TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Elina Sergeeva 195565IVSB

The Role of Open Source Intelligence in Employee Security Awareness Program

Bachelor's thesis

Supervisor: Kaido Kikkas
Doctor of Philosophy
in Engineering (PhD)

Tallinn 2022

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Elina Sergeeva 195565IVSB

Avatud lähtekoodiga teabe roll töötajate turvateadlikkuse tõstmise programmis

Bakalaureusetöö

Juhendaja: Kaido Kikkas
Tehnikateaduste doktor

Tallinn 2022

Author’s declaration of originality

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

Author: Elina Sergeeva

21.04.2022

Abstract

In the 21st century, individuals and companies are generating more data than ever. Besides that, the cost of data breaches is growing, and cyberattacks are becoming more targeted per individual as a result of the increased teleworking rate. The two above-mentioned factors create a demand for businesses to raise security awareness in order to address the risks and lower financial losses. Moreover, this forces businesses to seek gaps in their security programs. Such improvements in security awareness will be offered by this thesis.

In the course of this work, a security awareness training about Open Source Intelligence was designed and developed. This training is dedicated to employees of various organizations regardless of their business nature and was developed in a form of an e-course. The level of this e-course in defined as slightly advanced, and it is recommended employees have taken basic security awareness training before. The success of the chosen solution was tested in a real Baltic organization (which for the scope of this paper will be named Company X) and evaluated by running double feedback. It was also evaluated based on software and didactical indicators.

Besides practical contribution, this thesis presents analytical part which includes a deep analysis of OSINT's background and its role in modern employee security awareness programs.

This thesis is written in English and is 29 pages long, including 6 chapters, 9 figures and 1 table.

Annotatsioon
Avatud lähtekoodiga teabe roll töötajate turvateadlikkuse tõstmise programmis

21. sajandil toodavad üksikisikud ja ettevõtted rohkem andmeid kui kunagi varem. Peale selle kasvavad andmetega seotud rikkumiste kulud ning kaugtöö suurenemise tõttu on küberrünnakud üha rohkem suunatud üksikisikute vastu. Kaks eelnimetatud tegurit tekitavad ettevõtetes nõudluse tõsta turvateadlikkust, et riske ja rahalisi kaotusi vähendada. Lisaks sunnib see ettevõtteid otsima lünki oma turvaprogrammides. Selliseid turvateadlikkuse täiustusi pakub käesolev lõputöö.

Selle töö käigus töötati välja ja töötati välja turbeteadlikkuse koolitus edasijõudnud kasutajatele avalikult kättesaadavate andmete kohta. See koolitus on mõeldud erinevate organisatsioonide töötajatele sõltumata nende äritegevusest ja on välja töötatud e-kursuse vormis. Valitud lahenduse edukust testiti reaalses Balti organisatsioonis (mis käesoleva töö raames saab nimeks Ettevõte X) ja seda hinnati kahekordse tagasiside abil.

Lisaks praktilisele panusele on selles lõputöös analüütiline osa, mis sisaldab põhjalikku analüüsi OSINTi taustast ja selle rollist kaasaegsetes töötajate turvateadlikkuse tõstmise programmides.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 29 leheküljel, 6 peatükki, 9 joonist, 1 tabelit.

List of abbreviations and terms

BYOD	Bring Your Own Device - the practice of allowing the employees of an organization to use their own computers, smartphones, or other devices for work purposes.
CA	Cambridge Analytica
Company X	Alias for the company where the practical solution of the current work was implemented. Such alias was chosen for providing anonymity for the company.
Google Dorking	Aa hacking technique that makes use of Google's advanced search services to locate valuable data or hard-to-find content.
GDPR	General Data Protection Law
ICT	Information and Communication Technology
IoT	Internet of Things
ISA	Information Security Awareness
MS	Microsoft
OSINT	Open Source Intelligence
PII	Personally Identifiable Information
SANS	SysAdmin, Audit, Network, and Security, the official name of the Sans Institute is the Escal Institute of Advanced Technologies
TAM	Technology Acceptance Model is an information systems theory that models how users come to accept and use a technology.
TPB	Theory of Planned Behaviour is a psychological theory that links beliefs to behaviour.
TRB	Theory of Reasoned Behaviour is a theory explaining the relationship between attitudes and behaviours within human action.
VR	Virtual Reality

Table of contents

List of figures

List of tables

1 Introduction

Today, in the age of digitalization, all kinds of information are accessible online at any moment of time from almost any part of the globe. Besides that, modern businesses which are producing that information are becoming more and more dependent on the ICT. Hence, ensuring integrity and security of information assets is becoming a big but unavoidable challenge for organizations worldwide. And one of the most difficult trials in that challenge is about lowering the amount of human errors, due to which the amount of data breaches and their cost has been increasing over the past years [1].

For instance, a study from Stanford University Professor Jeff Hancock and a cybersecurity organization Tessian showed that 9 in 10 (88%) data breaches are caused by employees' mistakes [2]. 2021 Data Breach Investigation Report by Verizon shows that almost 40% of data breaches were caused by the action of Phishing (Social), and almost 30% were caused by Credentials Theft [3], which are quite often resulted from human errors as well[1]. Another big place is taken by ransomware: 10% of data breaches are caused by such malware. Here, it is also important to understand how machine gets infected with a ransomware. Microsoft names phishing emails and suspicious macros in MS documents as one of the root sources of ransomware infection[2]. Such statistics clearly show that human's role in preventing or allowing data breach is significant. This in its turn makes ISA (information security awareness) programs for employees and citizens in general the key component to information security when speaking of the socio-technical aspect of information security and information security in general [4].

In this paper two types of notations are used for marking down the references. First are footnotes, which are used for illustrating the statements of local importance. Those can be website links, for example. The other type is references. References are specifying the

[1] https://www.cyberpion.com/learning-center/glossary/credential-theft/

[2] https://support.microsoft.com/en-us/windows/how-malware-can-infect-your-pc-872bf025-623d-735d-1033-ea4d456fb76b.

sources of statements, which have global importance in this thesis. The full list of global reference is provided after the Chapter 7.

Another point to be stated in the introduction part, is distinguishing difference between e-learning and e-course. While e-learning is the use of electronic devices and Internet technologies to deliver a variety of solutions to enable learning and improve performance [5], an e-course is a specific instance or portion of e-learning materials.

1.1 Problem Statement and Goal

Modern security awareness trainings for employees are not covering open-source intelligence and how it can be used against organizations or individual employees. Although today information security awareness is especially important for individuals, governments, public and non-public organisations, observing security practices often proves to be difficult and public awareness is still limited [6]. If 8 years ago intermediate and in-depth security trainings were recommended for management or specialized roles only [7], today the demand in more advanced security trainings for everyone has increased and became urgent due to the massive dependance on ICT, which has increased even more in the past two years due to COVID-19 pandemic. Restrictions introduced after virus spread caused massive teleworking rates and even higher load on ICT, what in its turn increases the role socio-technical aspect of individuals daily life and puts it more at risk [6]. Moreover, with this changes the average cost of a data breach in cases where teleworking was a factor in causing the breach has increased, compared to those where remote work was not a factor [1].

In the course of the research described in this paper, the author will present an analysis of modern approaches to ISA programs, identify gaps in it and suggest a possible solution. The analysis will be concentrated on the OSINT (Open Source Intelligence), in particular on providing reasons why this topic should be a must in a successful ISA program.

The solution will be developed throughout the practical part of this work and will be represented by an e-course about OSINT. Besides that, developed training will be launched in a real Baltic organization as a part of security program, after what the feedback will be collected and analysed.

The general aim of this work is to close the gap in existing security awareness programs and make individuals and therefore organizations more secure while expanding in socio-technical aspects.

1.2 Scope and Limitations

Security awareness program solutions studied in and proposed by this thesis are not limited to one specific company but rather devoted to various companies, regardless of their business nature. However, preliminary knowledge covered by basic security awareness trainings stays out of the scope and will not be discussed. In the course of this work, it is assumed that employees already possess basic or standard information security awareness knowledge.

Developed training will be placed in an internal learning system of the Company X. The choice of an e-course development platforms is limited to only one option which is already used by the company. The reason behind such decision, is employees' familiarity with the structure and functionality of such e-learning materials. This will save time, allow more people to participate in the training, and hence make results more trustworthy.

During the time period from 14.04.2022 to 14.05.2022 the amount employees successfully passed the training has reached 442 and the total amount of people enrolled in course – 2318. By enrolling into course employees simply add it to their library saving it for later.

2 Background

Office of the Director of National Intelligence (US) defines OSINT as "publicly available information appearing in print or electronic form including radio, television, newspapers, journals, the Internet, commercial databases, and videos, graphics, and drawings." [7]. The 21st century with the rapid growth of the Internet and the World Wide Web shows a significant increase in the volume of such publicly available information and therefore intelligence. This has a substantial impact on how people learn and perceive information, express ideas and interact with each other, both socially and professionally. Intelligence community in its turn has undergone a great change: it has been granted a new legitimate status and has become a core component of analytical products used by both military and civils [9]. Therefore, OSINT's existence has always been accompanied by a discussion about ethics of its technologies, and how they can be used against individuals [10].

While there are no defined restrictions on OSINT usage, it can be abused by both legitimate and malicious actors, therefore individuals have to be aware of threats posed by open-source intelligence for the sake of both personal and corporate security and integrity. However, nowadays background research on the importance of OSINT topics inclusion into security awareness programs is limited, yet it exists contributing into this work in an indirect way. Such background will be studied in the course of this chapter.

For a comprehensive analysis and exhaustive background overview, a few aspects will be included into this part of the work: existing related work, analysis of modern approach to security awareness programs for employees, and an overview of historical events where OSINT was used against society and/or organizations.

2.1 Examples from History

Learning about how certain OSINT skills might be abused with no context provided might be confusing for a trainee. Moreover, knowing the context or specific example will enhance employees' understanding of OSINT skills implementation and, depending on the context, ability to recognize such abuse or potential threat or the prospect of positive use of OSINT. Therefore, a few historical examples will be provided in the training.

In 2015 an entire headquarters building of an Islamic State group was located with the use of OSINT and hence destroyed, as reported by Hawk Carlisle, commander of Air Combat Command, at a June 1 speech in Arlington, Virginia.[1] The experts working on the case, reported that in total the Islamic State group has published 1700 pictures, videos and other media publications, reaching up to 200,000 viewers on Twitter and other social media platforms. Although the group was using social media for recruitment, intelligence has been using it to track down Islamic State militants. In particular, one specific and key

[1] https://www.airforcetimes.com/news/your-air-force/2015/06/04/carlisle-air-force-intel-uses-isis-moron-s-social-media-posts-to-target-airstrikes/

post allowed to locate the building exactly and destroy it just after mere 22 hours. According to Carlisle the photo, which was also discovered on social media, was picturing the group's member standing at command-and-control capability for Da'Esh, ISIL. It was therefore analyzed, and location defined.

In 2016 a famous social media persona Kim Kardashian was robbed at her residence in Paris by several men dressed as police officers.[1] The total sum of stolen items exceeds 10 million dollars. When the criminals were detained by the police, the group leader admitted they used social media, in particular Kim's feed, for planning the robbery.[2] The leader mentioned: "The jewels were shown on the Internet, and [she said] that she didn't wear fakes . . . the time she would arrive in France, you just had to look at the Internet and you knew everything, absolutely everything,". The group has been monitoring Kim's media and collecting facts about her travels building up some sort of intelligence. "She gives information on social media all the time," – added the group leader to his testimony.

Another big and well known across the world case is the Facebook-Cambridge Analytica Data scandal. In 2018 Wired has published an article where it was revealed that CA had improperly obtained the personal data of more than 87 million Facebook users (where 70.7 million were from US)[3] in order to influence both the Brexit referendum and the 2016 U.S. presidential election.

Data was collected by Dr. Aleksandr Kogan's app called "thisisyourdigitallife" in 2014. Although it is a third-party application in relation to Facebook, Thisisyourdigitallife used Facebook Login[4] service to sign up and authenticate its users. This means, when choosing this option users were giving their consent on access to some range of information from their Facebook profiles.

According to the same publication from Wired, 270 000 people installed Thisisyourdigitallife and authenticated using Facebook in 2014. However 270 000 is just 0, 31% from 87 million. The reason behind this difference of registered people and

[1] https://www.bbc.com/news/world-europe-37538453

[2] https://www.vanityfair.com/style/2017/01/kim-kardashian-paris-robbery-social-media-heist

[3] https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/

[4] https://developers.facebook.com/docs/facebook-login/

number of people whose data was actually collected from Facebook is that Alexander Kogan's application was able to access not only users' data but also the user friends' profile data published on Facebook.

Although, this act of collecting data cannot be referred to as data breach or leakage, since all rights were granted to Thisisyourdigitallife by users when they agreed to terms and conditions. Regardless legitimacy of such data collection, Facebook's representatives made accusation towards Kogan's application when it was revealed that developers were sharing obtained data with Cambridge Analytica. Facebook contended it was against the company's terms of service, which at that time stated that developers are not allowed to transfer any data received from Facebook (including anonymous, aggregate, or derived data) to any ad network, data broker or other advertising or monetization-related service.

This resource along with others played a big role in the US elections in 2016. According to Aleksandr Nix's presentation at the 2016 Concordia Annual Summit in New York[1], CA was collecting from open sources the following information on each voter in the US:

Table 1. Data parameters collected by Cambridge Analytica

Demographics/Geographics (Factual)	**Psychographics (Attitudinal)**	**Personality (Behavioral)**
Age, Gender, Ethnicity, Religion, Education, Income, Homeowner, Socio-economic status, Geographic factors;	Advertising Resonance, Automotive Data, Consumer Confidence – Economy/Business, Lifestyle Data, Buying Styles/Patterns, Civic / Political Engagement Segments, Cellular / Mobil Opinions	**Psychology:** Openness Conscientiousness Extraversion Agreeableness Neuroticism **Persuasion:** Reciprocity Scarcity Authority Fear Social Proof

[1] https://www.youtube.com/watch?v=n8Dd5aVXLCc

Based on the data collection described in Table 1, CA was conducting a large-scale analysis on population and identifying triggers for changing its opinion from one state to another as desired by customer. However, not every person was a target for pulling the triggers. Company was trying to identify so called “persuadables” - people whose opinion could have been affected and therefore changed, it especially mattered in swing states, meaning those states of US where voices ratio was 50% to 50%. When such persuadable individuals were identified, they were targeted with a content specially made in accordance with other collected parameters, aiming to persuade individual towards desired vote effectively. This way opinions were changed slightly more towards required candidate on the elections.

Based on previous research [11] most participants were aware of the Cambridge Analytica scandal and its supposed attempts to influence people's political preferences. However, they lacked understanding of how data was collected and used in, and that personal information could be inferred from one’s connections networks (friends). Despite expressing concern over how organizations may use their data in future, all participants believed they would be immune to any attempts to persuade or influence their behavior. This proves one more time, that people need more awareness on such topics as OSINT, in particular skills and techniques used in its scope.

2.2 Previous Work at the University

Previous studies on OSINT-related topics among Tallinn University of Technology students include three papers. The earliest work “Estonian Government Related Challenges in Protection of Personal Data” by Romet Saaliste was written back in 2018 [12]. While the analytical goal of this work was to overview how GDPR relates to the Estonian jurisdictional framework, the practical part of this thesis resulted into developing an OSINT tool for extracting publicly available personal data from several Estonian government registers and combining into one combined data set, potentially leading to a wide scale data leakage. The developed tool was a showcase of how automated queries can be utilized in the scope of an offensive OSINT techniques, and therefore it has showed that existing at that time safeguards needed to be reviewed and more efficient protections needed to be established for data protection against intelligence collection. Although the general goal of the current paper is different from Romet’s work, the idea of demonstrating the possibilities of offensive OSINT techniques for increasing security awareness is employed in both works as in the materials developed in the current thesis, training participants will be taught OSINT skills in order to understand their essence and to be able to protect oneself efficiently and consciously.

Another Tallinn University of Technology graduate in 2019 studied gamification of OSINT and reverse engineering exercises and suggested such as a teaching method in the above-mentioned university [11]. Results showed an increase in students' extrinsic motivation for OSINT and reverse engineering topics. This work by Saber Yari was found as a highly relatable to the present work, since it was aiming to create educational materials for teaching OSINT skills and techniques in-depth, what implies raising awareness about OSINT methods as well. However, the problem statement of Saber's work remains different as well as exact methods and tools chosen for developing gamified learning materials.

Last but not least is the work by Siim Kurvits written in 2021. The "Social Media Scraping for Cybersecurity: Performing Open-Source Intelligence with Twitter" offers a possible solution for extracting social media data for its later utilization in cyber threat intelligence creation [14]. In contrast the two above mentioned theses, this work is focusing on the defensive use of the created OSINT tool. Therefore, this work is found the least inter-related with the presented thesis, although Siim's research has brough a distinctive contribution into OSINT development as well as into widening the background of open-source intelligence topic in general.

2.3 Existing ISA Solutions

An analysis or existing ISA program solutions for organizations is essential for an exhaustive state of art review and for creation of an effective and relevant training materials. For this purpose, an overview of reputable security awareness program providers will be reviewed, as well as individual OSINT certifications available online on fee basis.

Infosec IQ, one of the world leaders in providing ISA software, training, bootcamps and similar, has named “Top 10 security awareness training topics for your employees” [1]. Those include: email scams, malware, password security, removable media, safe internet habits, social networking dangers, physical security and environmental controls, clean desk policy, data management and privacy, BYOD policy. From all mentioned above it is worth elaborating on the following:

Safe internet habits: recognizing suspicious and spoofed domains, identifying an insecure connection, suspicious software on the internet, the risks of entering credentials into untrusted websites.

Social networking dangers: recognizing phishing attacks over social media and minding information contents before publishing it as a preventative measure from data collection and crafting of spear phishing emails.

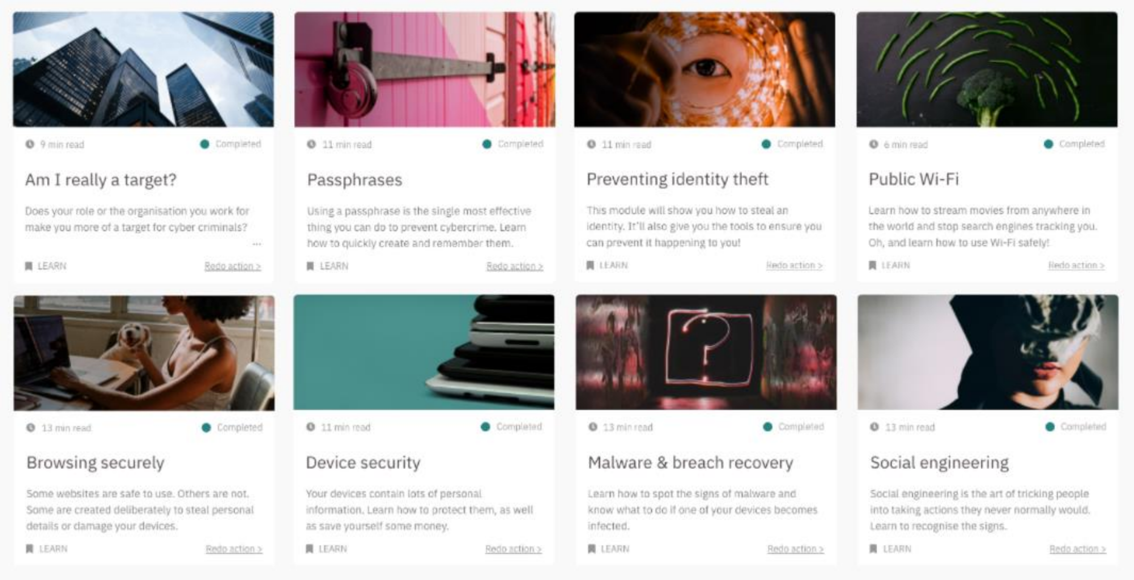
Data management and privacy: information classification and secure usage guidelines according to information class as well as appropriate protection methods for handling and/or storing each information type.

Pout of all mentioned Social Networking Dangers is the most relevant to the current work. However, OSINT goes far behind the scope of just social media, although social media plays a large role in intelligence collection. This means, that neither under this topic nor under any other from the list, OSINT could be covered comprehensively.

Looking at another reputable ISA provider CybSafe and the scope of their training materials[2], the same can be concluded: OSINT is not covered in-depth. Although, a wide variety of topics is represented among the modules, each individual topic’s approximate read duration is 6-13 minutes, which is not enough for learning it on an advanced level (see Figure 1. for the examples of modules and their duration).

[1] https://resources.infosecinstitute.com/topic/top-10-security-awareness-training-topics-for-your-employees/

[2] https://helpcentre.cybsafe.com/en/articles/5161632-cybsafe-content



9 min read · Completed

Am I really a target?

Does your role or the organisation you work for make you more of a target for cyber criminals? ...

LEARN · Redo action >

11 min read · Completed

Passphrases

Using a passphrase is the single most effective thing you can do to prevent cybercrime. Learn how to quickly create and remember them.

LEARN · Redo action >

11 min read · Completed

Preventing identity theft

This module will show you how to steal an identity. It'll also give you the tools to ensure you can prevent it happening to you!

LEARN · Redo action >

6 min read · Completed

Public Wi-Fi

Learn how to stream movies from anywhere in the world and stop search engines tracking you. Oh, and learn how to use Wi-Fi safely!

LEARN · Redo action >

13 min read · Completed

Browsing securely

Some websites are safe to use. Others are not. Some are created deliberately to steal personal details or damage your devices.

LEARN · Redo action >

11 min read · Completed

Device security

Your devices contain lots of personal information. Learn how to protect them, as well as save yourself some money.

LEARN · Redo action >

13 min read · Completed

Malware & breach recovery

Learn how to spot the signs of malware and know what to do if one of your devices becomes infected.

LEARN · Redo action >

13 min read · Completed

Social engineering

Social engineering is the art of tricking people into taking actions they never normally would. Learn to recognise the signs.

LEARN · Redo action >

Figure 1. CybSafe training style modules, their description and duration

Another known company providing ISA materials for companies is Infosequre. They not only provide gamified trainings, VR experience, cybersecurity culture scans and basic security awareness materials, but also, they have a separate block of advanced e-learning materials. The topics which “dive right into the core of the issue” include[1]: phishing, social engineering, mobile devices, cyber security, working in the cloud, information classification, malware, risk management, physical security, GDPR.

The approach taken by Infosequre for structuring training materials is found very relevant for the current work, since Infosequre is providing both introduction program and separate in-depth e-courses, which can be taken on top of the basic knowledge. Hence a known ISA provider has already implemented such structuring of information security awareness program for employees, it can be concluded that current thesis’ chosen method is justified and relevant. However, none of the in-depth modules introduced by Infosequre are covering OSINT, therefore the present work remains novel and actual.

[1] https://www.infosequre.com/security-awareness-elearning

3 Methodology

First, for solving the problem of the lack of training materials on OSINT topic it was chosen to develop and introduce such training. This will allow to test whether introduction of OSINT training would improve the ISA situation in the organization and prove or refute the relevance of the problem stated by the author of this paper.

Training will be developed in a form of a self-paced e-course, which will take place fully online and will not require any participation of a teacher or collaboration with other employees. It will be possible to pause and revisit the training any time, the training will be available on the company's learning system.

The name of the exact tool used for developing the e-course cannot be revealed, since information about tools and systems used by the organization is considered to be confidential and cannot be revealed.

The choice of an e-course format and corresponding development tool is motivated by the following:

- employees of the Company X are already familiar with the e-course format, therefore no additional education or introduction into the training structure will be required, what implies saved time, more participants, and hence higher trustworthiness of the results.

- the e-course development platform utilized in the Company X allows exporting created trainings in various e-learning compatible formats as well as in web and PDF. This makes created work reusable and upgradable in the future research, what is also an essential trait of an e-learning according to Terry Anderson, "The Theory and Practice of Online Learning" [15].

The flow for defining training scope, developing its plan, or syllabus, and translating it into the e-course is represented in the Figure 2.

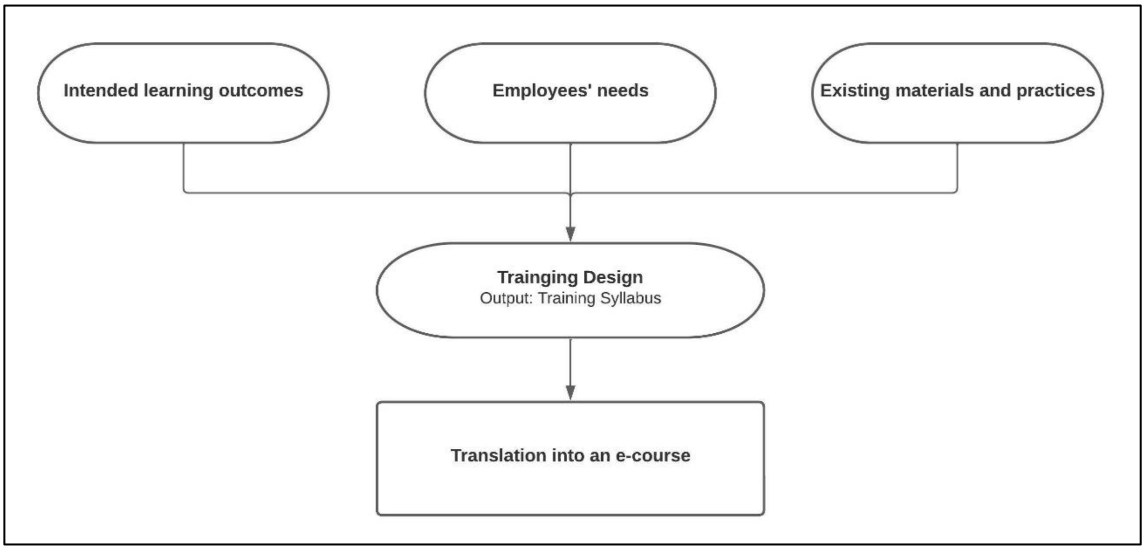

Intended learning outcomes
Employees' needs
Existing materials and practices
Trainging Design
Output: Training Syllabus
Translation into an e-course

Figure 2. Methodology for training syllabus and its translation

The methodology or reason behind each element:

Intended learning outcomes. According to Terry Anderson [13], all learning systems shall be based on the following two points: the needs of the intended students, and the intended learning outcomes of the course.

Employees' needs. As mentioned in previous point, must be considered for defining scope according to Anderson [13].

According to ENISA, quantitative measurement of cybersecurity provides background on the cybersecurity thinking and behavioural patterns of people. This gives important guidance for awareness raising activities. Public surveys and statistics can provide useful and necessary insights for planning more targeted and effective awareness raising activities facilitating successful outcomes [6]. For this reason, a survey was conducted to understand employees' needs.

The platform for running a questionnaire is MS Forms. For ensuring transparent data collection, a privacy notice will be shared along with the questionnaire. Both the list of questions and the privacy notice can be found in the Appendix section and Appendix 1 and Appendix 2 respectively.

Existing materials' analysis. Analytical and exploratory research of existing recourses for OSINT educational materials to understand their target students, and scope.

Training syllabus and its sequencing: syllabus to be compiled as an outcome of three above mentioned points. The sequencing methodology based on chapter 4 from "E-learning methodologies and good practices" by FAO e-learning Academy [5].

Syllabus translation into materials. After training syllabus is done, it is needed to be translated into practical e-learning materials. This will be done based on Chapter 7 from above mentioned FAO's practices [14]. It provides guidance on applying various instructional techniques to create engaging, clear, and effective e-learning content. Methodology describes how to choose an appropriate presentation technique (diagrams, pictures, storytelling, flows, etc.) for different types of knowledge (facts, concepts, attitudes, etc.).

Other aspects to consider. While developing solution, it is important to know a difference between education and training [16]. As mentioned by several articles[1], at-work trainings are usually skill oriented, narrow focused, short, depend on educational knowledge, and are intended to improve performance and productivity. Whereas education is aimed to deliver knowledge about facts, values, beliefs, general concepts, principles, etc. to the students. Education is intended to develop intellect: a sense of reasoning, understanding and judgment[2]. In the case of the current work, developed materials will mostly have traits of an educational materials, however applied in the context of a typical workplace training. Because the goal of this thesis is not only developing employees' OSINT specific skills, created e-learning materials can be considered as a hybrid of educational and workplace course. It is aimed that employees understand the essence of OSINT, and how it can be used for businesses' needs as well as against individuals and organizations. In general, employees are intended to develop awareness about OSINT security related topics through realizing the existing threats and understanding some offensive techniques.

[1] https://coredifferences.com/difference-between-training-and-education/

[2] https://keydifferences.com/difference-between-training-and-education.html#:~:text=Training%20refers%20to%20an%20act,a%20typical%20system%20of%20learning.

As an outcome, it is expected that developed materials show positive effect on ISA in the chosen company. The effect will be evaluated based on pre- and post- training feedback.

It is also expected that the developed e-learning becomes a part of ISA framework in a target company and gets implemented on a regular basis.

4 Solution

As described in Chapter 3, the solution part will go through the training development flow. First, intended outcomes of the training will be defined by the author, then employee needs will be determined, and finally existing OSINT educational materials studied. After what, these three aspects will be combined into a plan, which later will be translated into e-course.

4.1 Intended outcomes

On a higher level, it is intended that employees develop understanding of the following aspects:

1. OSINT basic concepts, terms, and definitions
2. OSINT related historical events and abuse cases
3. OSINT skills
4. OSINT community

4.1.1 OSINT Basic Concepts, Terms and Definitions

It is intended that after training completion, trainees understand and can explain the following:

- what is OSINT, and basic underlying definitions such as: intelligence, open source

  basic concept of sock puppets or fake accounts and what role they play in privacy

- how the Internet and the Web work, how is information being stored and located on the Internet, as well as a general understanding of what is IoT, and what role it plays in security

- how is OSINT used by organizations and by hackers (sock puppets and fake identity)

4.1.2 OSINT Related Historical Events and Abuse Cases

It is intended that after completing the training, employees are familiar with the historical events described in chapter 2.1. Employees shall understand the ethical and social problems caused by these events.

4.1.3 OSINT Skills

In the scope of this work, it is assumed that trainees do not have to master the skills, but rather they must be aware of them. Such approach is taken for avoiding an encouragement to use OSINT in malicious way, and rather make trainees skilled to recognise such misuses.

For determining the list of essential skills needed for a successful online research and creation of intelligence from open sources, the Toddington International Inc. Online Investigator’s Checklist [17] was analyzed, summarized, and trimmed to include basic skills only. Therefore, the list of practical skills is the following:

- Choose an effective search tool and use extended search capabilities such as Google search techniques or Google Dorking, and web archives such as Wayback Machine[1].

- Review social media platforms such for intelligence collection as well as with the use of special tools like Social Seacrher[2]. Search names, usernames, account

[1] https://archive.org/

[2] https://www.social-searcher.com/

names, email, phone numbers, addresses, family members, friends, associates, including breached data with the help of tools like HaveIbeedPwned[1].

- Get metadata from files.

Besides online research and intelligence collection skills, it is also expected that trainees acquire skills necessary for protection own privacy online. The list of such skills will be based two sources [19][19] and will include the main takeaways that can be easily implemented in everyday personal and workplace life, that means including:

- Cleaning files' metadata
- Privacy Settings
- Managing unfamiliar connection/friend requests
- Managing likes
- Managing tagged photos

Besides the above-mentioned methods for enhancing security online, trainees will be "hack" themselves, meaning they will be encouraged to use the offensive skills for looking up own profiles, in particular, for researching what kind of information is publicly available on them. This will allow trainees to recalibrate and control own online profiles in a more secure way.

4.1.4 OSINT Community and Further Materials

As previous studies show, repeated, mandatory exposure to security and privacy news increases knowledge [20]. Also, knowledge has a greater impact on information protective behaviour than motivation [20]. For these reasons, it is intended that after training completion, employees continue acquiring knowledge about the topic through receiving news on OSINT topics through online communities and get a list of related materials. It is also done with an intention of showing how wide the topic of OSINT and security in general is.

[1] https://haveibeenpwned.com/

The trainees will be provided with:

- Articles on related topics
- Websites wholly devoted to OSINT
- Books about OSINT basics and OSINT skills
- Online communities on Reddit and Twitter

4.2 Employees' Needs

Employees' needs of the Company X were analysed based on the preliminary questionnaire, which was conveyed before launching the training.

In the survey employees were asked to go through several statements and evaluate how much they related to each one on a Likert scale (from Strongly Disagree to Strongly Agree). Two more questions were aiming to evaluate the rating of statement from to ten. Additionally, participants were asked to provide information about what department they are from and for how long have they been employed.

The questionary was fully anonymous, and participants were provided a privacy notice.

According to the results of the survey, 11.9% of respondents couldn't agree that they have been sufficiently trained on information security topics at the Company X. 7.1% out of that, showed strong disagreement with the following statement: "I feel I have been sufficiently trained in information security related topics at our company". Along with that 7.1% respondents indicated they somewhat disagree they feel motivated to follow security related practices learned at work in their personal and professional life. Another 11.9% of respondents showed they somewhat disagree they could recognize a security issue or incident if saw one, and additional 14.3% felt neutral about that, which in total gives 26.2% of those, who don't feel knowledgeable about security enough to recognise a potential threat. 47.6% of respondents agreed strongly on that their employer, Company X, is taking care of information security. 4.8% stated they somewhat disagree on that, and 2.4% strongly disagree, leaving 14.3% neutral about that. Finally, majority of respondents (69%) showed a strong interest towards increasing personal security related awareness and learning new skills.

Along with that, on average, employees participated in the survey rated the importance of their individual impact on the company's level of information security as 8.71 out of 10. This shows that people at the Company X realise that the overall security of the organization is up to them, or in other words that they are an important part of the security safety at the company.

After summarising the findings from the conveyed survey, it is possible to make a conclusion, that employees of the Company X need additional information security awareness training, because they feel insufficiently trained, and feel unconfident about recognizing threats. They also do not feel very motivated to implement learned skills in their life, what indicates a need for such motivation or reasons. However, the prime indicator for a need of training is employees’ strong interest towards information security and acquiring related skills. The survey has shown that employees understand their importance in ensuring the security of the company, however they don’t know how (low confidence in ability to recognize threat and high desire for learning new skills). Above mentioned concludes that employees of the Company X are in need for a continuous engaging training as a part of company’s ISA. Continuity of the training will allow constant development and confidence, and engagement would motivate to implement the learned skills.

The above analysis is very important not only for understanding of employees needs but also for being aware of general situation in the Company X. Tracking the overall satisfaction of employees about the ISA framework can help improving the successfulness of this framework over time. When the practical part of the current work is closed, results before and after training completion will be compared.

Statements in the feedback form will allow assessing whether after training completion:

- employees feel more satisfied with the security awareness program in their organization
- employees feel more motivated to implement information security-related knowledge both at work and in personal life
- employees’ interest in information security-related topics has increased

- employees’ trust towards security in the organization has increased
- employees’ awareness about the number of security threats has increased

4.3 Existing OSINT Materials

On the market of OSINT specialized certifications, the “SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis” by the SANS Institute[1] is the one which stands out, since SANS Institute is one of the most trusted and largest providers of cyber security trainings and certifications to both government and commercial institutions world-wide. According to the training description, the participants will go through 5 modules:

1. Foundations of OSINT
   This module consists of basic definitions of OSINT and theory behind it, such as understanding of OSINT process, anonymous environment, sock puppets and data analysis foundations.
2. Core OSINT Skills
   In this part students go through leveraging advanced searching engine techniques and harvesting web data, file metadata analysis and advanced image/map analysis.
3. People Investigations
   In this module students start with data about people, such as email addresses and usernames, and proceed with search and extraction techniques within different social media platforms.
4. Website, Domain, and IP Investigations
   This module is devoted to computer-focused sources of OSINT data. Website investigations, WHOIS, DNS, IP Addresses, IT Infrastructure, and wireless OSINT are the topics of this module.
5. Business and Dark Web OSINT
   This part reveals how to use dark web for research, including research about organizations.

[1] https://www.sans.org/cyber-security-courses/open-source-intelligence-gathering/

The finishing module (6^{th}) includes capture the flag activities to bring hands-on experience to students. The structure of these materials can be taken as a framework for creating further materials, since SEC487 covers both theoretical and practical aspects, from both offensive and defensive sides.

SEC487 is stated as helpful for a broad spectrum of cybersecurity professionals, including security awareness staff. This drives to a conclusion that OSINT is considered a topic for security awareness by SANS Institute as well.

4.4 Theoretical Basis of the Solution

Many theoretical research works on ISA are based on psychological and behavioural theories. M.E. Thomson and R. von Solms studied the application of social psychology for educating users and/or employees successfully [13]. In particular they developed a system for influencing individuals’ attitude through persuasion. Qing et al. has developed a framework for evaluating the effectiveness of persuasive communications, which after application showed that persuasive communication in a form of messages is showing positive results [14]. These and similar research show that attitude can be successfully changed through persuasion. However, author of the present thesis is aiming to achieve not only change in attitude but also increase intrinsic motivation towards information security. Therefore, Siponen’s set of practical principles will be chosen as a basis for developed materials [22]. His set of practical approaches are developed with respect to motivation, including logic, emotions, morals and ethics, well-being, feeling of security and rationality. Intrinsic motivation, theory of reasoned action (TRA), theory of planned behaviour (TPB), and the technology acceptance model (TAM) are the conceptual basis for security awareness according to Siponen.

Summarizing Siponen’s work, the following points can be distinguished for developing a successful ISA framework:

- the consequences of executing security guidelines must be desirable
- people's perception of the ease of performing the behaviour of interest is best taken care of by technical education, meaning raising skills

- to form intrinsic motivation, people have to feel free to make their own choices concerning their behavior, i.e., internal aspirations and external forces (such as security requirements) should reflect one's feeling of freedom

- to form intrinsic motivation, people have to feel excitement and challenge

- the knowledge should be "sold" to the people by providing an exhaustive explanation why the knowledge is important, this will increase motivation

- Successful organizational awareness or education requires more actions than merely the giving of a set of rules

As Anderson describes how the developed flow shall be used for creating the content. Ideally, the learning outcomes are translated into the course content and appropriate strategies for the learning process that will allow students to achieve those earlier defined outcomes. Then the development team (thesis author) is responsible for translating the theory and intentions into practice in the form of a courseware, stored on a Content Management System, and online learning functions, which are delivered by the Learning Management System (LMS), which is interfaced with the library and other digital resources, related services, and the student information system via a secure server that can authenticate the student login. Since the interface and digital parts and other services like secure server and authentication are already provided by the company, the author will take care only of developing the flow and translating it into the courseware (see Picture below, where X'es represent each point of a syllabus and Y'es represent the corresponding materials translated into e-course chapter).

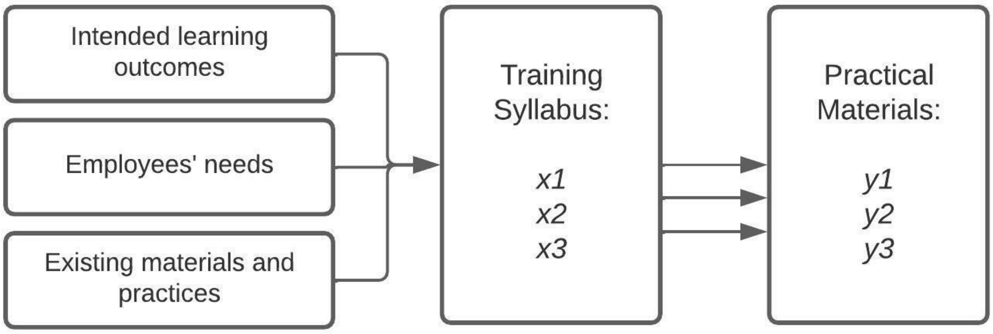


Figure 3. Syllabus translation into e-course flow

For ensuring the effectiveness of the developed e-course, it was evaluated based on software and didactical indicators for evaluating the effectiveness of e-learning described by Elvis Pontes in “Methodologies, Tools and New Developments for E-Learning” [16]. The developed solution was found to be compliant with both software and didactical indicators, what concludes that the designed solution is effective from software and didactical point of view.

4.5 Training Design

The training design chapter will describe the last two steps described in the methodology (Figure 2), which are Training Syllabus and Sequencing and Translating Syllabus into Materials.

The e-course syllabus was based on intended outcomes, employees’ needs, and existing materials as described in above chapters 4.1, 4.2 and 4.3. After the whole list was compiled, it was structured based on the sequencing methodology described in chapter 4 of “E-learning methodologies and good practices” by FAO e-learning Academy [14]. This method uses a learning objectives hierarchy, meaning that first those skills should be taught that seem to be prerequisites for all other skills. The complete and sequenced list of chapters included into the e-course along with the learning objectives and resources can be found as Appendix 5.

Following the structured syllabus, prepared materials were translated into practical e-course based on instructional techniques described in chapter 7 of the above-mentioned FAO’s best practices [14].

The created e-course was uploaded on the Company X e-learning system, where was available for all employees. It was also advertised internally.

Besides Company X e-learning system, the developed e-course is available for a review under the following address: shorturl.at/otzB4

4.6 Collecting Post-Training Feedback

The second round of feedback was collected after the training completion and was done in the same manner as first round of feedback. The same questionnaire with only two new additional questions was incorporated into the “Further Materials” Chapter of the training. The additional questions are aiming to assess the popularity of the developed e-learning materials and get detailed feedback (optional). Additional questions are the following:

- What did you like about the training?
- On a scale from 1 to 10, how likely would you recommend this training to your colleagues and/or friends?

42 employees of the Company X took the e-course and participated in the feedback.

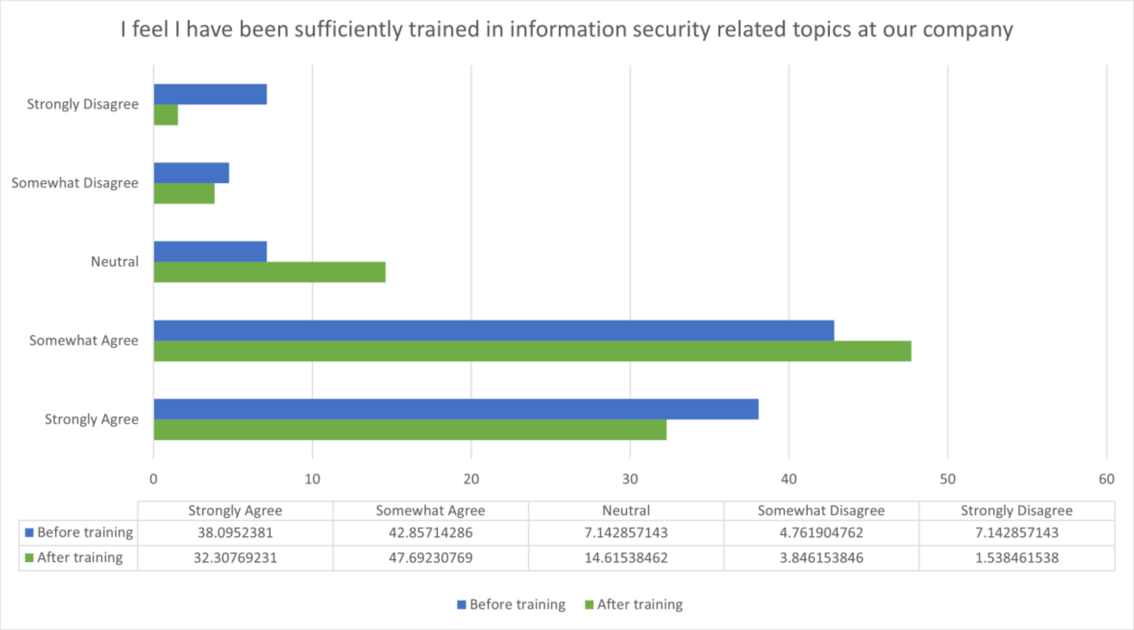
5 Results

This chapter will bring an overview of results achieved by the developed e-course in a form of comparison of the first and second rounds of feedback. Based on notes taken during the process of development, the further improvements and prospects for work are also described in this chapter.

5.1 Feedback Analysis and Comparison

The comparison of pre-training and post-training questionnaire results shows a great improvement of the chosen indicators. Below you can see a comparison of every parameter, where graphs in blue represent situation before taking the training and graphs in green represent the situation after taking the training.

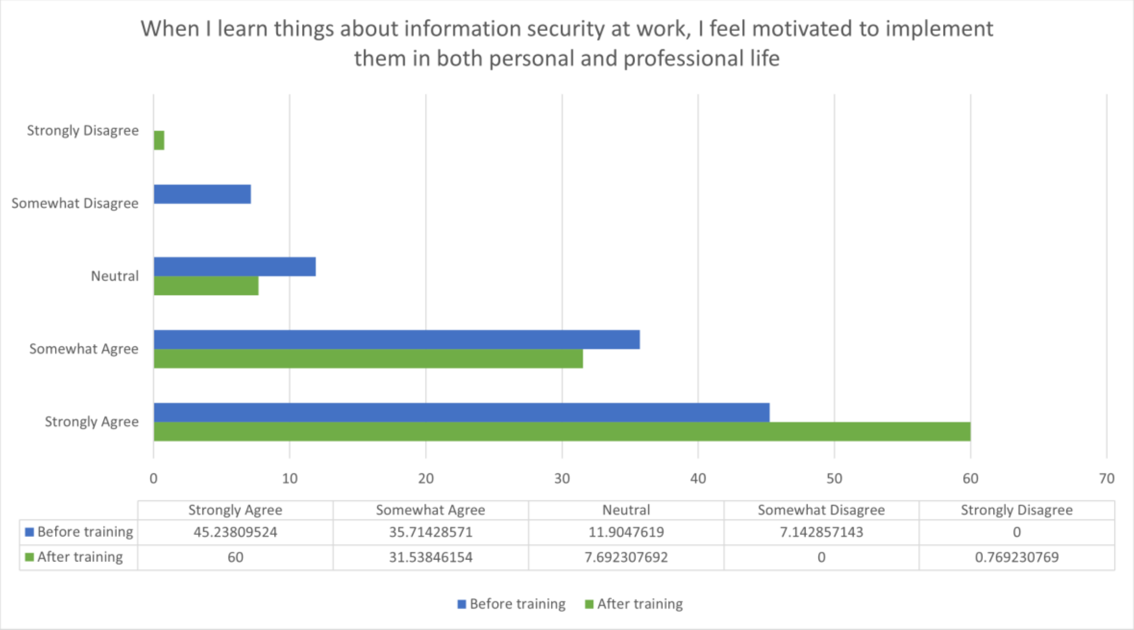
You can see the question itself on top of the figure, all numbers represent the percentage from total number of surveyed people. Figures 4-8 display the numbers in detail.



	Strongly Agree	Somewhat Agree	Neutral	Somewhat Disagree	Strongly Disagree
🟦 Before training	38.0952381	42.85714286	7.142857143	4.761904762	7.142857143
🟩 After training	32.30769231	47.69230769	14.61538462	3.846153846	1.538461538

Figure 4. Feedback comparison: first question

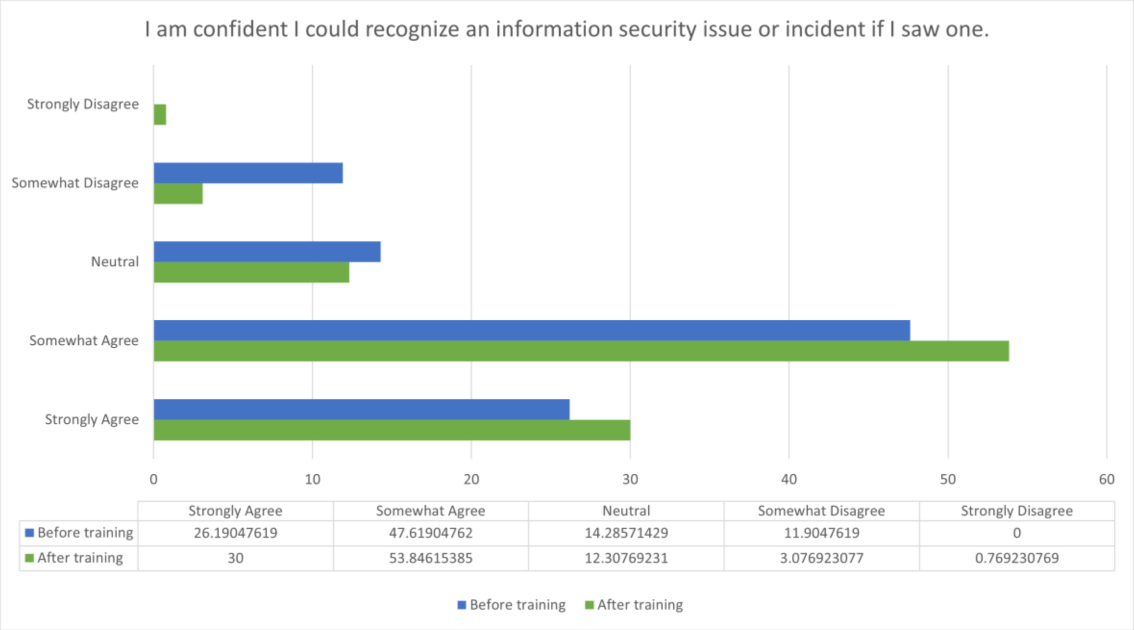
As follows from the Figure 4, after taking the training employees feel more satisfied with the security awareness program in their company. Before the training 7.1% of respondents expressed strong disagreement with the following statement: “I feel I have been sufficiently trained in information security related topics at our company”, whereas after the training just 1.5% of respondents have shown strong disagreement and only 3.8% expressed that they somewhat disagree with the above statement. Although, the total agreement rate (somewhat agree with strongly agree combined) stayed the same – around 80%. More people moved to Neutral position, which has grown from 7% to 14%.



	Strongly Agree	Somewhat Agree	Neutral	Somewhat Disagree	Strongly Disagree
🟦 Before training	45.23809524	35.71428571	11.9047619	7.142857143	0
🟩 After training	60	31.53846154	7.692307692	0	0.769230769

Figure 5. Feedback comparison: second question

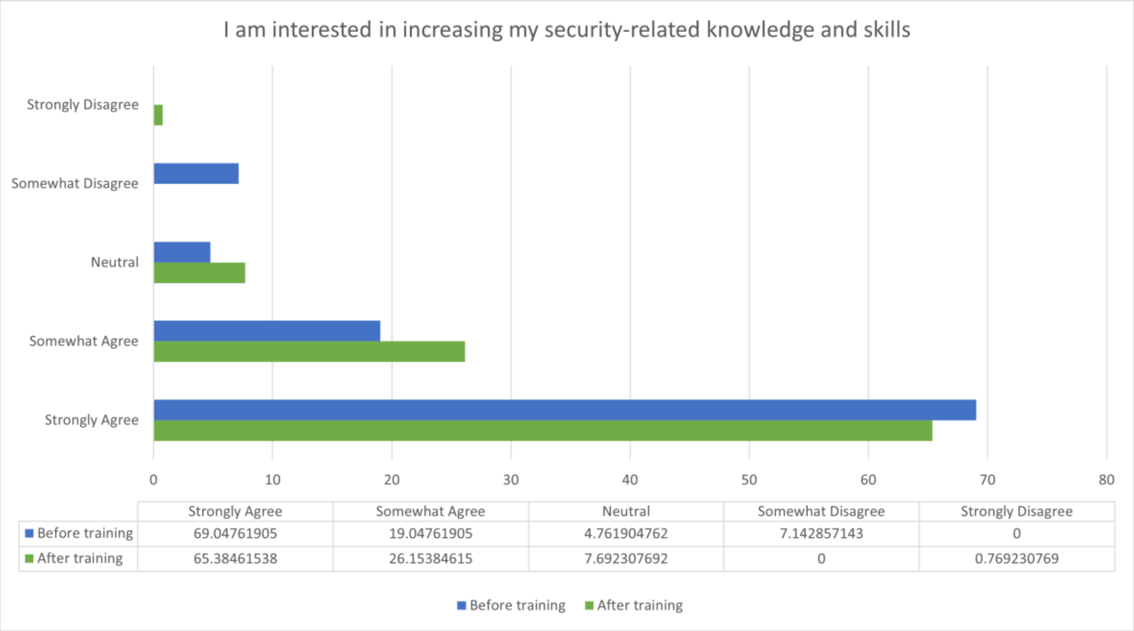
Figure 5 shows that those who completed the e-course feel more motivated to implement information security-related knowledge both at work and in personal life. The rate of those who strongly agree with the related statement has grown almost 15% reaching 60% of total answers. Additionally, the number of respondents who would disagree with such statement is less that 0% in total (combining somewhat disagree and strongly disagree), whereas before training 7% of participants disagreed. 3% less employees felt neutral about it.



	Strongly Agree	Somewhat Agree	Neutral	Somewhat Disagree	Strongly Disagree
■ Before training	26.19047619	47.61904762	14.28571429	11.9047619	0
■ After training	30	53.84615385	12.30769231	3.076923077	0.769230769

Figure 6. Feedback comparison: third question

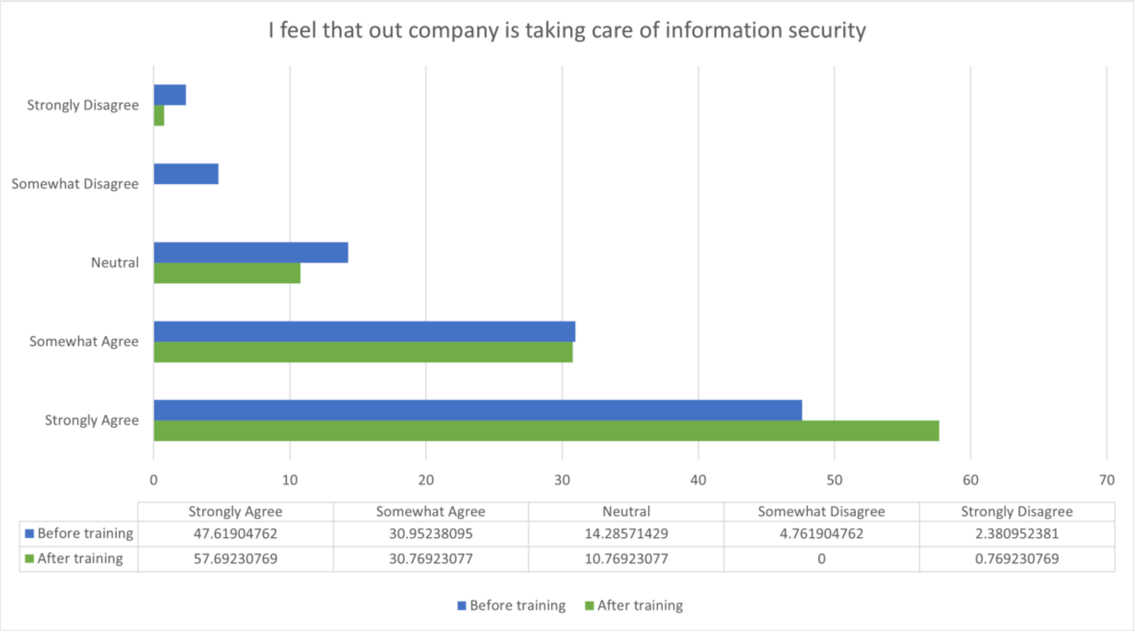
Judging by Figure 6 it is possible to conclude that those who have taken the e-course feel more confident they could recognize an information security incident if they saw one. The disagreement with the corresponding statement dropped by almost 9% from 11.9% to only 3%. And the overall agreement raised around 10% reaching 83.8 (somewhat agree and strongly agree combined).



	Strongly Agree	Somewhat Agree	Neutral	Somewhat Disagree	Strongly Disagree
🟦 Before training	69.04761905	19.04761905	4.761904762	7.142857143	0
🟩 After training	65.38461538	26.15384615	7.692307692	0	0.769230769

Figure 7. Feedback comparison: fourth question

In Figure 7 it is visible that employees feel approximately the same about increasing own security-related knowledge. The most noticeable change is the drop almost to 0% of those who disagreed with the statement: “I am interested in increasing my security-related knowledge and skills”. This shows that employees’ interest was already high before the training, and that their interest was maintained and slightly raised afterwards, which is a positive trend, and an indicator of maintained motivation to learn security skills, which can also mean that developed materials were interesting and actual enough that learning them didn’t feel like burden of obligatory training.



	Strongly Agree	Somewhat Agree	Neutral	Somewhat Disagree	Strongly Disagree
🟦 Before training	47.61904762	30.95238095	14.28571429	4.761904762	2.380952381
🟩 After training	57.69230769	30.76923077	10.76923077	0	0.769230769

Figure 8. Results comparison: fifth question

Lastly, the Figure 8 shows that the trust towards security in the organization has increased for those who have taken the e-course. 88.6% of second round feedback respondents somewhat or totally agree with the statement “I feel that our company is taking care of information security”, and other 10.7% feel neutral, whereas before training 2.3% disagreed totally and 4.7% somewhat disagreed.

Employees have also provided positive feedback about the training, saying it has great examples, was useful, practical, understandable, and introducing new interesting topics. On a scale from one to ten, employees would recommend this e-course to their colleagues or friends with the likelihood 9.25. More detailed statistics about the rating can be seen in the Figure 5.

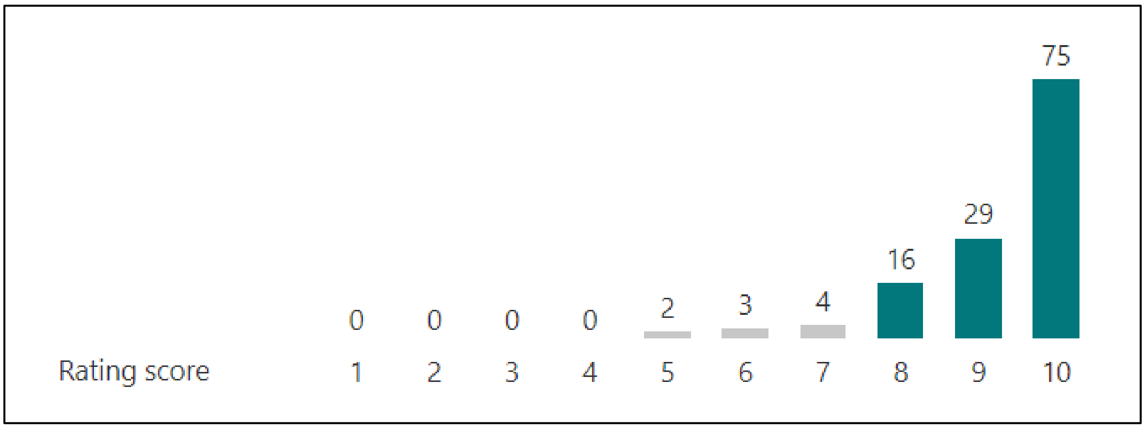


Figure 9. Likelihood of recommending the course to others

Based on all the observations above made during the analysis and comparison of first and second round feedback, it is possible to make a few conclusions:

1. **Employees needs were met.** They feel more like sufficiently trained and feel more confident about recognizing threats. They also feel more motivated to implement learned skills in their life. As the prime indicator for a need of a training was employees’ strong interest towards information security and acquiring related skills, it is also important that this indicator has raised even more, meaning that **employees have formed an intrinsic motivation for improving own information security awareness**.

2. **Addition of OSINT related training materials has a potential for enhancing company’s ISA framework.** Developed e-course has shown to positively affect security awareness level among the employees who have taken the e-course in the Company X.

5.2 Future Work

The present paper has a potential for further development. This chapter will describe some of the points which can potentially be added to this work in the future.

Customisation. Based on the collected results some divisions of the Company X have showed more interest and involvement in the developed e-course than the others, therefore further materials should aim to achieve balanced participation ratio between all the departments. One of the strategies for this might be making the course customized based on the division’s sphere of duties and responsibilities. For example, Human Resource employees might get more detailed training about metadata in files shared externally and about posting job offers without revealing sensitive information about company’s structure. Meanwhile the amount of technical details in their training can be reduced. Employees with managerial positions can be taught more about targeted, spear-phishing attacks based on the information they have available online.

Facilitation. The future work can implement facilitation features into the training. Some asynchronous (e-mail-based) or synchronous (audio and video) tools can be introduced for collaboration. For example, additional live sessions can be prepared for training specific skills along with the facilitation manager.

Knowledge check. However, while the developed e-course has some knowledge-testing features, they are not sufficient for making objective judgements about learning progress and success of employees. Further work could include developing or adding testing blocks to the training materials, which would allow to evaluate how well trainees have understood the materials and whether they have grasped the practical skills as well.

Customisability for other organisations. The e-course developed in this training was delivered based on inputs of a specific company, although the developed materials can be called universal in terms of knowledge presented. Further work could address and describe, what exact steps need to be taken in case such approach is implemented in another organisation. In other words, further research shall provide clear instructions on applying the e-course for any organisation that wishes to do so, with defined by that organisation inputs and expected by it results.

6 Conclusion

The intention of this thesis was to close the gaps in modern employee security awareness programs by introducing advanced e-course about OSINT. Theoretical part of this paper consists of literature and historical background analysis. Whereas practical contribution is represented by developed e-learning materials, successfully tested on a real Baltic organization.

Analytical part has shown that existing employee security awareness programs do not cover advanced open-source intelligence topics, however there is a variety of personalized online materials available on the Internet. These materials are mostly online courses or self-paced e-courses, sold and advertised by reputable companies or individuals.

Studied examples from history are forcing us to look towards the inclusion of socio-technical aspects such as OSINT into the employee information security awareness programs. Based on the overviewed cases, for the past two decades information and communication technologies have been developing in such a rapid pace that society, what implies any organization, is becoming coherent with them and can no longer be considered separate. This forces us to change our view on such topics as IT risks and cyber incidents and think of them as of not only technological phenomena but also social.

As a practical contribution, an advanced e-course about OSINT was designed aiming to close the identified gaps. Developed solution was released and tested in the Company X. 442 employees have successfully completed the training and 130 have provided feedback on it. Based on quantitative and qualitative analysis of feedback received, the designed solution is showing positive results in enhancing security awareness program and raising overall level of security awareness in organisation as well as raising employees' personal interest and intrinsic motivation towards information security. Such results justify the methods and tools chosen for solving the problem, and the supposed gap can be considered as correctly identified and closed.

References

[1] "Cost of a Data Breach Report 2021 | IBM." https://www.ibm.com/security/data-breach (accessed Feb. 17, 2022).

[2] "The Psychology of Human Error," *Tessian*. https://www.tessian.com/research/the-psychology-of-human-error/ (accessed Feb. 26, 2022).

[3] "2021 DBIR Master's Guide," *Verizon Business*. https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/ (accessed Feb. 23, 2022).

[4] P. Tasevski, "Methodological approach to security awareness program," *undefined*, 2015, Accessed: Feb. 15, 2022. [Online]. Available: https://www.semanticscholar.org/paper/Methodological-approach-to-security-awareness-Tasevski/42de90ad29425bcffd7e6dd6f5b535a75d6887ee

[5] FAO, *E-learning methodologies and good practices: A guide for designing and delivering e-learning solutions from the FAO elearning Academy, second edition*. Rome, Italy: FAO, 2021. doi: 10.4060/i2516e.

[6] "Raising Awareness of Cybersecurity," *ENISA*. https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity (accessed Feb. 15, 2022).

[7] PCI Security Standards Council, "Information Supplement: Best Practices for Implementing a Security Awareness Program." PCI Data Security Standard (PCI DSS), Oct. 2014. [Online]. Available: https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf

[8] "What is Intelligence?" https://www.dni.gov/index.php/what-we-do/what-is-intelligence (accessed Feb. 20, 2022).

[9] "Open Source Intelligence in the Twenty-First Century," 2014, Accessed: Feb. 20, 2022. [Online]. Available: https://www.academia.edu/5489296/Open_Source_Intelligence_in_the_Twenty_First_Century_New_Approaches_and_Opportunities

[10] H. Bean, "Is open source intelligence an ethical issue?," *Res. Soc. Probl. Public Policy*, vol. 19, pp. 385–402, Jan. 2011, doi: 10.1108/S0196-1152(2011)0000019024.

[11] J. Hinds, E. J. Williams, and A. N. Joinson, "'It wouldn't happen to me': Privacy concerns and perspectives following the Cambridge Analytica scandal," *Int. J. Hum.-Comput. Stud.*, vol. 143, p. 102498, Nov. 2020, doi: 10.1016/j.ijhcs.2020.102498.

[12] R. Saaliste and O. M. Maennel, "Isikuandmete kaitsega seotud Eesti avaliku sektori väljakutsed," May 2018, Accessed: Feb. 27, 2022. [Online]. Available: https://digikogu.taltech.ee/en/Item/ddb3b9f4-c06a-43b4-b064-0a26e0d6c635

[13] S. Yari and S. Mäses, "OSINT ja pöördprojekteerimise harjutuste loomine," May 2019, Accessed: Feb. 17, 2022. [Online]. Available: https://digikogu.taltech.ee/en/Item/e4a7d91e-bb4c-4228-b32b-231b50e6837b

[14] A. Juhasoo-Lawrence, K. Kikkas, and S. Kurvits, “Sotsiaalmeedia kaapimine küberturvalisuse eesmärkidel: andmekogumine avalikest allikatest Twitteri näitel,” Jun. 2021, Accessed: Feb. 17, 2022. [Online]. Available: https://digikogu.taltech.ee/en/Item/f7768473-efad-4598-9ef6-b17dfc526294

[15] “The Theory and Practice of Online Learning - Athabasca University Press | Athabasca University Press.” https://www.aupress.ca/books/120146-the-theory-and-practice-of-online-learning/ (accessed Mar. 13, 2022).

[16] “Methodologies, Tools and New Developments for E-Learning,” p. 444.

[17] “TII_Online-Investigators-Checklist_v2-1.pdf.” Accessed: Feb. 22, 2022. [Online]. Available: https://1x7meb3bmahktmrx39tuiync-wpengine.netdna-ssl.com/wp-content/uploads/TII_Online-Investigators-Checklist_v2-1.pdf

[18] A. Quan-Haase and D. Ho, “Online privacy concerns and privacy protection strategies among older adults in East York, Canada,” *J. Assoc. Inf. Sci. Technol.*, vol. 71, May 2020, doi: 10.1002/asi.24364.

[19] M. Bazzell, *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information*, 5th ed. North Charleston, SC, USA: CreateSpace Independent Publishing Platform, 2016.

[20] F. Bélanger, J. Maier, and M. Maier, “A longitudinal study on improving employee information protective knowledge and behaviors,” *Comput. Secur.*, vol. 116, p. 102641, May 2022, doi: 10.1016/j.cose.2022.102641.

[21] T. Qing, B.-Y. Ng, and A. Kankanhalli, “Individual’s Response to Security Messages: A Decision-Making Perspective,” 2007, pp. 177–191. doi: 10.1007/978-0-387-48137-1_10.

[22] M. Siponen, “A conceptual foundation for organizational information security awareness,” *Inf Manag Comput Secur*, 2000, doi: 10.1108/09685220010371394.

[23] “News from the blog | Open Source Initiative.” https://opensource.org/ (accessed Apr. 21, 2022).

[24] “Recital 30 - Online Identifiers for Profiling and Identification,” *General Data Protection Regulation (GDPR)*. https://gdpr-info.eu/recitals/no-30/ (accessed Apr. 21, 2022).

[25] “What is IoT Security?,” *Fortinet*. https://www.fortinet.com/resources/cyberglossary/iot-security (accessed Apr. 21, 2022).

[26] I. Böhm and S. Lolagar, “Open source intelligence,” *Int. Cybersecurity Law Rev.*, vol. 2, no. 2, pp. 317–337, Dec. 2021, doi: 10.1365/s43439-021-00042-7.

[27] “What are Sock Puppets in OSINT | How to Create One,” *CYBERVIE*, Apr. 02, 2021. https://www.cybervie.com/blog/what-is-sock-puppets-in-osint-how-to-create-one/ (accessed Apr. 21, 2022).

[28] “How OSINT is Used Against Your Employees - Hoxhunt.” https://www.hoxhunt.com/blog/how-osint-is-used-against-your-employees (accessed Feb. 15, 2022).

[29] “The Ultimate Beginner’s Guide to OSINT [2022].” https://www.osint-jobs.com/post/the-ultimate-beginners-guide-to-osint (accessed Feb. 21, 2022).

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

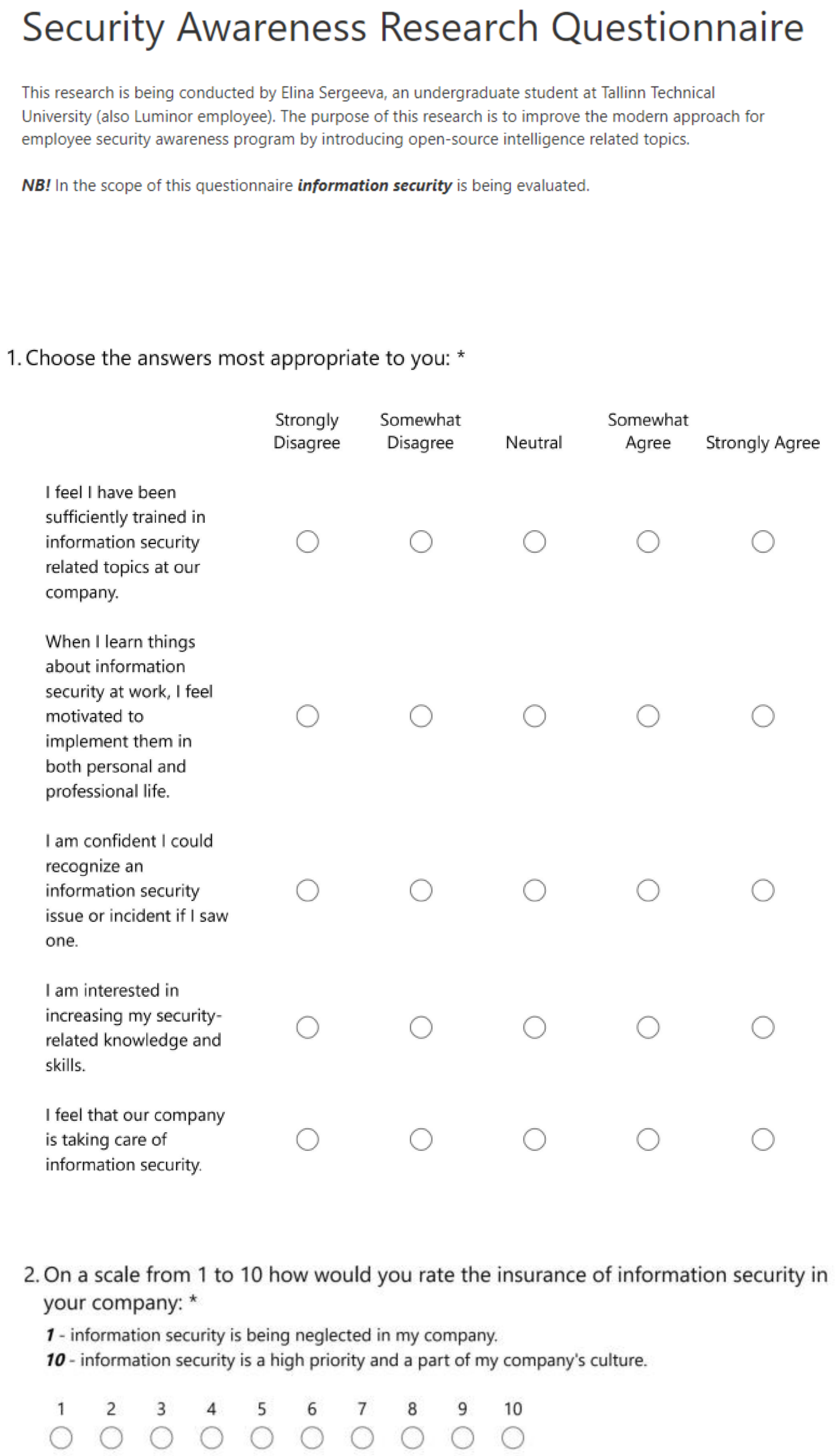
I Elina Sergeeva

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “The Role of Open Source Intelligence in Employee Security Awareness Program”, supervised by Kaido Kikkas
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

21.04.2022

[1] The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 - Pre-training questionnaire form.



Security Awareness Research Questionnaire

This research is being conducted by Elina Sergeeva, an undergraduate student at Tallinn Technical University (also Luminor employee). The purpose of this research is to improve the modern approach for employee security awareness program by introducing open-source intelligence related topics.

NB! In the scope of this questionnaire ***information security*** is being evaluated.

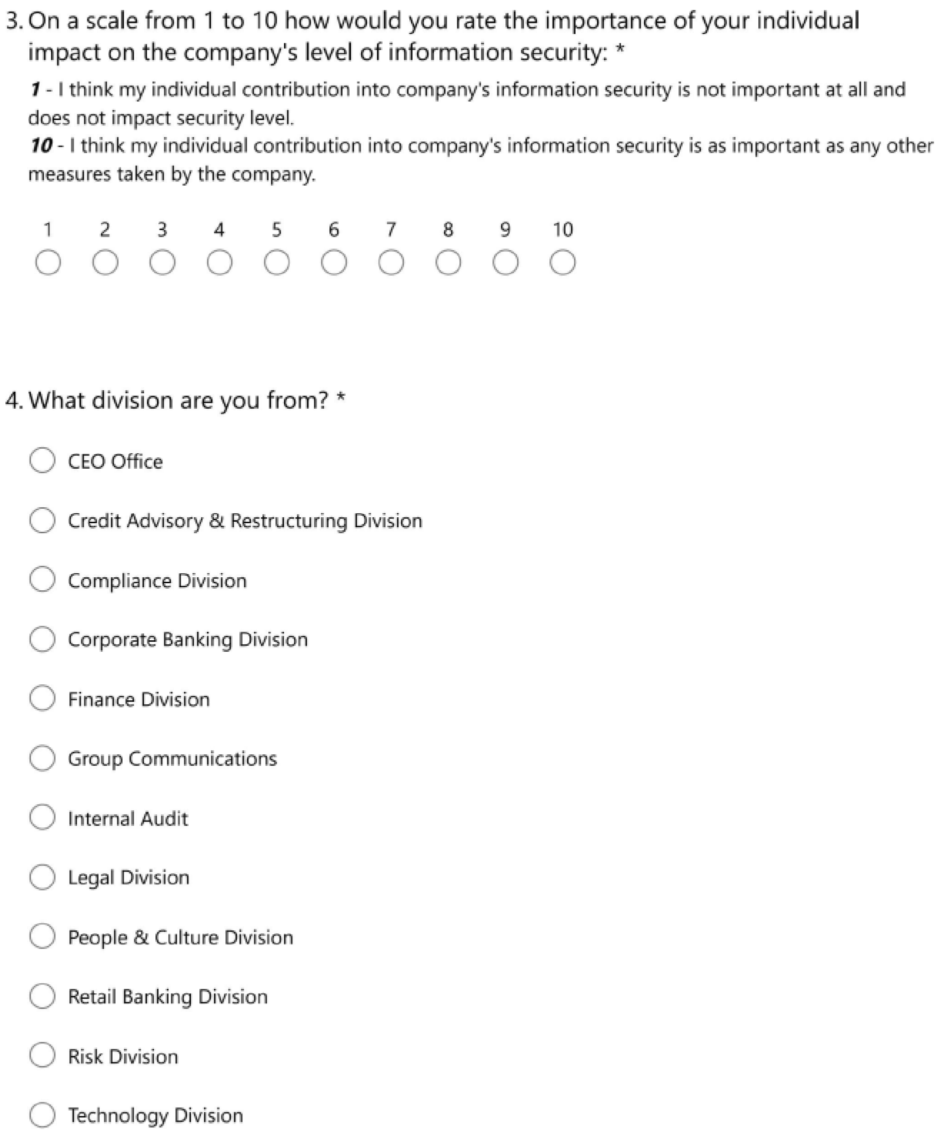
1. Choose the answers most appropriate to you: *

	Strongly Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Strongly Agree
I feel I have been sufficiently trained in information security related topics at our company.	○	○	○	○	○
When I learn things about information security at work, I feel motivated to implement them in both personal and professional life.	○	○	○	○	○
I am confident I could recognize an information security issue or incident if I saw one.	○	○	○	○	○
I am interested in increasing my security-related knowledge and skills.	○	○	○	○	○
I feel that our company is taking care of information security.	○	○	○	○	○

2. On a scale from 1 to 10 how would you rate the insurance of information security in your company: *

1 - information security is being neglected in my company.
10 - information security is a high priority and a part of my company's culture.

1	2	3	4	5	6	7	8	9	10
○	○	○	○	○	○	○	○	○	○



3. On a scale from 1 to 10 how would you rate the importance of your individual impact on the company's level of information security: *

1 - I think my individual contribution into company's information security is not important at all and does not impact security level.
10 - I think my individual contribution into company's information security is as important as any other measures taken by the company.

1	2	3	4	5	6	7	8	9	10
○	○	○	○	○	○	○	○	○	○

4. What division are you from? *

○ CEO Office

○ Credit Advisory & Restructuring Division

○ Compliance Division

○ Corporate Banking Division

○ Finance Division

○ Group Communications

○ Internal Audit

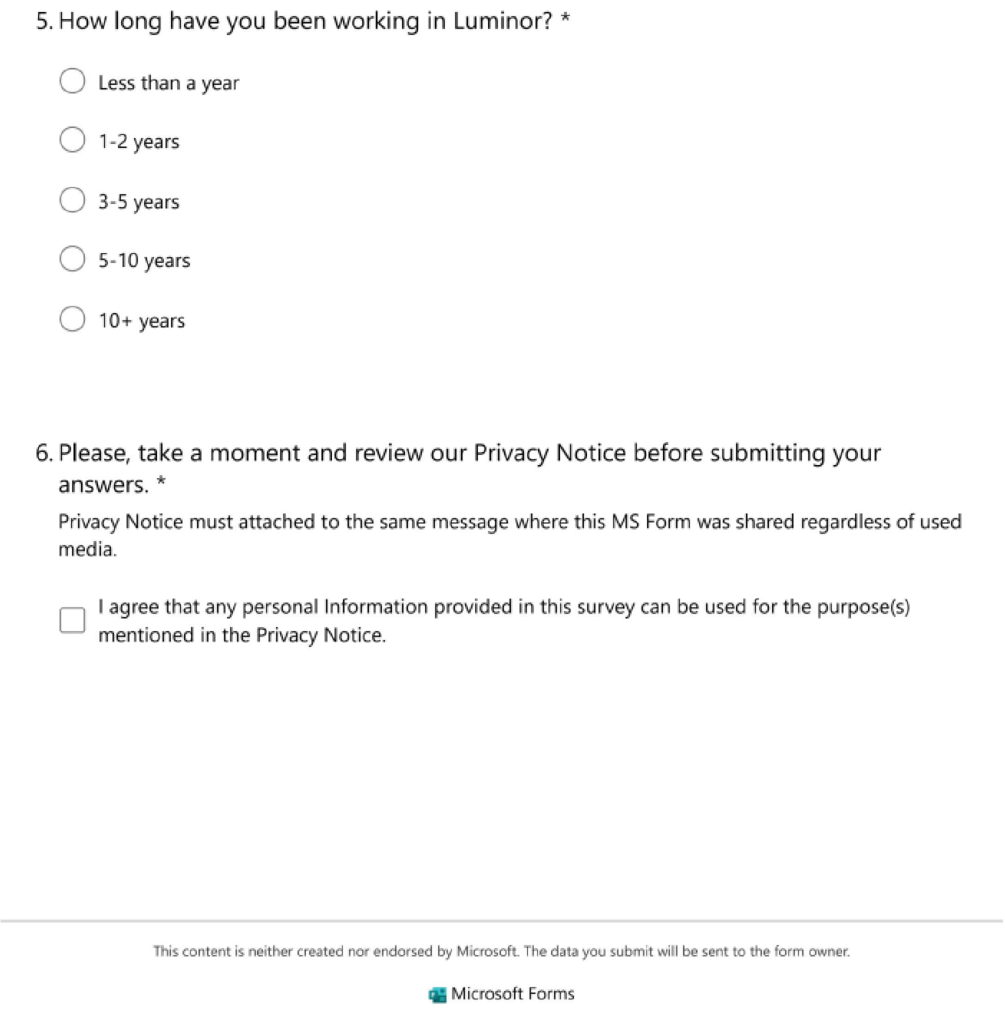
○ Legal Division

○ People & Culture Division

○ Retail Banking Division

○ Risk Division

○ Technology Division



5. How long have you been working in Luminor? *

○ Less than a year

○ 1-2 years

○ 3-5 years

○ 5-10 years

○ 10+ years

6. Please, take a moment and review our Privacy Notice before submitting your answers. *

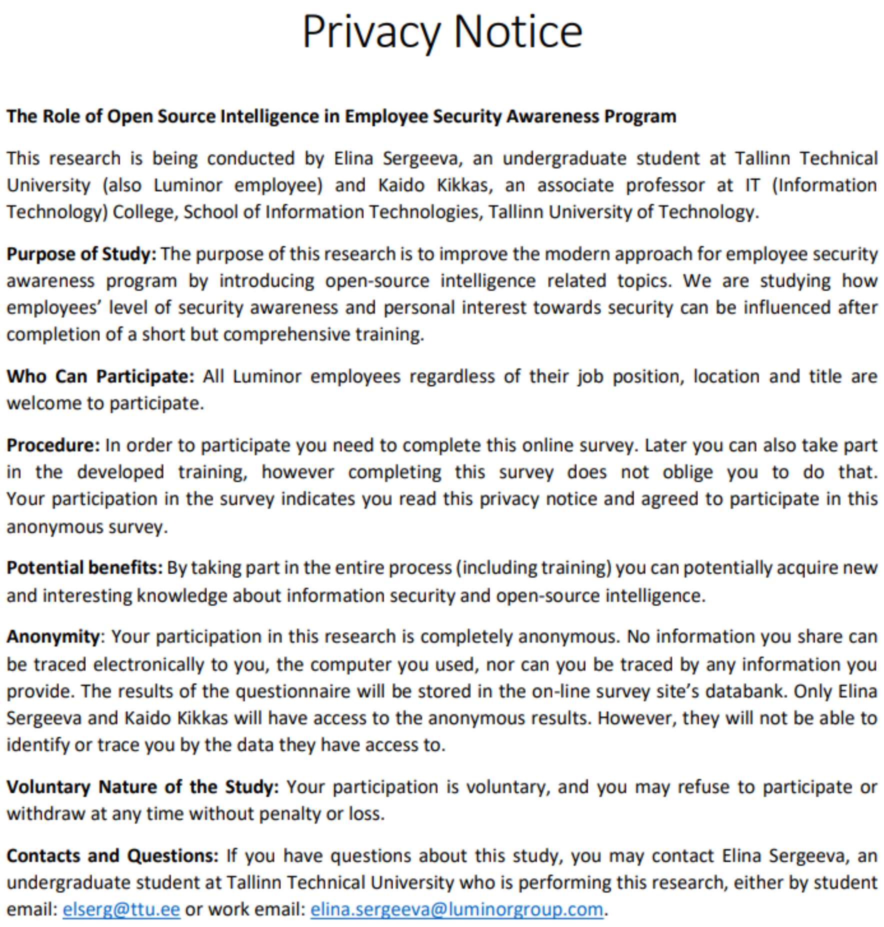
Privacy Notice must attached to the same message where this MS Form was shared regardless of used media.

□ I agree that any personal Information provided in this survey can be used for the purpose(s) mentioned in the Privacy Notice.

This content is neither created nor endorsed by Microsoft. The data you submit will be sent to the form owner.

Microsoft Forms

Appendix 3 - Privacy notice for the pre-training survey



Privacy Notice

The Role of Open Source Intelligence in Employee Security Awareness Program

This research is being conducted by Elina Sergeeva, an undergraduate student at Tallinn Technical University (also Luminor employee) and Kaido Kikkas, an associate professor at IT (Information Technology) College, School of Information Technologies, Tallinn University of Technology.

Purpose of Study: The purpose of this research is to improve the modern approach for employee security awareness program by introducing open-source intelligence related topics. We are studying how employees' level of security awareness and personal interest towards security can be influenced after completion of a short but comprehensive training.

Who Can Participate: All Luminor employees regardless of their job position, location and title are welcome to participate.

Procedure: In order to participate you need to complete this online survey. Later you can also take part in the developed training, however completing this survey does not oblige you to do that. Your participation in the survey indicates you read this privacy notice and agreed to participate in this anonymous survey.

Potential benefits: By taking part in the entire process (including training) you can potentially acquire new and interesting knowledge about information security and open-source intelligence.

Anonymity: Your participation in this research is completely anonymous. No information you share can be traced electronically to you, the computer you used, nor can you be traced by any information you provide. The results of the questionnaire will be stored in the on-line survey site's databank. Only Elina Sergeeva and Kaido Kikkas will have access to the anonymous results. However, they will not be able to identify or trace you by the data they have access to.

Voluntary Nature of the Study: Your participation is voluntary, and you may refuse to participate or withdraw at any time without penalty or loss.

Contacts and Questions: If you have questions about this study, you may contact Elina Sergeeva, an undergraduate student at Tallinn Technical University who is performing this research, either by student email: elserg@ttu.ee or work email: elina.sergeeva@luminorgroup.com.

Appendix 4 - Software and didactical indicators for evaluating the effectiveness of e-learning

The below evaluation criteria originate from “Methodologies, Tools and New Developments for E-Learning” by Elvis Pontes [15].

Software indicators

Indicator	Description	Is the e-course compliant?

1.Personalized teaching	The tools for self-teaching helps the students to study according to their capabilities and free time, to choose the form and the way of providing the material on the basis of their own predilections;	**Yes**. The developed e-course allows students to study the materials in their free time, making pauses when needed.
2.Interoperability	To support content from different sources and multiple vendors' hardware / software solutions, the system should be based on open industry standards for Web deployments (XML, SOAP or AQQ) and support the major learning standards (AICC, SCORM, IMS and IEEE);	**Yes**. The development platform allows to export the training materials in the following LMS formats: SCORM 1.2, SCORM 2004, AICC, xAPI, cmi5. Besides that, training can be exported as webpage or PDF file. Additionally, the training can be shared via link, which can be open in any browser.
3.Reliability	To give acceptable results even if there are invalid inputs. The assessment gives an opportunity refusals and situations that involve refusals to be predicate;	**Yes**. The chosen interactive parts where the input from trainees is required are designed in a way, that feedback is provided in case wrong answer was given by a trainee. Or wrong answer would be recorded, and trainee can restart the activity.
4.Flexibility	To exit an opportunity for changes in the content	**Yes**. Developed training materials are upgradable.
5.Portability [modularity]	To be independent from the users' operating system and to be used by widespread browser	**Yes**. Users can open training materials in any browser. Besides that, training can be

	such as Internet Explorer, Netscape Communicator etc.	exported in formats such as PDF, web, HTML, what allows to study them even with no internet connection.
6.Functionality	To be useful;	**Yes**. Based on collected post-training feedback, it is possible to conclude that the developed e-course was useful.
7.Accountability	The classifying, testing and the assessment have to be automated in such a way that the participants to be distributed according to their responsibilities in the process of learning;	**N/A.** This criteria is not applicable to the present work, since the developed e-course doesn’t have functionality for group work as well as functionality for providing different materials based on job duties and responsibilities.
8.Security	The system should selectively limit and control access to online content and resources for its diverse user community;	**Yes**. The training platform is a separate system, which has only educational resources displayed on it.
9.Costs indicator	Measures the costs for purchasing the system, its exploitation and support, etc.;	**Yes**. In the case of the Company X, the solution is cost effective, because it did not require purchase of any additional software or service subscription.

Didactical indicators

Indicator	Is the e-course compliant?

The material should be presented in a logical sequence. Broken into small, incremental learning steps;	**Yes.** The sequence was defined based on the sequencing methodology described in chapter 4 of “E-learning methodologies and good practices” by FAO e-learning Academy [14].
The material should be linked to other sources, with reading assignments clearly specified;	**Yes.** Links to additional sources are provided in two ways: incorporated into the main e-course materials; as additional materials (“Further Materials” chapter).
The material should be Illustrated by examples and/or case studies when new information is presented;	**Yes.** Where appropriate, materials are supported by illustrated study cases, or illustrated process flow. This is ensured by instructional techniques for content development described in chapter 7 of FAO e-learning Academy best practices [14].
Encouragement for critical thinking, creativity, and problem-solving;	**Yes.**
Relation to other material the learners may have studied or experiences they may have had;	**Yes.** The e-course has materials targeted to be implemented as practices related to workplace. The e-course is considered advanced, meaning employees are required to take basic ISA training, present in Company X.
Usage of illustrations, photographs, animation, and other forms of multimedia in order to present facts and reinforce concepts;	**Yes.**
Abbreviations and symbols are defined;	**Yes.**
Appropriate language level for the intended audience.	**Yes.** Based on e-course participants’ feedback, the language was appropriate and easy to understand.

Appendix 5 - Complete and Sequenced List of Topics

Content Type	**Content Name**	**Learning Outcomes**	**Sources**
Block	INTRODUCTION TO OSINT AND BASIC CONCEPTS		
Chapter	What is OSINT?	Trainees understand the definition of OSINT and underlying concepts, such as intelligence and open source.	[23]
Chapter	The Internet	Trainees know the difference between the Internet and the Web and can describe how both are structured and work. Trainees are familiar with the 3 layers of the Web: surface web, deep web and dark web, and know basic properties of each. Trainees understand the concept behind IoT and what security challenges it poses.	[25][24]
Chapter	OSINT Use Cases	Employees understand how broad the use of OSINT is and who uses it: from journalists and law enforcement agencies to cyber criminals. Trainees know a few examples of how OSINT legal use and illegal misuse.	[26]
Block	OSINT SKILLS		
Chapter	Fake Accounts	Trainees are familiar with the concept of fake accounts and how they can be used online for spreading misinformation or committing fraud. Employees are familiar with the tools used for the fake account creation for understanding how easy it is for a malicious actor to create a convincing fake profile.	[27]
Chapter	OSINT Skills Introduction	Trainees distinguish 3 types of OSINT skills: those which will provide them with useful skills for the Internet usage, those which will show how malicious actors abuse OSINT, those which will promote enhanced safety against OSINT.	
Chapter	Google Hacking	Trainees know what Google hacking is and are familiar with the search operators: site, filetype, asterisk.	[19]

		Employees know how to use those operators.	
Chapter	Web Archives	Trainees understand how information spreads across the Internet, and how hard it is to ensure traceless data deletion. Employees are familiar with the Wayback Machine service and know how to use it.	
Chapter	Metadata	Trainees understand what metadata is, how to review, edit and remove it from files. Trainees understand how metadata removal promotes security.	[28]
Chapter	Social Media and Profile	Employees understand how much and what personal data is displayed on social media profiles. They are also familiar with tools which can assimilate and analyse such data collected from different social media platforms.	[19]
Chapter	Tips for Staying Secure Online	Trainees understand what steps shall be taken for enhancing the security of their social profiles online. They know how to recalibrate and control data available on themselves online in open source. In particular, participants know how to adjust privacy settings, choose strategy for managing friend requests, manage likes and tagged photos on Facebook.	[19][18]
Chapter	Summary		
Block	THANK YOU FOR TAKING THE COURSE!		
Chapter	Further Materials	Trainees are familiar with OSINT communities on some social media platforms as well as some other related to the topic resources: websites, books, articles. Trainees are engaged into the topic and provided with further materials to enrich their knowledge about the topic.	[29]