition should further be controlled on a regular basis in order to avoid the development of a contrary but tolerated behaviour which might then lead to a common practice.[85] This common practice consequently would lead to limited options for data controlling as it is regarded equal to the situation when an employer allows the private use of the device. As noted before, the employer must ensure that the employment contract or internal regulation includes the reasoning and conditions for such monitoring (even if done irregularly as spot checks), and these must be in accordance with law.

If email is to be used for both private and business communication, this must be as transparent as possible. For example, the employer could require the employee to delete personal emails after they have been sent or received, to clearly label private emails, or to store them in a specific folder only for private use.[86]

If the employer has allowed the private use of devices provided by the employer, 'proportionate controlling' may be introduced. This means that there could be an agreement according to which limited access to certain service providers such as Gmail or Yahoo! are allowed which would possibly make it easier for the employee to separate private and work-related communication.[87] Of course, such policies would not prevent the employee from illegally transmitting business data.

When monitoring the content of the emails the four-eye-principle should be used and the results recorded, stating why and to what extent emails have been opened and read. A second person should be the Data Protection Officer of the company.[88]

The employer should also consider announcing an explicit prohibition on the use of a private email account for business-related communication.[89]

5.4. Requiring Essential Personnel to Relinquish Their Private Cryptographic Keys

It is important for an organisation to protect data from being exposed to unintended audiences. It is even more important to detect when someone is trying to intentionally exfiltrate data from the organisation. Continuous monitoring of the organisation's computer systems and networks is essential in detecting when someone is exfiltrating data. Using end-to-end encryption is a good technique to protect data from being read by unintended recipients, but encrypting data using privately generated cryptographic keys that are not shared

[83] Ibid [100].
[84] IKS § 15, IKS § 19 [85]. Also, § 4 III BDSG foresees a notification of the affected person when using personal data [100].
[85] Oettinger, Renate, *Wie weit darf der Chef Mails kontrollieren?*, 02 June 2015 [61].
[86] Estonian Data Protection Inspectorate (AKI), *Isikuandmete töötlemine töösuhetes*, 2011, p 58 [72].
[87] See also Intersoft consulting services, *Überwachung am Arbeitsplatz: E-mail vs Datenschutz*, 13 December 2010 [98]; Riedemann, Sonja, *Spähangriff im Büro*, 19.07.2013 [60].
[88] See also for example Intersoft Consulting Services, *Darf der Arbeitgeber e-mails der Mitarbeiter lesen?*, 27 November 2014 [98].
[89] For example, in case a personal profile is set up on some business-related web service for business purposes only, such as Linked-in or other social media, agreement in the employment contract could include the obligation of the employee to use the business email address as registration and contact email address, the obligation of the employer to provide necessary payments as well as agreement on having at least a 2nd person know about the passwords that this person may also access the account for business purposes.

with the organisation would allow an insider to transmit any data to an external environment without it being examined by the monitoring system.

Scenario 4

In order to verify that no sensitive data is leaving the organisational network, the Security Officer (SO) needs to gain visibility of the encrypted data streams. This would also allow him to investigate security incidents more efficiently when any suspicion arises. To achieve a first level of protection, a man-in-the-middle proxy has to be implemented and all traffic originating from the organisational network diverted through the proxy. However, this solution does not help when, data (e.g., a file) has been already encrypted by the sender before being transmitted over the network. To address this, it would be necessary to acquire any private cryptographic keys that are self-generated by employees for storing and transmitting encrypted data. The SO would like to introduce a new internal regulation that requires employees to hand over any cryptographic keys that they are using in the work environment.

Can the SO require personnel to relinquish their private cryptographic keys, which can be used to decrypt any intercepted data?

5.4.1. Differentiation between Private and Work-only Use

Like Scenario 1 above, once the employment contract is terminated, all the claims deriving from the employment relationship (such as returning all the devices or private cryptographic keys the employee used for fulfilling work tasks, or terminating access to work-related email accounts) need to be satisfied.[90] Also, according to the German Civil Code, the employer has the right to information as he is the owner not only of the device and work results but also of the system which is used to run the computer. However, it is questionable whether the employer may demand the private cryptographic keys that the employee claims to have used only for private purposes.[91]

5.4.2. Recommendation

In order to avoid problems regarding accessing the system in general, the employer should ensure that private cryptographic keys are not used for the fulfilment of work-related tasks or that cryptographic keys are shared with an assigned trustful person (e.g. Data Protection Officer) and stored in a secure manner.

5.5. Requiring Essential Personnel to Relinquish Their Communication Devices for Inspection

The various features and connectivity that mobile devices offer has been increasing rapidly during the past decade. Mobile devices are used for much more than just calling other people. For example, they can be conveniently used for accessing e-mail (including work e-mail), taking photos, and sharing files. This can be a problem when people are working with sensitive data on a daily basis, and are using their mobile devices to access and (maybe even unknowingly) store this data.

[90] Estonian Employment Contracts Act RT I, 12.07.2014, 1., § 84 (1) [84].
[91] E.g. Data Protection Act – see above mentioned notes on § 32 BDSG on Scenarios 2 and 3 [100].

Scenario 5

The security team wants to introduce new security checks to verify that employees working with sensitive data have not stored any of that data on their mobile communication devices (phones, tablets, etc.). Doing so would violate organisational policy and also put the data at risk from theft or malware that is becoming more common for mobile devices. The security checks would require essential personnel to relinquish their communication devices (both personal and those assigned by employer) to make sure that they comply with policies and regulations.

It is common for employers to allow personally owned devices to be brought to the office and used in the work environments. Alternatively, even if the device is provided by employer, then, due to human factors, it might still contain some private data (e.g., messages, e-mails, etc.).

Is it allowed to have random security checks to inspect what kind of data is stored on and transmitted using either personal or employer's mobile device?

5.5.1. Return of the Device Provided by the Employer

Like Scenario 1, once the employment contract is terminated, all the claims deriving from the employment relationship (such as returning all communication devices) need to be satisfied.[92] Also, according to the German Civil Code, the employer retains the right to information as he is the owner not only of the device and work results but also of the system which is used to run the computer.[93] If the employer discovers private data then he is limited in accessing or using that data even if the private use of the device was prohibited.[94] If the employer discovers private data on the device, he would immediately have to stop reading and close the message.[95] He may delete private data[96] unless there is reason to assume that the legitimate interests of the employee would be impaired.[97] It would be different if the employer had allowed the employee to use the device also for private purposes because then the private use of the device is considered part of the remuneration.[98] In this case the employee is entitled to keep the device until the very last day of the employment which would give the employee time to eliminate all private data from the device. If the employee is asked to turn over the device at once, it may amount to cutting back on his salary which in the end could lead to a claim for damages.[99]

On the differentiation between the business and private data, please refer to section 5.3.3.

[92] Estonian Employment Contracts Act RT I, 12.07.2014, 1., § 84 (1) [84].
[93] LAG Köln, *Urteil vom 21.07.2011*, Az: 7 Sa 312/11 (verdict of the Higher Labour Court Cologne) [70].
[94] § 32 BDSG [99], see scenarios 2 and 3.
[95] This consequence derives from the personal rights of the employee which have to be considered when making use of § 32 BDSG [100]; see also Intersoft Consulting Services, *Darf der Arbeitgeber E-mails der Mitarbeiter lesen?*, 27 November 2014 [87].
[96] § 35 II BDSG [99].
[97] § 35 III Nr. 2 BDSG [99].
[98] See Schwand, Frank, *Wenn Mitarbeiter Unternehmens-Laptops privat nutzen, besteht Regelungsbedarf*; 23 April 2014 [59].
[99] According to § 615 BGB (German Civil Code) the employer can claim his salary. The private use of a business device such as notebook, cell phone is in contrast to the private use of a business car exempted by law from tax payment (German Taxation Act EStG § 3 Abs. 45) and therefore is usually not listed in the certificate of salary. It nevertheless constitutes part of the monthly salary as it is considered as financial advantage [80].

5.5.2. Handing Out the Private Device

If the employee uses a private device for working purposes, it is difficult for the employer to get access to the device without the consent of the employee.[100] The employee is the owner of the device and therefore the only person entitled to control the data stored on it. It might be possible to enforce the claim to data deletion on the private device and to reclaim stored business data by legal action (so called 'action of trover', see also 5.3.3 subsection c)) at the Labour Court.[101] The employer's only way to find out what kind of business data is stored on the private device is by filing a suit as the employer has the right to that information[102] and the employee will most likely have to provide the information and an affidavit.

Although the discussion of criminal proceedings is out of the scope of this paper, there may be grounds for law enforcement to access that data, in accordance with national legislation.

5.5.3. Recommendation

The employer should always provide the employee with a company device and explicitly prohibit (in the employment contract or internal regulations) its private use. If the employee is entitled to keep the device until the day of termination of the contract, the employer might rather run the risk of being sued for damages than the risk that the employee might meanwhile delete not only private but also business data on the device that he or she is supposed to give back.

5.6. Conducting Forensic Activities on Any Devices which are Provided by Contractors

Running basic security and background checks when hiring contractors is most likely commonplace, however, it is important to be persistent even after a long-term contract has been signed. It can prove difficult to verify whether all the contractors are actually maintaining the same level of security standards that were specified when making the contract – especially in unexpected situations (e.g., when an employee falls ill and somebody is quickly required as a replacement). Contractors regularly come in to bring supplies or perform maintenance (e.g., printers, coffee machines, and water coolers). Some of these devices might even be situated in areas where sensitive information is handled or discussed. Therefore, it would be wise to review in which areas these devices are located, and consider which devices external contractors are able to access, and whether they are accompanied at all times.

Scenario 6

The Security Officer would like to initiate regular (forensic) checks of devices that are being maintained by external contractors. He does not want to notify the contractors of the checks since that might alert the contractor and create additional concerns.

Is the security team allowed to conduct forensic activities on any devices which are provided by contractors (e.g. water cooler or coffee machine in the security area)?

[100] Note that in Germany this justifies a warning about being dismissed; under certain circumstances it can justify the immediate termination of the employment (*BAG, Urteil v. 24.03.2011, Az.: 2 AZR 282/10 – verdict of the Federal Labour Court)* [91].

[101] OLG Düsseldorf, *Urteil vom 27.09.2012*, Az. I-6 U 241/11 (Higher Regional Court sentence concerning handing out data from an insolvent company) [68].

[102] Deriving from the BGB/ German Civil Code [80], see answer to Scenario 4.

5.6.1. Conditions Subject to Service Contract

Conducting forensic activities on electronic devices is subject to the conditions of the contract between the service provider and the employer, or the specific consent of the service provider. Any forensic activities without such legal basis may bring a civil liability, especially if causing damage,[103] or even criminal liability.[104]

5.6.2. Recommendation

Regular forensic activities need to be agreed on beforehand in the contract with the service provider.

In general devices like coffee machines, copying machines and water coolers should be installed in areas where business talks usually do not take place to avoid interception. As to other risks (sound-disturbing mechanisms, automatic forwarding of scanned or copied documents via email from a high-tech copy machine) specific measures to examine the device should be discussed prior to finalising the contract in order to modify the general terms of the standard contract.

The examination of the device on a regular schedule is recommended and could be agreed on in the contract, for example under the condition of the presence of the provider.

5.7. Setting Up Decoy Targets

In cyber security, the use of honeypots and honey-tokens to gather information and learn about adversaries is not a new concept. The same approach could be taken to identify employees who are perhaps too curious and are looking for information that is not intended for them (e.g., PII about co-workers, budget information, salaries, contracts, etc.).

Scenario 7

The security team is interested in setting up decoy targets on the organisational network. Those targets are not used or required for everyday work, but they are simply imitating environments where some seemingly sensitive and valuable data is actively stored and modified. All data accesses and transmissions from these targets will be monitored and logged for later analysis.

Is the employer allowed to set up decoy targets (i.e., honeypots) within their organisation? If there is a suspicion that an employee might be stepping over boundaries, can the security team craft custom honeypots that would seem more interesting for suspected individual, and optionally direct the said person to it?

5.7.1. Legal Assessment

If the employer wants to test the loyalty[105] of an employee by setting up a decoy target, such testing needs to be in accordance with the law. There are two risks which have to be considered. Firstly, directing an employee actively to commit a crime might easily cross the threshold of illegal incitement.[106] This very much depends on the type of trap set.

[103] §§ 280 ff. BGB [80].
[104] § 303 StGB [77].
[105] Note that in general, testing employees' awareness on cyber security and responsible behaviour with employer's data and devices is not against the law and even encouraged by cyber security professionals.
[106] According to the German Penal Code, such activities can end up being considered as incitement and as such it is equally being punished as the active criminal himself, §§ 206, 26 StGB [77]; Estonian Penal Code, RT I, 12.03.2015, 7, § 22^1 [82], 'Attempt of instigation to criminal offence, consent to proposal to commit criminal offence and agreement to commit joint criminal offence'.

Secondly, there is the risk of liability. If the employee uses the decoy system set up by the employer with the intention to damage other third systems, the employee might be liable for damages according to the Civil law[107] and punishable according to the German Penal Code.[108]

In Germany, testing the loyalty or reliability of an individual employee requires that the employer can present already concrete evidence of suspicion (see Scenarios 2 and 3).[109] German courts have accepted this approach as an exception when there is no other way to determine the loyalty of the employee.[110] This may be necessary if the employee does not work within the direct physical sphere of the employer or usually works independently and without supervision.

Setting up a honeypot, for example, to find out on who might be the one accessing the system illegally could be comparable to an employer leaving his wallet near the copy machine in order to see whether the suspected individual takes out some money.[111] In general, setting up a honeypot in the employer's own systems is not illegal. However, the legal analysis depends on how the honeypot is used. Both of the previously provided legal examples – possible incitement and liability – may apply here.

5.7.2. Recommendation

The employer should always check with a lawyer on his specific intention on how he wants to proceed as he otherwise might end up committing a crime himself.

[107] § 823 BGB (German Civil Code) [80].
[108] § 27 StGB (German Penal Code), aiding and abetting, complicity to a crime [77]; Estonian Penal Code, 7, § 22^1, 'Attempt of instigation to criminal offence, consent to proposal to commit criminal offence and agreement to commit joint criminal offence' [82].
[109] Seifert, in Simits, BDSG, § 32, Rn. 100 [100].
[110] Ibid [100].
[111] It might also be comparable with the so-called 'agent provocateur', meaning the undercover police operation in order to disclose serious crimes – which is common practice and received constant approval by the highest German Courts, for example BVerfG NJW 1995, 651 (Federal Constitutional Court) [89]; BGH, *Urteil vom 23.05.1984*, g.M.u.L. StR 148/84; BGHSt 32, 345 = NJW 1984, 2300 (Supreme Court) [90].

6. Future Work

This study serves as an excellent gateway for further research in the field of insider threat detection. As we mentioned, this topic has been receiving more attention in the recent years, however, the technology and methods are far from mature. The broad overview of different aspects can b

While working on this study, we established contacts with several interesting organisations who we would like to cooperate with. For example, since the Carnegie Mellon University's SEI CERT has more than a decade of experience on collecting and studying insider threat data, we would have a lot to learn from them.

Regarding future activities, we have planned our upcoming work towards more academic research. Our next endeavour focuses on the development of novel detection methods for data exfiltration from organisational computer networks.

7. Project Summary

This study focused on the issue of *insider threat*. We identified that the topic in essence is not new, as there are high-profile examples (e.g., the case of Daniel Ellsberg) dating back several decades. Furthermore, the proliferation of IT systems and especially the internet has exponentially increased the number of ways in which insiders could potentially inflict damage on an organisation. We believe that this study serves as a good source of information for all organisations that are in the process or considering to implement their own Insider Threat Programme (InTP), but are having difficulties with finding support and guidelines.

It is important to note that most of the research regarding insider threat has been conducted in the United States, most notably by the CERT Division of the Software Engineering Institute at Carnegie Mellon University. Thus, many of the sources in this study also reference US-centric papers and studies. Although there seems to be a lack of research in European countries, there are, however, some national organisations (e.g., Estonian Data Protection Inspectorate) offering practical as well as legal guidance on the topic.

We also established how we define the terms *insider* and *insider threat* within our study. Those terms seem intuitive, but it was revealed that there are many sources which have introduced conflicting definitions which differ in slight technicalities. We decided to follow one of the proposed techniques to define insider threat from the perspective of three different categories – knowledge, access and trust.

In order to understand the motivation of different insiders, it is necessary to establish *insider profiles*. The study discussed five different profiles, namely IT sabotage, insider theft of intellectual property, insider fraud, espionage, and unintentional insider. To describe these profiles in more detail, we answered questions such as *who*, *when*, *why*, *how*, and *what*. Note, that the fifth profile, the unintentional insider, does not fit directly with the other four traditional profiles due to lack of intent, but since it is relevant we nevertheless included it in the discussion.

To detect and mitigate insider threats, organisations should develop and implement an InTP. This is not a product that can be bought, but rather it is a continuous process. Different products can and do have their role in an InTP, however they serve as modules rather than a full-blown solution to the problem. An InTP is going to need people who will work with the information that the programme requires. The study also discussed several key components that should always be considered in the development phase before starting to implement an InTP.

An InTP has four phases – initiation, planning, operations, and reporting. The last three phases form a loop that essentially makes InTP a continuous process. It was revealed that on the technical level there are often some organisational best practices and guidelines (e.g., BSI's IT baseline protection) already in place, however, when it comes to implementing an InTP, most problems seem to arise from the lack of support from management and the lack of consistency when implementing new solutions.

The study proposed six different types of detection indicators – three of those were more related to behavioural aspects and the other three were more technical. For each indicator we provided an assessment of its relevance to each of the insider profiles that we had defined earlier.

Finally, we discussed the legal and privacy concerns related to insider threats. We took a scenario-based approach to express various situations and questions that might arise when implementing and managing an InTP. The study brings forward seven different scenarios and presents the legal analysis related to this scenario. As a result, for some scenarios we were able to offer practical recommendations for organisations that might be facing similar situations in real life.

References

[1] D. Kushner, “The Real Story of Stuxnet,” 2013. [Online]. Available: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

[2] B. Burrough, S. Ellison and S. Andrews, “The Snowden Saga: A Shadowland of Secrets and Light,” 5 2014. [Online]. Available: http://www.vanityfair.com/news/politics/2014/05/edward-snowden-politics-interview.

[3] E. Nakashime, “Who is Bradley Manning,” 2011. [Online]. Available: http://www.washingtonpost.com/lifestyle/magazine/who-is-wikileaks-suspect-bradley-manning/2011/04/16/AFMwBmrF_print.html.

[4] E. Hansen, “Manning-Lame chat logs revealed,” 2011. [Online]. Available: http://www.wired.com/2011/07/manning-lamo-logs/.

[5] A. T. Networks, “Daniel Ellsberg, Bigraphy,” 2015. [Online]. Available: http://www.biography.com/people/daniel-ellsberg-17176398.

[6] D. Ellsberg, “Extended bigraphy,” 2006. [Online]. Available: http://www.ellsberg.net/bio/extended-biography.

[7] M. of Foreign Affairs, “The case of Herman Simm,” 2008. [Online]. Available: http://vm.ee/sites/default/files/content-editors/web-static/319/Herman_Simm.pdf.

[8] KAPO, “Judicial Decisions,” 2015. [Online]. Available: https://www.kapo.ee/eng/judicial-decisions.html.

[9] D. J. Hagemann, “Profile of Major Nidal Malik Hasan,” 2009. [Online]. Available: http://www.homelandsecurityus.com/archives/3262.

[10] K. Cooke and J. Shiffman, “Snowden as a teen online: anime and cheeky humor,” 6 2013. [Online]. Available: http://www.reuters.com/article/2013/06/13/us-usa-security-snowden-anime-idUSBRE95B14B20130613.

[11] J. Jacob, “Edward Snowden Scandal: 'CIA Sent Him Home But NSA Hired Him Later',” 10 2013. [Online]. Available: http://www.ibtimes.co.uk/edward-snowden-scandal-cia-nsa-hired-warning-513190.

[12] R. Greenslade, “How Edward Snowden led journalist and film-maker to reveal NSA secrets,” 8 2013. [Online]. Available: http://www.theguardian.com/world/2013/aug/19/edward-snowden-nsa-secrets-glenn-greenwald-laura-poitras.

[13] F. Schmid and A. Ulrich, “Betrayer and Betrayed,” 2010. [Online]. Available: http://www.spiegel.de/international/europe/betrayer-and-betrayed-new-documents-reveal-truth-on-nato-s-most-damaging-spy-a-693315.html.

[14] “Insider Threat,” [Online]. Available: http://www.cert.org/insider-threat/.

[15] B. M. Bowen, M. B. Salem, S. Hershkop, A. D. Keromytis and S. J. Stolfo, “Designing Host and Network Sensors to Mitigate the Insider Threat,” in *IEEE Security and Privacy*, vol. 7, 2009, pp. 22-29.

[16] P. Institute and Raytheon, “Privileged User Abuse \& The Insider Threat,” 2014. [Online].

[17] C. P. Pfleeger, “Reflections on the Insider Threat,” 2007. [Online]. Available: http://www.springer.com/cda/content/document/cda_downloaddocument/9780387773216-c2.pdf?SGWID=0-0-45-517500-p173789752.

[18] J. Hunker and C. W. Probst, “Insiders and Insider Threats An Overview of Definitions and Mitigation Techniques,” 2011. [Online]. Available:

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.465.7490&rep=rep1&type=pdf.

[19] M. Bishop and C. Gates, “Defining the insider threat,” 2008. [Online]. Available: https://web.cs.dal.ca/~gates/papers/csiirw08.pdf.

[20] C. W. Probst, J. Hunker, M. Bishop and D. Gollmann, “08302 Summary -- Countering Insider Threats,” in *Countering Insider Threats* , Dagstuhl, Germany, 2008.

[21] G. Silowash, D. Cappelli, A. Moore, R. Trzeciak, T. J. Shimeall and L. Flynn, “Common Sense Guide to Mitigating Insider Threats 4th Edition,” 2012.

[22] J. C. of Staff, “Joint Intelligence, Joint Publication 2-0,” 2013. [Online]. Available: http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf.

[23] Carnegie Mellon University, “Insider Threat Program Manager (ITPM) Certificate,” Carnegie Mellon University, [Online]. Available: http://www.cert.org/insiderthreat/insider-threat-program-manager-itpm-certificate.cfm?. [Accessed 15 September 2015].

[24] Intelligence and National Security Alliance, “Insider Threat Resource Directory,” [Online]. Available: http://www.insaonline.org/i/p/5/i/sub/insider/index.aspx?hkey=1a611934-f929-4b9a-8f38-387509620474.

[25] “Combating Insider Threat,” 5 2014. [Online]. Available: http://www.dhs.gov/science-and-technology/csd-insider-threat.

[26] D. Cappelli, A. Moore and R. Trzeciak, The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud), New York, New York: Pearson Education, Inc., 2014.

[27] Insider Threat Center, “Handling Threats from Disgruntled Employees,” Carnegie Mellon University, 15 July 2015. [Online]. Available: https://insights.sei.cmu.edu/insider-threat/2015/07/handling-threats-from-disgruntled-employees.html. [Accessed 25 September 2015].

[28] M. Collins, “InTP Series: Key Elements of an Insider Threat Program (Part 2 of 18),” 3 2015. [Online]. Available: https://insights.sei.cmu.edu/insider-threat/2015/03/intp-series-key-elements-of-an-insider-threat-program-part-2-of-18.html.

[29] M. Hanley and J. Montelibano, “Insider Threat Control: Using Centralized Logging to Detect Data Exfiltration Near Insider Termination,” 2011.

[30] S. R. Band, L. F. Ficher, A. P. Moore, E. D. Shaw and R. F. Trzeciak, “Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis,” 2006.

[31] D. L. Charney, “True Psychology of the Insider Spy,” *Intelligencer: Journal of U.S. Intelligence Studies,* 2010.

[32] CERT Insider Threat Center, “Insider Threat Deep Dive: IT Sabotage,” Carnegie Mellon University, 22 September 2010. [Online]. Available: https://insights.sei.cmu.edu/insider-threat/2010/09/insider-threat-deep-dive-it-sabotage.html. [Accessed 15 September 2015].

[33] L. Flynn, J. W. Clark, A. P. Moore, M. L. Collins, E. Tsamitis, D. Mundie and D. McIntire, “Four Insider IT Sabotage Mitigation Patterns and an Initial Effectiveness Analysis,” The Hillside Group, 2013.

[34] A. Moore, D. Cappelli and R. F. Trzeciak, “The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures,” Software Engineering Institute, 2008.

[35] K. Corbin, “Economic Impact of Cyber Espionage and IP Theft Hits U.S. Businesses Hard,” 7 2013. [Online]. Available: http://www.cio.com/article/2384269/cybercrime/economic-impact-of-cyber-espionage-and-ip-theft-hits-u-s--businesses-hard.html.

[36] L. M. Wortzel, “Cyber Espionage and the Theft of U.S. Intellectual Property and Technology,” 7 2013. [Online]. Available: http://docs.house.gov/meetings/IF/IF02/20130709/101104/HHRG-113-IF02-Wstate-WortzelL-20130709-U1.pdf.

[37] D. C. Blair, J. M. H. Jr., C. R. Barrett, W. J. L. III, S. Gorton, D. Wince-Smith and M. K. Young, “The IP Commission; The Commission on the Theft of Americal Intellectual Property,” 5 2013. [Online]. Available: http://www.ipcommission.org/report/ip_commission_report_052213.pdf.

[38] MacDailyNews, “Samsungā€™s record of IP theft, other ruthless business tactics, and why Apple might win the battles but still lose the war,” 5 2014. [Online]. Available: http://macdailynews.com/2014/05/03/samsungs-record-of-ip-theft-other-ruthless-business-tactics-and-why-apple-might-win-the-battles-but-still-lose-the-war/.

[39] M. Riley and A. Vance, “Inside the Chinese Boom in Corporate Espionage,” 3 2012. [Online]. Available: http://www.bloomberg.com/bw/articles/2012-03-14/inside-the-chinese-boom-in-corporate-espionage.

[40] A. P. Moore, D. McIntire, D. Mundie and D. Zubrow, “Justification of a Pattern for Detecting Intellectual Property Theft by Departing Insiders,” Software Engineering Institute , 2013.

[41] A. Cummings, T. Lewellen, D. McIntire, A. P. Moore and R. Trzeciak, “Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector,” 2012.

[42] D. L. Charney, “NOIR: A White Paper,” 2014.

[43] J. White and B. Panda, “Insider Threat Discovery Using Automatic Detection of Mission Critical Data Based On Content,” in *International Conference on Information Assurance and Security*, 2010, pp. 56-61.

[44] T. C. I. T. Team, “Unintentional Insider Threats: A Foundational Study,” 2013.

[45] M. Bunn and S. D. Sagan, “A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes,” 2014. [Online]. Available: https://www.amacad.org/multimedia/pdfs/publications/researchpapersmonographs/insiderThreats.pdf. [Accessed 28 Sept 2015].

[46] H. Boström, S. F. Andler, M. Brohede and R. Johansson, “On the Definition of Information Fusion as a Field of Research,” 2007.

[47] Intelligence and N. S. Alliance, “A Preliminary Examination of Insider Threat Programs in the U.S. Private Sector,” 9 2013. [Online]. Available: http://www.insaonline.org/CMDownload.aspx?ContentKey=4eef93c3-7505-47d0-8246-155294f094de&ContentItemKey=dc21572f-2bdf-4f2e-851d-182cfbaf8938.

[48] Intelligence and National Security Alliance, “Insider Threat Resources,” [Online]. Available: http://www.insaonline.org/i/z/docs/ITResources.aspx.

[49] Federal Office for Information Security (BSI), “IT-Grundschutz,” [Online]. Available: https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz.html. [Accessed 19 October 2015].

[50] M. D. Guido and M. W. Brooks, “Insider Threat Program Best Practices,” in *System Sciences (HICSS), 2013 46th Hawaii International Conference on*, 2013, pp. 1831-1839.

[51] Office of the National Counterintelligence Executive, “http://www.ncsc.gov/,” Oct 2011. [Online]. Available: http://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf. [Accessed 3 Sept 2015].

[52] P. Schweizer, “Congressional Record,” 23 June 1992. [Online]. Available: http://fas.org/irp/congress/1992_cr/s920624-spy.htm. [Accessed 8 09 2015].

[53] B. Hoffman, C. Meyer, B. Schwarz and J. Duncan, “www.rand.ORG,” Feb 1990. [Online]. Available:

http://www.rand.org/content/dam/rand/pubs/reports/2007/R3782.pdf. [Accessed 28 Sept 2015].

[54] U.S. Department of Justice, “A Review of FBI Security Programs,” March 2002. [Online]. Available: http://fas.org/irp/agency/doj/fbi/websterreport.html. [Accessed 2 Oct 2015].

[55] S. Wood, K. S. Crawford and E. L. Lang, “Reporting of Counterintelligence and Security Indicators by Supervisors and Coworkers,” 5 2005. [Online]. Available: https://www.fas.org/sgp/othergov/dod/cireporting.pdf.

[56] E. D. Shaw and H. V. Stock, “Behavioral Risk Indicators of MaliciousInsider Theft of Intellectual Property: Misreading the Writing on the Wall,” 12 2011. [Online]. Available: http://www.symantec.com/content/en/us/about/media/pdfs/symc_malicious_insider_whitepaper_Dec_2011.pdf.

[57] D. M. Cappelli, R. F. Trzeciak and R. Floodeen, “The Key to Successful Monitoring for Detection of Insider Attacks,” 2010. [Online]. Available: http://resources.sei.cmu.edu/asset_files/Presentation/2010_017_001_52308.pdf.

[58] J. H. Weitzmann, “Was darf der Chef wann kontrollieren?,” iRights.info, 14 March 2013. [Online]. Available: http://irights.info/artikel/computer-und-internet-am-arbeitsplatz-was-darf-der-chef-wann-kontrollieren-3/12889. [Accessed 14 September 2015].

[59] F. Schwand, “Wenn Mitarbeiter Unternehmens-Laptops privat nutzen, besteht Regelungsbedarf,” acant.service GmbH, 23 April 2014. [Online]. Available: http://www.acant-makler.de/2014/04/23/unternehmen-laptops-private-nutzung/. [Accessed 14 September 2015].

[60] S. Riedemann, “Spähangriff im Büro,” SPIEGEL ONLINE GmbH, 19 July 2013. [Online]. Available: http://www.spiegel.de/karriere/berufsleben/private-e-mails-im-buero-was-darf-der-chef-a-911970.html. [Accessed 14 September 2015].

[61] R. Oettinger, “Wie weit darf der Chef Mails kontrollieren?,” IDG Business Media GmbH, 2 June 2015. [Online]. Available: http://www.channelpartner.de/a/wie-weit-darf-der-chef-mails-kontrollieren,2610576. [Accessed 15 July 2015].

[62] R. Jofer and C. Wegerich, “Betriebliche Nutzung von E-Mail-Diensten: Kontrollbefugnisse des Arbeitgebers,” K&R, 2002, pp. 235-240.

[63] P. Gola and G. Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rechtsfragen und Handlungshilfen für die betriebliche Praxis, 5th ed., Cologne, 2009.

[64] S. H. Gifis, Law Dictionary, 5th ed., NY, 2003.

[65] W. Däubler, Gläserne Belegschaften? Das Handbuch zum Arbeitnehmerdatenschutz, 5. Auflage ed., Frankfurt am Main, 2009.

[66] *VGH Karlsruhe, Higher Administrative Court, 2 K 3249/12,* 27 May 2013.

[67] *VGH Baden-Württemberg, Higher Administrative Court, 1 S 1352/13.,* 30 July 2014.

[68] *OLG Düsseldorf, Higher Regional Court, Az. I-6 U 241/11,* 27 September 2012.

[69] *LAG Niedersachsen, Labour Court of 2nd Instance, 12 Sa 875/09,* 31 May 2010.

[70] *LAG Köln, Labour Court of 2nd Instance, Az: 7 Sa 312/11,* 21 July 2011.

[71] *LAG Berlin-Brandenburg, Labour Court of 2nd Instance, 4 Sa 2132/10.,* 16 February 2011.

[72] Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon), “Isikuandmete töötlemine töösuhetes,” 2011. [Online]. Available: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhe

tes%20juhendmaterjal26%2005%202014_0.pdf. [Accessed 16 July 2015].

[73] Estonian Labour Inspectorate (Tööinspektsioon), "Isikuandmed töösuhetes ja reeglid töökorraldusele, pp. 7," [Online]. Available: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed-toosuhetes_ja_reeglid_tookorraldusele.pdf. [Accessed 16 July 2015].

[74] "German Telemedia Act (TMG), Telemediengesetz," *BGBl. I S. 179, 26 February 2007, last amended in BGBl. I S. 434,* 1 April 2015.

[75] "German Telecommunication Act (TKG), Telekommunikationsgesetz," *BGBl. I S. 1190, 22 June 2004, last amended in BGBl. I S. 1266,* 25 July 2014.

[76] "German Federal Civil Service Act, BBG, Bundesbeamtengesetz," *BGBl. I S. 160, 5 February 2009, last amended in BGBl. I S. 250,* 6 March 2015.

[77] "German Criminal Code, Strafgesetzbuch," *BGBl. I S. 3322, 13 November 1998, last amended in BGBl. I S. 926,* 12 June 2015.

[78] "German Constitution, Grundgesetz," *BGBl. S. 1, 23 May 1949, last amended in BGBl. I S. 2438,* 23 December 2014.

[79] "German Competition Act 'UWG'; Gesetz gegen den unlauteren Wettbewerb," *BGBl. I S. 3714, 3 March 2010, last amended in BGBl. I S. 3714,* 1 October 2013.

[80] "German Civil Code, Bürgerliches Gesetzbuch," *BGBl. I S. 42, 2909; 2003 I S. 738, 2 January 2002, last amended in BGBl. I S. 1042,* 29 June 2015.

[81] Council of the European Union, "General Data Protection Regulation (draft)," *Interinstitutional file 2012/0011 (COD),* no. 9565/15, 11 June 2015.

[82] "Estonian Penal Code," *RT I,* no. 7, 12 March 2015.

[83] "Estonian Law of Property Act," *RT I,* no. 4, 30 June 2015.

[84] "Estonian Employment Contracts Act," *RT I,* no. 1, 12 July 2014.

[85] "Estonian Civil Service Act," *RT I,* no. 109, 29 June 2014.

[86] The European Parliament and of the Council of the European Union, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," *Official Journal,* no. L 281, pp. 0031 - 0050, 23 November 1995.

[87] Intersoft consulting services, "Darf der Arbeitgeber Emails der Mitarbeiter lesen?," 27 November 2014. [Online]. Available: https://www.datenschutzbeauftragter-info.de/darf-der-arbeitgeber-e-mails-der-mitarbeiter-lesen/. [Accessed 9 July 2015].

[88] *BVerfG, Federal Constitutional Court of Germany, BvR 209/83, = BVerfGE 65, 1, 'Volkszählung',* 15 December 1983.

[89] *BVerfG, Federal Constitutional Court of Germany, Az.: 2 BvR 435/87, = NJW 1995, 651.,* 19 October 1994.

[90] *BGH, Federal Court of Justice, g.M.u.L. StR 148/84; BGHSt 32, 345.,* 23 May 1984.

[91] *BAG, Federal Labour Court of Germany, Az.: 2 AZR 282/10.,* 24 March 2011.

[92] *BAG, Federal Labour Court of Germany, Az.: 2 AZR 153/11,* 21 June 2011.

[93] *AG Hamburg, Labour Court of 1st Instance, Az. 29 Ga 2/13,* 24 January 2013.

[94] Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon), “Töötajate arvutikasutuse privaatsus,” [Online]. Available: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/T%C3%B6%C3%B6tajate%20arvutikasutuse%20privaatsus_.pdf. [Accessed 16 July 2015].

[95] Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon), “Töösuhted,” [Online]. Available: http://www.aki.ee/et/eraelu-kaitse/toosuhted. [Accessed 16 July 2015].

[96] Deutscher Bundestag, “Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes,” 15 December 2010. [Online]. Available: http://dipbt.bundestag.de/dip21/btd/17/042/1704230.pdf. [Accessed 26 June 2015].

[97] Intersoft Consulting Services, “Vorschriften, Kommentar und Urteile zum Arbeitnehmerdatenschutz,” [Online]. Available: http://www.arbeitnehmerdatenschutz.de. [Accessed 26 June 2015].

[98] Intersoft Consulting Services, “Überwachung am Arbeitsplatz: E-mail vs Datenschutz,” 13 December 2010. [Online]. Available: https://www.datenschutzbeauftragter-info.de/ueberwachung-am-arbeitsplatz-e-mail-vs-datenschutz/. [Accessed 9 July 2015].

[99] “German Federal Data Protection Act, Bundesdatenschutzgesetz (BDSG),” *BGBl. I S. 66, 14th of January 2003, last amended in BGBl. I S. 162,* 25 February 2015.

[100] S. Simitis, Bundesdatenschutzgesetz, legal commentary, 7th ed., Nomos, Baden-Baden, 2011.

[101] “The code of civil procedure, Zivilprozessordnung (ZPO),” *BGBl. I S. 3202, 5th December 2005; BGBl. I S. 431, 2006; BGBl. I S. 1781, 2007, last amended in BGBl. I S. 1474,* 31 August 2015.