TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Marco Fontana 233931IVCM

HUMAN ASPECTS OF OSINT IN CORPORATE ESPIONAGE: HOW EMPLOYEES UNKNOWINGLY LEAK CRITICAL INFORMATION

Master's Thesis

Supervisor: Ricardo Gregorio Lugo
PHD in Psycology

Tallinn 2025

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Marco Fontana 233931IVCM

INIMFAKTORID OSINT-IS ETTEVÕTTESPIONAAŽI KONTEKSTIS: KUIDAS TÖÖTAJAD TEADMATA LEKITAVAD KRIITILIST TEAVET

Magistritöö

Juhendaja: Ricardo Gregorio Lugo
PHD in Psycology

Tallinn 2025

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: Marco Fontana

27.05.2025

Abstract

This thesis explores the unintentional leakage of sensitive corporate information caused by employee online behavior. The focus is on the Estonian banking system, which is part of the national critical infrastructure. This research investigates how publicly accessible data gathered through open source intelligence techniques can be used by cybercriminals to map internal infrastructures, identify potential vulnerabilities, and enable targeted attacks. The analysis of social media profiles of banking employees on platforms such as LinkedIn, Facebook, Instagram, X, TikTok, and GitHub will support this discussion. The results from this analysis demonstrate the potential risk posed by human behavior in digital spaces, where harmless information, such as job roles, tools used, screenshots, or internal URLs, can undermine corporate security. This research emphasizes the need for banking institutions to invest in employee cybersecurity awareness and properly adapt existing frameworks to account for OSINT related threats. The study also provides a set of recommendations for resilience improvement as a safeguard against corporate espionage and human centric vulnerabilities in critical infrastructure sectors.

The thesis is written in English and is 68 pages long, including 13 chapters 8 figures and 1 table.

Annotatsioon

Inimfaktorid OSINT-is ettevõttespionaaži kontekstis: kuidas töötajad teadmata lekitavad kriitilist teavet

See magistritöö käsitleb tundliku ettevõttesisese teabe tahtmatut lekkimist, mille põhjustajaks on töötajate veebikäitumine. Töö keskendub Eesti pangandussüsteemile, mis on osa riigi kriitilisest infrastruktuurist. Uurimuse eesmärk on näidata, kuidas avalikult kättesaadavat teavet, mis on kogutud avatud lähtekoodiga luure (OSINT) meetodite abil, saavad küberkurjategijad kasutada sisemiste infrastruktuuride kaardistamiseks, võimalike haavatavuste tuvastamiseks ja sihitud rünnakute läbiviimiseks. Analüüs põhineb pangatöötajate sotsiaalmeedia profiilidel platvormidel nagu LinkedIn, Facebook, Instagram, X, TikTok ja GitHub.

Analüüsi tulemused näitavad, et inimkäitumine digikeskkondades kujutab endast potentsiaalset turvariski – näiliselt süütu teave, nagu ametinimetused, kasutatavad tööriistad, ekraanipildid või sisemised URL-id, võivad ohustada ettevõtte turvalisust.

Uurimus rõhutab vajadust, et pangandusasutused investeeriksid töötajate küberhügieeni ja -teadlikkuse tõstmisesse ning kohandaksid olemasolevaid raamistikke OSINT-ist tulenevate ohtude arvestamiseks. Samuti antud uurimistöös antakse soovitusi vastupanuvõime suurendamiseks, et kaitsta ettevõttespionaaži ja inimkesksete haavatavuste eest kriitilise infrastruktuuri sektoreid.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 68 leheküljel, 13 peatükki, 8 joonist, 1 tabel.

List of Abbreviations and Terms

BEC	Business Email Compromise
CVE	Common Vulnerabilities and Exposures
GDPR	General Data Protection Regulation
ECSF	European Cybersecurity Skills Framework
IoT	Internet of Things
MRQ	Main Research Question
OSINT	Open Source Intelligence
PII	Personally Identifiable Information
SOC	Security Operations Center
SRQ	Sub Research Question
SIEM	Security Information and Event Management

Table of Contents

List of Figures

List of Tables

1. Introduction

In the contemporary digital landscape, the boundary between personal and professional online presence has become increasingly blurred. Employees' extensive use of social media platforms, collaborative digital tools, and publicly accessible communication channels often leads to the inadvertent exposure of sensitive organizational information. This phenomenon has been widely documented in cybersecurity research, highlighting the risks associated with human behavior in digital environments [1].

The aim of this thesis is to investigate how human digital behavior intersects with open source intelligence (OSINT) practices, focusing on the Estonian banking sector, a critical component of national infrastructure. Employees' daily online activities, particularly their interactions on platforms like LinkedIn, are the focus of this research. Apparently harmless disclosures can unintentionally lead to data leakage, increasing the risk of targeted cyber threats against financial institutions.

Threat actors actively exploit publicly available information to conduct data gathering, craft highly targeted phishing campaigns, and facilitate corporate espionage. Studies such as DeCusatis et al. [2] show how OSINT techniques are systematically employed during the pre-attack phase to gather intelligence about organizational structures, employee roles, and internal operations. Social engineering attacks, for example, often begin with information collected from publicly accessible employee profiles, blog posts, or professional announcements. Prior research demonstrates that OSINT based information gathering can lead to measurable exposure in the financial sector. For example, a study on Croatian banks by Matvej, Morić, and Papić [3] revealed that employees frequently disclosed internal tool names, system types, and professional roles on social media platforms. These behaviors enabled attackers to develop targeted phishing and impersonation campaigns, highlighting the importance of OSINT analysis at the institutional level in highly digitized regions.

This thesis focuses on behavioral insights derived from social media analysis to provide a deeper understanding of how OSINT related vulnerabilities emerge through human actions. The concern around such vulnerabilities has also been emphasized in the OSINT based cyber threat inspection framework for critical infrastructures proposed by Lee and Shon [4], which identifies public information exposure as a major attack vector.

In exploring these dynamics, this research seeks to contribute to a more comprehensive

understanding of OSINT risks in critical sectors and inform strategies for enhancing organizational resilience in the face of evolving human centric cybersecurity threats.

2. Background and motivation

2.1 Background

This thesis explores the extent to which human behavior, particularly employees' online activities contributes to the unintentional disclosure of sensitive corporate information through publicly accessible sources. It focuses on Estonia's banking sector and how employee engagement with social media and other platforms may inadvertently reveal information exploitable by threat actors. Recent events illustrate this risk. For instance, in September 2023, several Estonian residents lost thousands of euros due to phishing attacks designed to resemble banking communications that impersonated legitimate messages and exploited victims' trust in online banking systems [5]. While these incidents did not directly originate from bank employee disclosures, they demonstrate the ongoing exploitation of human behavior in financial cyberattacks. Furthermore, in March 2024, a cyber incident at Hansab, a company providing secure banking infrastructure, caused the malfunctioning of self service banking machines in Estonia [6]. While the attack did not target banks directly, it revealed the interconnected nature of digital service providers and the potential risks arising from the exposure of technical infrastructure. These examples reinforce the relevance of studying open source intelligence risks not only at the organizational level but also across the broader ecosystem that supports financial services.

As demonstrated by Capano [7], human factors remain a critical vulnerability in cybersecurity ecosystems. Whether due to inadvertent mistakes or susceptibility to manipulation, employees can become channels for corporate espionage, especially when adversaries leverage OSINT techniques. Such vulnerabilities do not only threaten individual organizations but may also undermine the resilience of the wider financial system.

Recent analysis from the European Union Agency for Cybersecurity (ENISA) highlights this concern. Between January 2023 and June 2024, ENISA documented 488 cybersecurity incidents in the European finance sector, with credit institutions accounting for 46% of those affected. DDoS attacks were the most prevalent (46%), followed by data-related threats (15%) and social engineering (13%) [8]. These attacks often exploit publicly available data, including that generated by employees, highlighting the relevance of this study to open source intelligence based reconnaissance and targeted attacks.

Positioning the analysis within Estonia's banking sector, this research aligns with threat

intelligence findings and addresses a critical gap in the existing literature. In digitally advanced societies where professional visibility is promoted, employee generated content may unintentionally become an asset for adversarial intelligence gathering. This thesis thus contributes to understanding the human dimensions of OSINT exploitation within critical infrastructure and supports arguments for integrating behavioral risk assessments into national and sectoral cybersecurity strategies.

To properly evaluate mitigation strategies for these type of risks, this thesis draws on internationally recognized cybersecurity frameworks. The NIST SP 800-53 Revision 5 framework, published by the U.S. National Institute of Standards and Technology, provides a comprehensive catalog of security and privacy controls applicable to critical infrastructure sectors, including financial institutions [9]. While open source intelligence is not explicitly addressed, several control families can be interpreted and adapted to reduce human driven exposure. The Awareness and Training (AT) family [10] supports the development of employee education programs aimed at minimizing digital footprint risks and promoting secure online behavior. The Personnel Security (PS) [10] controls establish mechanisms for managing user responsibilities, including access agreements and oversight of third party personnel. Risk Assessment (RA) controls [10] guide organizations in identifying exposure points through periodic evaluations and passive reconnaissance methods such as Google Dorking. Additionally, the System and Communications Protection (SC) and Planning (PL) control families [10] reinforce technical safeguards and policy driven governance structures that contribute to the minimization of publicly accessible sensitive data. Complementing this, the ISO/IEC 27001 standard introduces a structured approach to information security management based on continuous improvement cycles [11], while ENISA provides ongoing threat landscape assessments and strategic guidance on social engineering and employee targeted attack vectors [12]. These frameworks collectively establish the theoretical foundation for Chapter 9, where mitigation strategies are critically assessed in relation to the OSINT risks identified in Estonia's banking sector.

2.2 Motivation

The motivation for this research arises from an interest in understanding how corporate espionage can be leveraged through OSINT tools that exploit information employees unknowingly share on social media. Information disclosed on social media, when combined with other publicly available online resources, can create a comprehensive and highly exploitable intelligence profile. This combination enables malicious actors to map corporate structures, identify vulnerabilities, and plan targeted attacks.

In an environment where organizations are heavily reliant on digital infrastructure, even

minimal public exposure of corporate or technical metadata can present serious consequences. This is particularly critical in the banking sector, where breaches can lead to significant financial and reputational damage.

While studies like the one on Croatian banks highlight how information disclosed by employees can increase organizational exposure to threats related to OSINT [3], Estonia presents a unique case. Its technological advancements and distinctive cybersecurity landscape justify further investigation. The evolution of cyber threats and Estonia's highly digitized environment necessitate updated, geographically focused research to understand current vulnerabilities.

This thesis seeks to fill a gap in the existing cybersecurity literature through an examination of how OSINT-driven vulnerabilities manifest within Estonia's financial industry. While general risks have been discussed by previous studies, sector and context specific analyses remain limited. Narrowing the focus to Estonia's banking sector, this research aims to contribute to the development of tailored cybersecurity practices that specifically address human centric vulnerabilities. Similar calls for targeted approaches have been made by scholars including Mitchell [13], Bizouarn, Abdulnabi, and Tan [14], and Lee and Shon [4], who emphasize the importance of integrating behavioral risk into open source intelligence threat models for critical infrastructure protection.

3. Research problem and objectives

The increasing integration of digital technologies in professional environments has transformed how employees communicate and share information. Digital transformation improves operational efficiency but also introduces new risks, particularly related to the unintentional exposure of sensitive information [15].

OSINT techniques, which involve collecting information from publicly accessible sources, have become significant tools during the information gathering phase of cyberattacks [4]. Human behavior, particularly that of employees active on platforms such as LinkedIn, Twitter/X, Instagram, Facebook, TikTok, and GitHub, plays a critical role in creating these vulnerabilities.

The concept of the non-malicious insider threat is especially relevant in this context. Unlike malicious insider threats, non-malicious insiders do not intend to harm their organization, but through careless or unaware behavior, they contribute to the leakage of critical information [15]. Through their public profiles, posts, and online interactions, employees can unintentionally reveal details such as organizational structures, project information, internal tools, and technology stacks. Threat actors can aggregate this information through open source intelligence techniques to build a comprehensive attack profile.

Each social media platform presents unique exposure risks. On LinkedIn, employees frequently share information about their roles, technologies used within the organization, and team structures. According to Hayes [1], LinkedIn is a powerful tool for identifying key employees in an organization and understanding their networks and areas of expertise. While not originally designed for reconnaissance, this structured information can be repurposed for profiling by external observers, including adversaries during the pre-attack phase [7].

Twitter/X is used for short, real time updates that may unintentionally disclose work-related developments or internal events. Instagram and Facebook often feature images from daily work life, including work from home setups, that may capture customer names, internal software, or sensitive environments without realizing it. TikTok, with its short form videos, can also reveal internal processes or office layouts. GitHub repositories may unintentionally contain sensitive code, documentation, or even security credentials.

A concrete example is illustrated in Figure 1. In this case, an employee shared a Facebook story during a work from home day, where a photo showed their laptop screen. Although the post was intended to be personal, it inadvertently revealed a customer name and the internal tool being used. While the employee's identity and sensitive details have been anonymized for this thesis, this case highlights how easily sensitive data can be exposed without malicious intent.

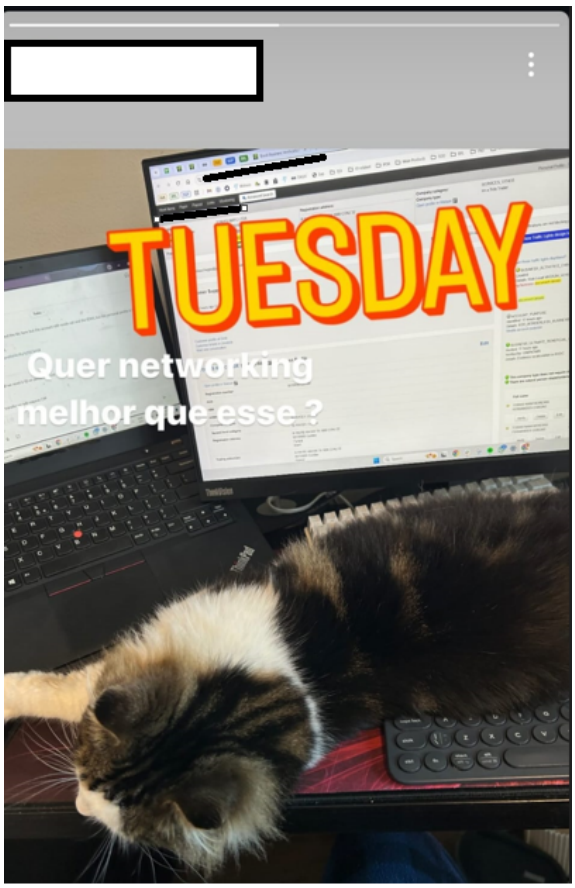

Figure 1. *Facebook story posted by an employee during remote work, unintentionally exposing customer information and internal tools.*

Although the risks associated with OSINT have been acknowledged in previous cybersecurity research [4, 15], specific attention to sectoral and geographical contexts remains limited. The Estonian banking sector, deeply integrated with national digital infrastructure, presents a critical area where public digital footprints of employees may contribute to organizational exposure.

Understanding how digital footprints created by bank employees contribute to organizational vulnerabilities, is important for developing mitigation strategies tailored to the sector's needs. For example, monitoring public disclosures and implementing targeted awareness campaigns can significantly reduce the exposure surface. Additionally, banks can introduce internal policies to guide employees on safe social media behavior and

conduct regular security trainings. They can also deploy technical solutions, such as monitoring for leaked credentials on public repositories or social media platforms. ENISA recommends that financial institutions adopt both technical and procedural controls to manage human centric risks, including credential monitoring, social media policy enforcement, and OSINT auditing [8]. These measures align with best practices for enhancing cyber resilience in high-risk sectors.

This research is guided by one main research question and four sub-research questions:

Main Research Question **(MRQ)**: What role do human factors play in the unintentional exposure of corporate data across critical industries?

Sub-Research Questions **(SRQs)**:

- **SRQ1**: How do threat actors exploit employee data from social media platforms?
- **SRQ2**: How do different social media platforms contribute to data exposure risks?
- **SRQ3**: What are the specific OSINT risks for the banking sector in Estonia compared to other industries?
- **SRQ4**: How can cybersecurity frameworks be adapted to mitigate OSINT risks in specific industries?

Together, these questions aim to fill the current knowledge gap between human digital behavior and cybersecurity risk governance in critical infrastructure environments, considering the Estonian bank sector.

4. Scope and goals

The objective of this study is to examine how human behavior on social media platforms contributes to the unintentional leakage of corporate information. It further investigates how data collected through OSINT techniques can be exploited in corporate espionage, with a specific focus on the Estonian banking sector as part of the nation's critical infrastructure. The scope is limited to information that is publicly available, including data voluntarily disclosed by employees through public social media activities. Breaches involving unauthorized access to internal systems or confidential information not intended for public disclosure are intentionally excluded from this study.

5. Literature review

5.1 OSINT and human behaviour in data exposure

The literature on open source intelligence and corporate security emphasizes the significant role that human behavior plays in unintentional data exposure [7, 15]. Unintentional data exposure refers to instances where individuals, without malicious intent, share information on public platforms that could later be used against the organization [15].

Different studies demonstrate how social media platforms are rich sources of OSINT, where employees' online behaviors such as disclosing job roles, technical competencies, internal tools used, or organizational affiliations, create potential vectors for threat actors [16, 3]. For example, employees' LinkedIn profiles may list technologies they are familiar with (e.g., AWS, SAP), or internal project names, allowing attackers to build detailed organizational maps. Facebook posts showing office layouts or team events can also be used for physical or phishing attack planning.

These disclosures, even if unintentional, contribute to a digital footprint that adversaries can leverage for targeted phishing campaigns, social engineering, or broader corporate espionage operations [7, 1]. Threat actors typically collect fragmented public information to create detailed employee profiles, which in turn allow them to craft highly convincing phishing emails or social engineering pretexts. Attackers might, for instance, impersonate internal IT helpdesk personnel or request access to confidential resources, exploiting the perceived legitimacy built through OSINT gathering.

The risk is particularly significant when considering critical infrastructure sectors, including finance, where the exposure of internal operations, employee identities, or system details can have major consequences, such as facilitating fraud, credential compromise, or unauthorized access [8]. Researchers have shown that attackers increasingly utilize publicly available data to breach systems, simulate insider access, or plan highly targeted attacks to overcome conventional perimeter defenses [2, 17]. For example, DeCusatis et al. [2] demonstrated how combining public employee information with facility maps enabled successful physical penetration tests without needing to breach digital defenses.

Structured OSINT methodologies for threat analysis in critical infrastructure contexts have also been proposed in the literature [4], supporting the use of open data for adversarial

modeling and simulation of attack paths. These studies reinforce the importance of integrating behavioral risk into cybersecurity governance.

5.2 Sector-specific risks: banking and finance

Although the risks associated with social media data exposure are well documented in general corporate contexts, there remains a need to extend the awareness of these risks specifically within the banking and finance sector. These sectors possess distinct risk profiles due to regulatory pressures, centralized information systems, and critical dependence on employee access management [18, 19]. According to ENISA [8], the finance sector faces increased vulnerability to social engineering attacks, insider threats, and data breaches. The leakage of corporate data through the exploitation of employee digital footprints via OSINT techniques remains a real and growing threat.

One notable study investigating vulnerabilities in the Croatian banking sector showed how staff activity and lack of cybersecurity awareness contribute to OSINT related threats [3]. Through the analysis of publicly available employee profiles, particularly on LinkedIn, the researchers identified job titles, hierarchical roles, and technologies in use. These disclosures were then correlated with leaked email addresses found in previous breaches, allowing the reconstruction of internal organizational structures. Although no real world attacks were traced in the study, the researchers demonstrated how a threat actor could use this aggregated information to simulate internal reconnaissance and develop spear phishing or credential harvesting strategies tailored to specific job functions. This highlights how human driven exposure can act as a precursor to more targeted exploitation.

Similar challenges have been documented in the energy sector, where OSINT was used to aggregate staff and operational details from public sources, enabling adversaries to simulate insider access and model attack vectors without direct system penetration [4]. These examples emphasize the importance of sector specific analysis, particularly for industries managing critical infrastructure.

Estonia's banking sector forms a critical component of the country's digital infrastructure and economic stability [20, 21, 22, 23]. Despite Estonia's leading digital innovation, this makes the sector more exposed to OSINT threats due to its high reliance on interconnected services. The lack of research in this area complicates the development of mitigation strategies tailored to Estonia's specific national context, cybersecurity maturity, and digital banking model.

5.3 Integration of OSINT into cybersecurity frameworks

In parallel with the lack of sector specific studies, the literature reveals a weak integration of OSINT related risks into cybersecurity frameworks such as the European Cybersecurity Skills Framework (ECSF) developed by ENISA, NIST SP 800-53, and ISO/IEC 27001. While these frameworks recognize the importance of human factors in cybersecurity, defining them through domains such as 'Awareness and Training' (NIST Control Family AT), 'Personnel Security' (PS) [10], and 'Operational Security' (ISO Annex A.7 and A.8) [11], they typically address human related risks in broader terms, without specific consideration for unintentional OSINT exposures.

In particular, frameworks such as ENISA's ECSF highlight the need for continuous cybersecurity awareness programs, encouraging the education of employees about cyber hygiene and the threats posed by online information sharing [12]. NIST emphasizes periodic trainings to mitigate insider threats [9], while ISO/IEC 27001 mandates that organizations manage the risks arising from human error and ensure that personnel understand their security responsibilities [11]. However, despite these high level prescriptions, there remains a gap in explicitly integrating open source derived intelligence risks, such as those originating from employee social media disclosures, into formal risk management protocols.

Mitchell [13] emphasizes the need to integrate human behavior into cybersecurity frameworks because traditional models often overlook how employee actions, such as oversharing on social media, reusing passwords, or failing to recognize phishing attempts, can undermine otherwise robust technical defenses. He argues that attacker methodologies are evolving to exploit behavioral patterns that are publicly visible, predictable, and often ignored in classical risk assessments. Therefore, incorporating behavioral awareness and OSINT specific vulnerabilities is essential for ensuring frameworks address both human and technical threat surfaces.

In this context, Lee and Shon [4] introduced a four step OSINT inspection framework for cyber threat analysis in critical infrastructure sectors. Their methodology begins with the planning phase, where the scope of the investigation is defined, and relevant targets, systems, and data sources are identified. This includes platforms such as company websites, employee directories, and social media profiles. The second phase, gathering, focuses on the passive collection of publicly available data using methods like search engine queries (e.g., Google Dorking), metadata extraction, and profile mining. In the analysis phase, the gathered data is correlated to reconstruct organizational hierarchies, detect references to systems or tools, and identify potential vulnerabilities or personnel who could be exploited.

The final phase, production, converts the results of the analysis into actionable intelligence, offering simulated attack paths, entry point prioritization, and tailored recommendations for mitigating human centric risks.

Their framework was validated through simulations applied to a national energy infrastructure provider. The results demonstrated that attackers could identify the types of control systems in use, determine shift schedules, and estimate access privileges purely by aggregating OSINT data. This model offers valuable insight into how adversarial reconnaissance functions in the real world, and it provides a strong benchmark for the passive methodology adopted in this thesis.

Despite its robustness, the operational integration of such a framework into organizational governance remains rare. Practical challenges include concerns over employee privacy, legal compliance with data protection laws such as the GDPR, and the resource burden of conducting regular OSINT reviews. Nonetheless, as this thesis demonstrates, behavioral exposure is an increasingly exploited vector by attackers, and addressing this risk domain through OSINT-informed governance is critical for institutions operating in high-risk environments like the banking sector.

5.4 Summary and relevance to this study

This thesis addresses the identified gaps, focusing on the Estonian banking sector. Specifically, it investigates how employee behavior on public platforms contributes to unintentional data leakage, increasing vulnerability to OSINT based cyber threats. It examines how threat actors can leverage publicly shared professional information to conduct targeted reconnaissance, phishing attacks, and social engineering campaigns [24].

Mapping behavioral OSINT indicators into cybersecurity frameworks such as ENISA, ISO 27001, and NIST SP 800-53, the research provides practical strategies for Estonian financial institutions to strengthen their defenses against human centric cyber risks. The study also contributes to broader cybersecurity policy development by contextualizing OSINT threats within Estonia's unique digital and regulatory environment, offering sector specific insights for resilience building in the banking sector.

5.5 Research gaps and systematic approach

To support the research objectives of this study, a systematic literature review was conducted. The review focused on collecting and analyzing academic and industry publications

addressing the role of human behavior in unintentional data exposure via open source intelligence, with a particular emphasis on risks affecting critical infrastructure sectors such as banking.

The literature search was performed across three major academic databases: Scopus, JSTOR, and EBSCO Discovery Service. To ensure the inclusion of recent research, only academic articles and journal papers published between 2015 and 2025 were considered. The initial keyword applied was "OSINT," which retrieved 552 records from EBSCO Discovery Service, 503 from Scopus, and 338 from JSTOR. To refine the search results, additional keyword combinations were used, including: “OSINT” and “corporate espionage”, “OSINT” and “LinkedIn”, “OSINT” and “critical infrastructure”, "OSINT" and "banking", “OSINT” and “employee”, “OSINT” and “social engineering”, and “corporate espionage” and “cybersecurity.” These queries helped filter the data to focus specifically on studies at the intersection of OSINT practices and human behavior in corporate environments.

The inclusion criteria required articles to published in English, and relevant to the main research question and the four sub-research questions defined for this study. Studies were selected if they addressed OSINT in relation to human factors, attacker tactics, vulnerabilities in critical infrastructure sectors (particularly finance), or the integration of OSINT findings into cybersecurity frameworks. Exclusion criteria omitted articles that were purely technical, unrelated to corporate or organizational settings, or not specifically addressing human centered risks.

Following the screening process based on titles and abstracts, 21 core academic articles and white papers were selected for detailed analysis. Each source was examined using a structured extraction form to assess its contribution to the predefined research objectives (see Appendix 2 for the complete extraction table).

To incorporate recent developments and contextual insights, additional sources were included. These consisted of two white papers published by ENISA in 2022 and 2024, as well as two gray literature reports: an industry report by Proofpoint (2023) and a governmental cybersecurity overview by the Estonian Information System Authority (RIA) in 2024. While these documents did not directly address the main research question or sub-research questions, they provided further context to the discussion, particularly regarding cybersecurity risks in the banking sector and the influence of human factors on organizational security posture.

The analysis evaluated how each study addressed human behavioral risks and the ways threat actors exploit OSINT. It also examined sector-specific exposures within the banking

industry and the practical integration open source intelligence into cybersecurity governance frameworks.

The findings of the systematic literature review highlighted two major research gaps. First, there is a limited body of research addressing OSINT related vulnerabilities specific to Estonia's banking sector. Second, while cybersecurity frameworks increasingly recognize the importance of human factors, practical methodologies for embedding OSINT findings into formal security governance remain underdeveloped. These identified gaps form the basis for the research problem addressed in this thesis.

6. Novelty and contribution

This thesis investigates OSINT-related risks within Estonia's banking sector, a critical infrastructure domain that has received limited attention in cybersecurity research. While previous studies have largely examined corporate environments or critical sectors such as energy [4, 25], this work specifically focuses on the financial sector in Estonia, offering a sector specific and national perspective.

Employee online activities, particularly on social media platforms such as LinkedIn, increasingly contribute to inadvertent exposure of sensitive information. Publicly available details about job roles, technical skills, or project involvements can create detailed digital footprints. Threat actors exploit these footprints to conduct targeted phishing attacks, social engineering, and broader corporate espionage activities. Although such risks have been conceptually acknowledged, systematic research in the context of Estonia's banking institutions remains limited.

Existing cybersecurity frameworks, including those developed by ENISA [8], the NIS2 Directive [26], NIST [10], and ISO standards, place significant emphasis on strengthening technical defenses, risk management, and incident reporting requirements. However, the adaptation of these frameworks to systematically address human behavior driven OSINT risks remains underdeveloped. While ENISA and the NIS2 Directive [26] recognize the human factor within risk management, specific recommendations targeting digital exposure through public platforms are scarce. Similarly, NIST and ISO frameworks address insider threats and security awareness but tend to treat OSINT related risks only implicitly, without defining them as a distinct and manageable risk category. As Henricks [27] argues, although social media and OSINT can significantly expand intelligence gathering capabilities, security frameworks are often slow to adapt in formally recognizing these tools' dual use nature both as enablers of intelligence and as exploitable vulnerabilities.

This study contributes to the field by identifying how employee behaviors create exposure vectors that are not yet fully captured in existing frameworks. The findings emphasize the need for cybersecurity policies that explicitly recognize open source intelligence as a distinct source of risk and propose adjustments for integrating OSINT based threat modeling into sector specific cybersecurity strategies. The research also provides practical recommendations tailored to Estonia's banking sector, supporting a more comprehensive and realistic approach to resilience building in critical infrastructure.

7. Research methodology

7.1 Methodology overview

This research adopted a qualitative methodology, using an OSINT-driven investigative approach combined with qualitative content analysis. The objective was to systematically collect publicly available information about employees of major Estonian banks, analyze patterns of data exposure, and assess potential vulnerabilities resulting from human digital behavior.

The study followed a structured process: data were collected through open source methods, coded into thematic categories, and analyzed for recurring patterns of sensitive information exposure. The credibility of the collected data was verified through triangulation, meaning that information was cross-checked across multiple independent sources. For example, an employee's role listed on LinkedIn was confirmed by reviewing corresponding Facebook posts or mentions on Instagram, and technical disclosures were validated through targeted Google Dorking queries. The thematic analysis was inspired by cybersecurity research practices where publicly available organizational data was organized into predefined categories such as job related disclosures, technical infrastructure exposure, and leakage of personal identifiers [2, 17]. Although thematic analysis traditionally applies to interviews, this study applied it to OSINT data by grouping evidence that different employees, sometimes directly or indirectly connected, posted or commented on, revealing consistent patterns. For example, multiple employees sharing posts mentioning internal tools such as ServiceNow provided grounds for identifying a theme of "technical infrastructure exposure."

This methodology ensures that data is systematically analyzed, patterns are objectively identified, and the findings are grounded in triangulated, credible sources.

7.2 Procedure

The structured OSINT profiling procedure involved five stages: (1) selection of platforms, (2) random selection of employee profiles across Swedbank, SEB, LHV, Coop Pank, and Luminor, (3) documentation of publicly accessible information, (4) categorization of the data according to thematic categories, and (5) triangulation for credibility.

The information collected included public job titles, role descriptions, and mentions of internal tools or technologies. It also covered disclosed certifications and skills, available work emails or phone numbers, and screenshots of public posts or digital environments where sensitive information was visible. Screenshots were only taken when information was publicly available, and all identifiable markers (such as names, faces, or emails) were blurred or masked to preserve anonymity.

Platforms selected for analysis included LinkedIn, Facebook, Instagram, X (formerly Twitter), TikTok, and GitHub, in line with prior studies identifying these platforms as common sources of employee information leakage in critical sectors [3, 28, 14, 1].

Google Dorking techniques were used to uncover indexed corporate information that may not be immediately visible on social profiles. Specific queries, such as `"Name Surname" "@bank.ee"`, `"Name Surname" "phone" site:bank.ee"`, or `"Name Surname" "+372" bank.ee"`, helped in locating corporate contact details and internal references accessible through search engines. These techniques mirror those used by threat actors, providing a realistic view of potential exposure without engaging in unauthorized intrusion.

Each finding was documented, classified, and when possible also validated by cross verifying data across at least two independent sources, ensuring consistency and mitigating bias.

7.3 Ethical considerations

The use of OSINT in cybersecurity research raises specific ethical and legal concerns, especially when analyzing publicly available personal data. This study was conducted under strict adherence to ethical principles: data minimization, transparency, and privacy preservation, fully aligned with the GDPR.

Only publicly available information was accessed; no social engineering, deception, or fake profiles were created. Information such as names, emails, and phone numbers, even if publicly visible, were anonymized or masked. Screenshots of profiles or posts were used selectively to illustrate findings, but all identifiable information was blacked out before inclusion.

Ethical discussions in the literature reinforce this approach. Henricks [27] emphasized that researchers must handle even public data responsibly, while Mitchell [13] warned about the thin line between ethical collection and invasive intelligence practices. DeCusatis et al. [2]

argued that ethical OSINT research should simulate attacker behavior without exceeding lawful and defensible boundaries, a principle strictly respected throughout this study.

7.4 Analytical approach

The analysis combined qualitative content analysis with thematic coding of collected OSINT data. The focus was on identifying patterns of sensitive information disclosure across employee profiles.

Each profile was assessed individually and then compared across the dataset to detect recurring exposure themes, such as disclosure of internal systems, job specific technical information, or personal contact data. Sensitive disclosures were classified into three risk levels: low-risk (general job titles), medium-risk (mention of internal platforms like Braze or ServiceNow), and high-risk (exposure of specific infrastructure tools or work contacts).

The data was organized according to these sensitivity levels to facilitate meaningful comparison between different banks and platforms. Cross bank analysis enabled the identification of which institutions and social media platforms exhibited greater vulnerabilities. The analytical method ensures systematic treatment of the data, following structured steps from coding to pattern identification. It also allows for replication in similar studies across different industries or national contexts.

7.5 Validation

Validation of findings was achieved through methodological triangulation and comparison with prior research in cybersecurity and critical infrastructure sectors. The exposure patterns identified mirrored those observed in earlier studies, particularly the work of Matvej, Morić, and Papić [3] on Croatian banking vulnerabilities and Lee and Shon [4] on energy sector reconnaissance through OSINT. Such similarities reinforce the credibility of the findings. Internal consistency checks were also performed: data categories were cross verified, and sensitive disclosures were checked for recurrence across independent sources. For example, the use of RabbitMQ at LHV Bank was independently validated by multiple employee posts.

This process supports the credibility of the answers to SRQ3 and SRQ4 and contributes empirical evidence for integrating OSINT vulnerability management into cybersecurity frameworks.

8. Results

8.1 Overview of data collected

This section provides an overview of data gathered from an open source intelligence investigation. The study focused on evaluating cases of unintentional corporate information exposure by employees in Estonia's banking sector from five major banks: Swedbank, SEB, LHV, Coop Pank, and Luminor. The analysis examined employees' digital footprints across a range of publicly accessible online platforms to identify behavioral and technical indicators that may facilitate cyber enabled threats.

In total, 184 employee profiles were examined across the following platforms: LinkedIn (184), Facebook (170), Instagram (128), Twitter/X (75), TikTok (57), and GitHub (4). The specific methods for profile collection and data gathering were previously detailed in Section 7.2. For each employee, publicly available information was collected and analyzed to detect patterns of information exposure.

Although GitHub is not traditionally considered a social media platform, it was included due to its relevance for technical project development and programming activity. Code repositories, even when not explicitly mentioning an employer, can indirectly expose internal technical standards, tool familiarity, or development frameworks.

Visual disclosures, such as screenshots displaying work environments, internal tools, or personal information leakage, were also identified during the investigation. An example of such a disclosure is shown in Figure 2, where an employee unintentionally exposed online meeting content with names of their colleagues and daily topic discussion on a public LinkedIn story.

Google Dorking techniques were applied to supplement the OSINT activity, supporting the retrieval of publicly accessible work contact details indexed on official websites and third-party platforms. As the methodology section explains, no subscription services or credential based access methods were used to maintain ethical compliance.

The results of the data collection indicated that LinkedIn was the most consistent and structured source of professional information. All 184 profiles were publicly accessible, providing information such as official job titles, departments, role descriptions, and in sev-

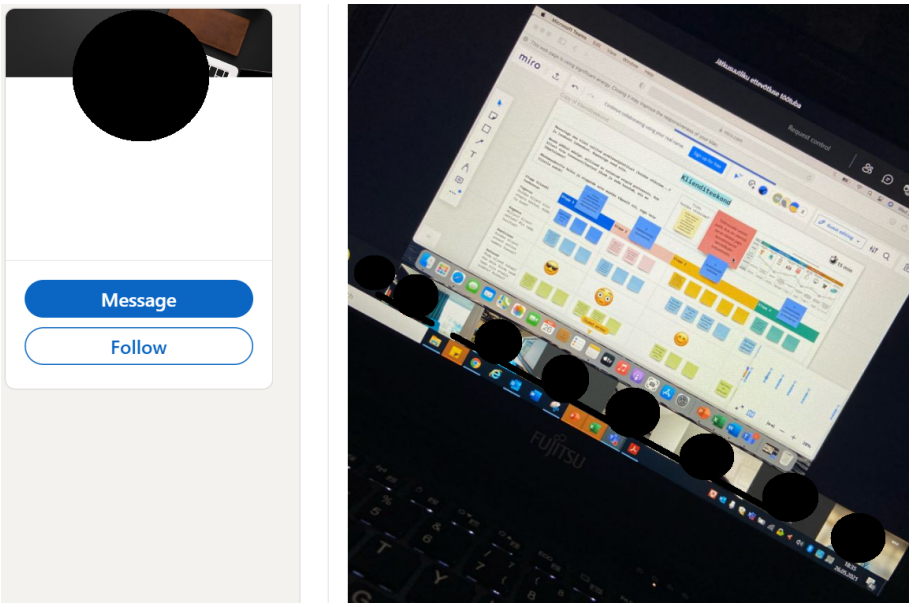

Figure 2. *LinkedIn story with exposure of employees info.*

eral cases, references to internal tools. This structured and standardized metadata leakage is particularly critical. It allows threat actors to map an organization's internal structure, identify key employees, and tailor phishing or social engineering attacks accordingly [7, 1].

Facebook represented the second most significant platform for OSINT exposure. Out of the 170 profiles identified, 159 were publicly accessible. Among these, 35 profiles confirmed workplace affiliation either through job related posts, comments, or visual contents, such as photographs of company environments, screenshots of internal communications, or promotional activities related to the employer. Figure 3 shows a work affiliation example. This data helped to verify information already collected on a specific employee, like the bank connection.

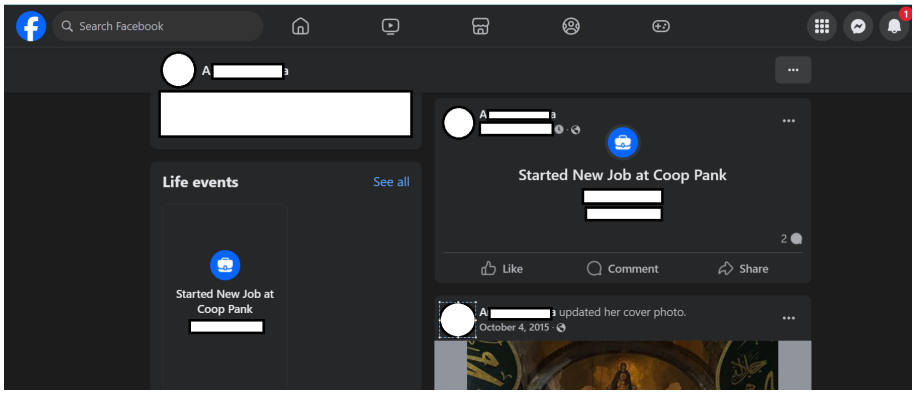

Figure 3. *Facebook profile with job affiliation info*

Instagram demonstrated relatively limited contribution to the dataset. While 128 employee

profiles were identified, only 38 profiles were publicly accessible. Moreover, the majority of Instagram content was unrelated to professional activities, focusing instead on personal interests, travel, or entertainment. This limited relevance is primarily attributed to the platform's default privacy settings and its social focus on personal rather than professional expression.

Similarly, Twitter/X and TikTok presented minimal relevance for OSINT exposure. Although 75 Twitter profiles (73 publicly accessible) and 57 TikTok profiles (36 publicly accessible) were identified, most of the content consisted of personal opinions, lifestyle posts, or entertainment material, with little to no references to work related activities. This finding aligns with the broader understanding that these platforms are less frequently used for professional disclosure in Estonia's banking sector.

GitHub was associated with four profiles, primarily belonging to software developers. This can be attributed to the platform's primarily technical nature, which narrows its use to specific professional profiles, such as developers or engineers. Additionally, the widespread practice of using pseudonyms on GitHub complicates the process of accurately mapping employee identities to their professional roles. The analysis of these 4 profiles and their public repositories, indicated that the projects were largely personal and did not explicitly reference their employers or workplace activities. Although GitHub can present a potential risk for corporate information disclosure, this study did not confirm such exposure in the examined cases. Furthermore, the overall presence of GitHub accounts among the 184 employees assessed was found to be very limited.

The findings from this comprehensive digital profiling activity suggest a consistent pattern of unintentional information disclosure across all five banks. LinkedIn metadata, Facebook visual content, and publicly indexed contact information together create a multi layered OSINT surface, which, if exploited, could provide threat actors with a detailed blueprint of organizational structures, technical environments, and employee networks.

8.2 Platform specific exposure pattern

This section analyzes the platform dependent nature of information exposure by employees in Estonia's banking sector. The objective is to understand how different social media platforms contribute to unintentional corporate data leakage and to evaluate the degree of risk associated with each. The findings in this section respond directly to **SRQ1** (How do threat actors exploit employee data from social media platforms?) and **SRQ2** (How do different social media platforms contribute to data exposure risks?).

The exposure patterns observed were shaped by the platform's core function, user behavior, and privacy settings. While all platforms surveyed can pose some level of risk, their potential for organizational harm varies significantly depending on the nature of information disclosed.

8.2.1 LinkedIn: structured professional disclosure

Among all platforms examined, LinkedIn demonstrated the highest potential for OSINT exploitation. All 184 employees analyzed had publicly accessible LinkedIn profiles. These profiles consistently included full names, job titles, departments, project responsibilities, and in some cases, technical competencies and internal tools. For instance, some profiles referenced technologies such as ServiceNow (2 mentions), RabbitMQ (2 mentions), or Braze (1 mention), all of which can be interpreted as indicators of internal infrastructure.

The public mention of these tools is particularly concerning. When attackers gain insight into an organization's technology stack, they can tailor reconnaissance efforts to identify known vulnerabilities, simulate phishing emails that reference internal tools, or plan targeted attacks. For example, if an attacker learns that a bank uses RabbitMQ, a system for managing internal message flows they can look for known software vulnerabilities to exploit. One such vulnerability, documented as Common Vulnerabilities and Exposures CVE-2025-30219, demonstrates how attackers could inject malicious code into the RabbitMQ management interface and trigger it through the browser of a system administrator [29]. This could allow the attacker to run unauthorized commands, gain access to sensitive functions, or manipulate the system's behavior using only a carefully crafted name string. Such weaknesses highlight how even small pieces of metadata can assist adversaries in launching precise and harmful attacks.

These metadata disclosures also enable social engineering through trust exploitation. As explained by Hayes [1], LinkedIn is widely used by threat actors to build trust and impersonate legitimate roles within companies. Capano et al. [7] further highlight that adversaries collect LinkedIn data to identify high value targets and organizational hierarchies for Business Email Compromise (BEC) attacks. The combination of structured professional metadata and publicly visible connections facilitates such threat actor activity.

Beyond text disclosures, visual elements also increased risk. Some LinkedIn stories and posts contained workplace photos or screenshots that revealed internal layouts, desks, and visible screens. These seemingly benign images can offer adversaries contextual intelligence, such as identifying the type of operating systems used, internal communication tools, or names of employees displayed on screen. One anonymized example is shown in

Figure 4, which illustrates the kind of internal environment exposure observed during the analysis.

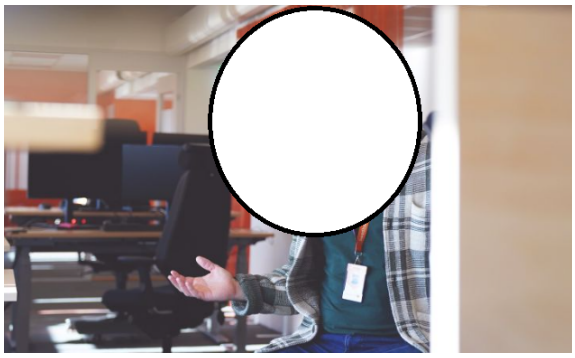

Figure 4. *LinkedIn story from an Estonian bank office. Computer stations and access badge visible, but not readable.*

8.2.2 Facebook: personal affiliated disclosure

Facebook posed a more modest, yet distinct OSINT risk due to its personal and visual content format. Out of 170 identified profiles, 159 were publicly accessible. In 35 of these, employees confirmed their workplace either through explicit job titles, affiliation mentions, or shared content related to their employer, including office events and job promotion posts.

While Facebook was not the primary source of technical disclosures, it served a critical role in validating identity and workplace connections. For example, multiple employees were observed promoting internal job openings or sharing branded material, indirectly confirming their team membership or department alignment. In some cases, the same individuals were also listed on LinkedIn, allowing cross platform triangulation of their role.

Visual disclosures included photos taken during office visits, team celebrations, or social activities. Figure 5 presents one such case, where SEB hosted a public event and employees shared group images within the office environment. Though seemingly benign, such content can reveal the spatial layout of workspaces, meeting areas, or even IT setups, which may be useful to adversaries conducting reconnaissance.

Notably, Facebook disclosures had a more personal nature. Although it was outside the scope of this thesis to process personal information, a number of profiles disclosed private phone numbers, secondary email addresses, and details about side jobs or freelance roles. While these data points were excluded from analysis to maintain ethical boundaries, it is important to acknowledge that such information increases the attack surface. Threat

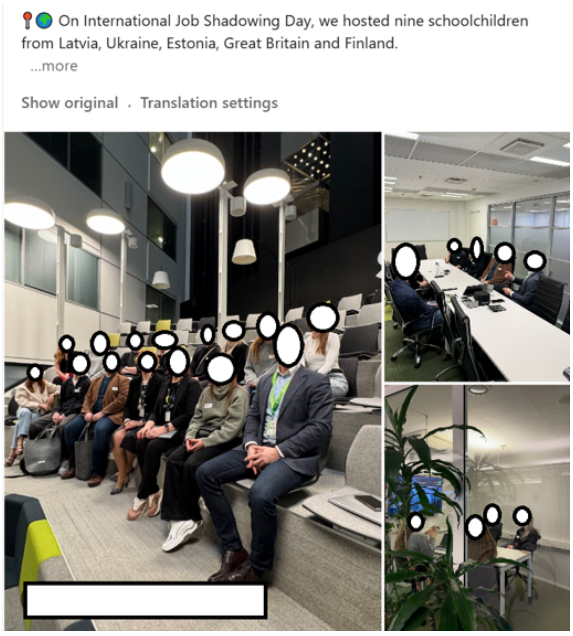

Figure 5. *Facebook post showing a company event, revealing internal office layout and employee group*

actors could use these additional identifiers for spear phishing, targeted phishing attacks aimed at specific individuals. Leveraging personal information such as phone numbers or email addresses found on social media, enable attackers to craft convincing messages that appear legitimate. The risk is an increasing likelihood of the victim disclosing sensitive information or clicking on malicious links.

While Facebook was not a major source of technical OSINT in this study, it contributed significantly to **SRQ1** (how threat actors exploit social media data) and **SRQ2** (how different platforms contribute to data exposure). Specifically, it validated job affiliation and revealed personal identifiers that, although ethically omitted here would likely be leveraged by adversaries targeting individuals within critical industries like banking.

8.2.3 Instagram: limited but contextual exposure

Instagram was associated with 128 employee profiles, but only 38 were publicly accessible. The platform played a minimal role in the exposure of professional information, as the majority of its content was unrelated to workplace settings. Most posts revolved around lifestyle, food, travel, or hobbies. The low risk level here is attributed both to privacy settings and the informal use of the platform.

8.2.4 Twitter/X and TikTok: minimal organizational relevance

Both Twitter/X and TikTok were found to be the least relevant in the context of professional exposure. While 75 Twitter accounts (73 publicly accessible) and 57 TikTok profiles (36 public) were identified, almost none included job related content. The type of posts found on these platforms focused on news commentary, humor, or personal entertainment, reflecting minimal engagement with professional identity. Their low value for OSINT purposes in this context is generated from the absence of both job related discussions and interlinkage with the employees' banking roles.

8.2.5 GitHub: technical fingerprints without employer disclosure

GitHub was linked to only 4 of the 184 employees analyzed. These were mostly developers who shared open source projects or code snippets. No explicit mention of the employer was made, and most repositories used pseudonymous or nickname based profiles. However, technical tools and coding frameworks were observable, which could hypothetically offer indirect insight into an organization's development practices or infrastructure stack. For example, repeated use of specific frameworks or libraries could hint at enterprise standards. Still, due to the low frequency of occurrence and limited identifiability, the overall risk was classified as moderate.

8.2.6 Summary of platform specific exposure pattern

The comparative analysis confirms that OSINT risks are not evenly distributed across platforms. LinkedIn poses the highest organizational risk due to structured disclosures of technical and professional metadata. Facebook follows closely, enabling personal affiliation risks and unintended workplace visibility. Instagram, Twitter/X, TikTok, and GitHub represent lower or context dependent risks, either due to privacy configurations, content irrelevance, or limited platform use.

This platform specific variation answers **SRQ2**, showing how each platform's design and user behavior shape data exposure differently. It also helps answer **SRQ1**, illustrating how threat actors may combine metadata from LinkedIn and social narratives from Facebook to create persuasive phishing pretexts, impersonation attempts, or infrastructure mapping.

A tabular classification of these platforms is presented in Table 1.

Table 1. *Platform-specific OSINT risk classification*

Nr	Platform and common data leaked	Risk level
1	LinkedIn – Job roles, internal tools, work emails, certifications, organizational structure	High
2	Facebook – Identity linkage, job confirmation, visual content (e.g., screenshots, photos)	High
3	GitHub – Technical code repositories, development preferences, indirect enterprise signals	Medium
4	Instagram – Primarily private or unrelated lifestyle content	Low
5	Twitter/X – Inactive or non-professional profiles; no corporate content observed	Very low
6	TikTok – Entertainment-focused content; no job-related exposure observed	Very low

8.3 Bank specific exposure overview

This section presents a comparative analysis of OSINT findings organized by institution. While the previous section analyzed how platform specific features impact disclosure, this section shifts the analytical focus to the organizational level. It aims to uncover which institutions exhibited higher levels of exposure, the nature of the information disclosed, and any recurring employee behaviors that may contribute to OSINT risks. In line with the research aim, the findings are contextualized with industry specific cybersecurity recommendations, particularly from ENISA and NIST, to understand their practical implications and threat exposure.

8.3.1 Swedbank

Swedbank holds a central position in Estonia's financial infrastructure and plays an important role across the Nordic-Baltic region, serving over 900,000 private and 131,000 corporate clients in Estonia alone [21]. Given its scale and criticality, the bank represents a high-value target for adversaries engaged in digital reconnaissance. The present investigation uncovered multiple layers of unintentional exposure resulting from employee online behavior, highlighting the potential exploitation vectors threat actors can leverage through publicly available information.

A sample of 35 LinkedIn profiles revealed job titles, departmental affiliations, and internal tool references. For example, ServiceNow was explicitly mentioned by employees in

two Swedbank profiles. While this may seem innocuous, it enables attackers to tailor exploits to known vulnerabilities associated with the platform. One confirmed vulnerability affecting ServiceNow, documented as CVE-2024-8924, involved a blind SQL injection flaw in the Now Platform. This type of vulnerability could allow a remote attacker with no login access to extract sensitive information from the system's database. Because the attacker does not need to be logged in, the risk is particularly high if a ServiceNow instance is exposed online. This illustrates how knowledge of internal tool usage, such as ServiceNow, can encourage adversaries to search for known vulnerabilities and address targeted attacks [30]. The mention of such enterprise service management tools, also helps threat actors to map internal environments. For instance, if attackers know ServiceNow is used, they may tailor spear phishing emails to impersonate IT support and deploy payloads mimicking support ticketing systems [31].

Additionally, 22 of the 35 employees had public Facebook accounts. Among them, four explicitly linked their profiles to Swedbank, and one user cross referenced LinkedIn and Facebook profiles. This detail facilitates identity confirmation and increases risk of impersonation. A particularly concerning disclosure included a screenshot of a professional certification which visibly contained the individual's national identification number. This finding, is not work related, so it cannot be identified as a corporate information leakage. However, this PII if not redacted, can be exploited for identity theft and credential stuffing attacks, as emphasized in ENISA's guidelines on personal data protection [8].

Google Dorking further supported the collection of additional data. Through queries such as `"Name Surname" "@swedbank.ee"`, `"Name Surname" "phone" site:swedbank.ee`, and `"Name Surname" "+372" swedbank.ee`, work email addresses and phone numbers of seven employees were discovered. This information was retrieved from public websites, primarily the official bank website, but also from other publicly accessible sources where digital footprints had been left. Initially, this exercise aimed to identify personal information through publicly available social media accounts; however, no work related emails or phone numbers were found on those platforms. NIST [10], referring to Access Control family (AC) recommend to limit external access to sensitive contact directories.

8.3.2 SEB Estonia

SEB Estonia, serving approximately 750,000 customers and employing over 1,000 individuals [22], showed a more conservative data exposure pattern.

All 35 selected LinkedIn profiles were public and detailed in job role information, though

none mentioned internal tools. Facebook activity was similarly high, with 31 public profiles and nine confirming SEB employment through posts or intro sections. One employee publicly displayed their work email address, directly increasing the risk of phishing or impersonation, a tactic often used in BEC attacks [31].

While no technical tools or internal systems were referenced directly, work contact information was identified for five employees using Google Dorking techniques. This technique supported the discovery of publicly accessible work related data. The following queries supported the research of emails and phone numbers within SEB employees, across official web pages and third-party sources: `"Name Surname" "@seb.se"`, `"Name Surname" "phone" site:seb.se`, and `"Name Surname" "+372" seb.ee`.

Despite the absence of tangible evidence related to the disclosure of technical details, the presence of publicly linked contact information still presents a significant risk in OSINT-based information gathering activities.

8.3.3 LHV Bank

LHV, one of Estonia's fastest growing banks with over 400,000 clients and more than 1,000 employees [20], was represented in this analysis by 38 employee profiles, through which several instances of technical disclosure were identified.

In one case, a public LinkedIn post featured a computer screen with project details, shown in Figure 6. Luckily, no information was disclosed due to the poor resolution of the picture. But, for these specific cases the risks of information leakage can be potentially high. Another employee mentioned a technical infrastructure migration from ActiveMQ to RabbitMQ (Figure 7). While this post may have been shared to showcase career progress, it inadvertently reveals information about backend system architecture. As explained in the previous section on LinkedIn disclosures, RabbitMQ has been associated with recent documented vulnerabilities, including CVE-2025-30219, which could enable attackers to execute malicious code in administrator browsers via the management interface. Even without direct exploitation, such disclosures provide reconnaissance value by revealing integration dependencies or possible misconfigurations that adversaries could further investigate.

Two LHV employees had GitHub accounts, but no direct employer references were found. On Facebook, 33 employees had public profiles, and 11 confirmed their employment with the bank. Contact data from six employees was extracted via Dorking, using queries such as

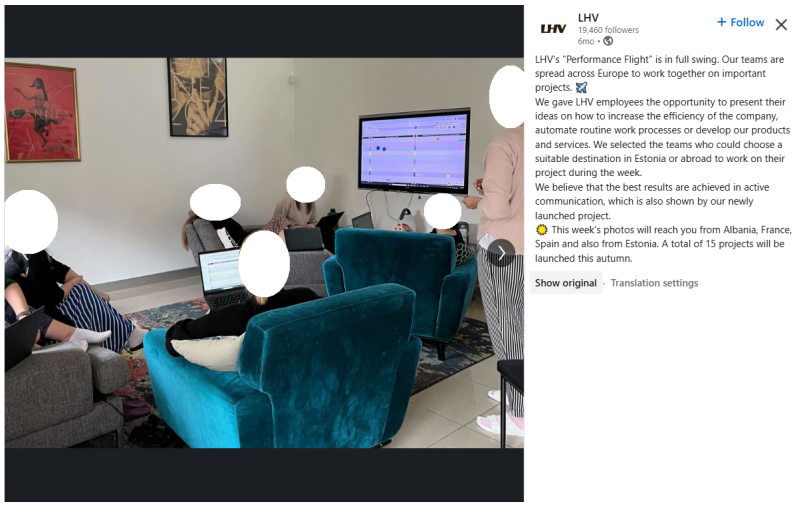

Figure 6. *Project related story on LinkedIn*

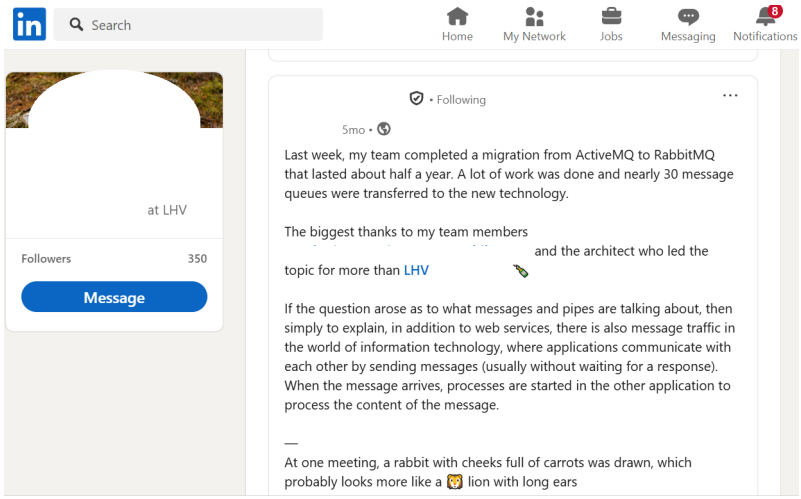

Figure 7. *A LinkedIn story with RabbitMQ tool disclosure*

`"Name Surname" "@lhv.ee"`, `"Name Surname" "phone" site:lhv.ee`, and `"Name Surname" "+372" lhv.ee`. These queries helped with the identification of six email addresses and five phone numbers.

LHV's OSINT exposure suggests a moderate to high risk, particularly due to disclosed technical migration data. As highlighted by NIST [9], detailed infrastructure discussions should be limited in public forums to avoid aiding threat modeling efforts.

8.3.4 Coop Pank

Coop Pank, which provides banking services through digital platforms and over 300 retail store branches across Estonia [23], was represented in this investigation by 40 employee profiles. Among these, the most prominent risks originated from technical disclosures and the sharing of visual content containing potentially sensitive information.

One employee publicly shared multiple stories about virtual meetings, unintentionally exposing internal interfaces and the names of team members. This can be considered a personal data leakage. However, this picture relates to a prior period when employed to another Estonian bank (Figure 8). Another employee explicitly mentioned the use of Braze, a customer engagement platform, offering insight into Coop Pank's marketing technology stack. Among the 40 profiles reviewed, 39 had publicly accessible Facebook profiles. None of them also disclosed their current employment status over this social media platform.

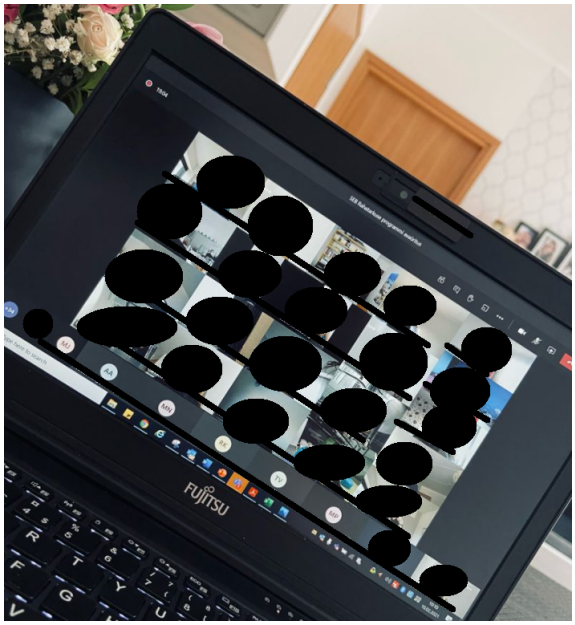

Figure 8. *Story related virtual meeting on LinkedIn*

Disclosing the use of tools like Braze can inadvertently aid attackers by revealing customer interaction strategies and backend integration points. As highlighted in ENISA's threat landscape overview [8], such information is often leveraged to design impersonation schemes or injection attacks.

Google Dorking revealed six emails and five phone numbers, mostly published on official and external websites like ebrd.com. The queries used included `"Name Surname" "@cooppank.ee"`, `"Name Surname" "phone" site:cooppank.ee`, and `"Name Surname" "+372" cooppank.ee`. One employee's work email was found through Facebook, an example of cross platform data convergence that adversaries exploit for triangulation attacks.

8.3.5 Luminor Bank

Luminor, with headquarters in Tallinn and operations across the Baltics, demonstrated the lowest OSINT exposure among the five banks analyzed [32].

All 36 employees screened had public LinkedIn profiles with role related information. Only two Facebook profiles showed employment affiliation, indicating a cautious social media presence. No internal tools, screenshots, or technical data were identified in this sample. Despite this, Google Dorking retrieved nine work emails and one phone number. The queries used included `"Name Surname" "@luminor.ee"`, `"Name Surname" "phone" site:luminor.ee`, and `"Name Surname" "+372" luminor.ee`. These details were associated primarily with public facing roles such as customer support. While minimal, this exposure still highlights the value of basic contact data for initial stage phishing operations.

8.3.6 Institutional exposure trends

The investigation into employee digital footprints revealed varying degrees of information exposure across the five Estonian banks assessed. The analysis of 184 profiles shown that LinkedIn was used as the central source of professional metadata, while Facebook and Google indexed content extended the visibility of personal and work related identifiers. Google Dorking techniques allowed the discovery of contact details, such as emails and phone numbers, openly available on official bank websites or third-party platforms. This info was collected without bypassing any access restrictions or subscription barriers. Although some platforms offered extended data in exchange of a monthly payment (e.g., Aeroleads.com or Rocketreach.co), these were excluded from the research scope to maintain adherence to publicly accessible information only.

The institutional comparison reveals varying degrees of OSINT-related vulnerability. Swedbank and LHV were associated with the highest levels of technical and contact data exposure, suggesting elevated infrastructure mapping risks. Coop Pank instead, presented visual content risks, especially from legacy content tied to previous employment. SEB maintained moderate disclosure levels, mostly tied to identity confirmation and contact exposure. Luminor had the lowest behavioral and technical exposure, aligning with best practices for OSINT containment.

These findings reinforce the need for continued attention to OSINT-related risks within Estonia's banking sector. This is especially important considering the critical role these institutions play in national infrastructure and their responsibility for safeguarding sensitive financial data. The research demonstrates that even in digitally mature organizations, employee-driven exposure remains a significant cybersecurity challenge. The combination of individual platform behavior and the institution's internal communication culture directly influences the extent to which sensitive information becomes publicly accessible.

9. Discussion

9.1 Purpose and scope of analysis

The primary purpose of this chapter is to critically interpret and contextualize the findings presented in Chapter 8. The objective is to analyze how employees' online behaviors contribute to the unintentional exposure of corporate data within Estonia's banking sector. The study, conducted using non intrusive OSINT techniques, has generated empirical evidence that reflects real world reconnaissance practices. These types of activities are also commonly employed by threat actors during the early stages of cyber operations. Within this context, the data collected through social media analysis and publicly available websites is not only informative. But, it also raises awareness and prompts security measures when it becomes clear that such vulnerabilities could be exploited for pretexting, phishing, or broader forms of corporate espionage.

The scope of the discussion focuses on four key areas, each corresponding to the sub-research questions: (1) exploitation tactics used by threat actors, (2) platform specific risks, (3) the unique risk landscape of Estonia's financial sector, and (4) the integration of OSINT risks into existing cybersecurity frameworks. The discussion also aims to provide a comprehensive interpretation of the MRQ, which investigates the role of human behavior in the unintentional leakage of sensitive organizational information.

The combination of the results generated from this OSINT activity together with the relevant academic literature and current cybersecurity practices, helps to have a deeper understanding of this problem. Moreover, it offers insight into mitigating strategies, and evaluates the implications for both policy and practice within critical infrastructure environments. The scope of this chapter is to address this discussion and address the questions proposed in Chapter 3.

9.2 Human behavior and the role of digital exposure (MRQ)

The main research question of this thesis, *"What role do human factors play in the unintentional exposure of corporate data across critical industries?"*, is addressed through the analysis of 184 employee profiles across five major Estonian banks. The data reveals that human digital behavior is a fundamental enabler of OSINT vulnerabilities, particularly when professional metadata and personal content converge across multiple public

platforms.

The evidences collected from this OSINT activity reveal a consistent behavioral pattern where employees disclose their roles, responsibilities, tools in use, and in some cases, internal processes or visual content. These disclosures are rarely malicious but are generated from a lack of awareness about the implications of publicly sharing work related information. According to Capano [7] and Hayes and Cappa [1], such digital footprints become vectors of exploitation in the hands of adversaries capable of aggregating data from multiple public sources. For instance, if an employee publicly lists "IT Support Specialist using ServiceNow" on LinkedIn and shares their work email on another platform, an attacker could create a spear phishing email mimicking a support ticket. This email could exploit known CVEs in the ServiceNow platform [33] to trick the employee into granting access or downloading a malicious payload. Similarly, public congratulations on internal tool migrations, as seen in LHV Bank, could guide an attacker to tailor infrastructure specific attacks using messaging queue vulnerabilities.

This study helped validate the hypothesis that human behavior, especially while using platforms like LinkedIn and Facebook, contributes to an unintended increase in an organization's attack surface. Considering that technical systems may be well defended, employees' online activity continues to present exploitable entry points. This has been demonstrated by incidents such as the 2020 SolarWinds campaign, where attackers gained access to the SolarWinds Orion Platform. This was possible through reconnaissance activity and collection of information on SolarWinds and their clients, eventually stealing authorized credentials [34]. This case scenario prove that publicly available employee information on social media can be used by malicious actors to identify targets within organizations, and craft spear phishing emails, for example to escalate access. Additionally, Proofpoint's 2023 report shows that over 84% of targeted phishing attacks leveraged social media data to personalize attacks, particularly focusing on job roles and tool mentions [31]. These cases emphasize that cybersecurity risks are no longer limited to systems and software but are increasingly shaped by human driven exposure in digital environments.

9.3 Adversarial use of publicly available employee data (SRQ1)

The first sub-research question *"How do threat actors exploit employee data from social media platforms?"* was also addressed in this study. It was examined from a threat actor's perspective through the simulation of the profiling phase of a cyber attack using OSINT techniques. The information gathered reveals that publicly accessible employee profiles are a significant source of intelligence that adversaries can use to study organizational hierarchies, key operational tools, and potential entry points.

Threat actors can exploit professional metadata to address convincing phishing or pre-texting campaigns, particularly when a profile reveals both the employee's role and the technologies they interact with. For example, references to tools such as ServiceNow, RabbitMQ, or Braze on LinkedIn enable threat actors to design highly specific attacks that replicate internal communications, such as fake support ticket notifications or system migration alerts. Or, knowing from publicly available information that a specific bank uses certain tools, a threat actor could leverage known vulnerabilities (e.g ServiceNow CVEs [33]), to craft an attack.

Additionally, the availability of work email addresses and phone numbers, obtained through Google Dorking and indexed web content constitutes a significant channel for adversary engagement. These contact details, often found on official bank websites or project documentation, enable attackers to bypass generic communication channels and target individuals with high precision. According to Yadav, Kumar, and Singh [28], contact information combined with organizational metadata can result in targeted attacks that are difficult to detect through conventional security measures. For example, a threat actor who gathers an employee's job title, department, and verified work email address can craft a spear phishing message that impersonates internal communication, such as an urgent request from a department head. BEC attacks rely heavily on this type of metadata; once the attacker identifies finance or HR staff and their reporting lines, they can send tailored emails requesting invoice payments or payroll changes. These threats are not theoretical. Estonia's Information System Authority (RIA) reported an increase in targeted social engineering campaigns in 2023, including impersonation attacks and payment diversion scams aimed at organizations in both the public and private sectors [35]. These incidents demonstrate how employee information, gathered through social media or open directories can be systematically exploited by threat actors.

The data confirms that publicly exposed employee information not only contribute with the information gathering process but also accelerates the weaponization of tailored attack vectors.

9.4 Platform specific risk landscape (SRQ2)

The second sub-research question *"How do different social media platforms contribute to data exposure risks?"* was addressed in Chapter 8 during the comparative analysis of six digital platforms: LinkedIn, Facebook, Instagram, GitHub, Twitter/X, and TikTok. Every single platform provide a different layer of risk exposure from high to very low that highly depend on user behavior, platform design, and privacy settings.

LinkedIn proved to be the most critical platform for OSINT related exposure. All 184 profiles reviewed were publicly accessible and included clearly described job titles. In most cases, departmental affiliation was also identifiable, often associated with interactions such as comments and reactions that revealed connections to colleagues or close peers. Several profiles featured images capturing the work environment. In a smaller number of cases, profiles included references to internal tools, professional email addresses, or visual content displaying projects and employee names. Due to the platform's structured professional format, high visibility, and the widespread public accessibility of the profiles reviewed, LinkedIn operates as a single point reference for organizational mapping. As also highlighted by Bizouarn et al. [14], LinkedIn data, combined with employee publications, open directories, or social media links enabled the authors to map organizational structures and identify technical infrastructure based on job titles, skill sets, and tool mentions. This confirms the findings in the current research, where Estonian banking employees on LinkedIn revealed structured professional metadata, internal tools like ServiceNow and RabbitMQ, and interlinked content that created a similar attack surface. Bizouarn et al. [14] developed an automated OSINT tool that aggregates data from open platforms like social media, GitHub, and company websites, then applies machine learning to detect organizational vulnerabilities. Their work demonstrates how publicly accessible digital traces can reveal exploitable insights, particularly when employees disclose technical tools or personal metadata across platforms. While their tool primarily supports vulnerability detection, the study highlights how such data, when systematically collected, may aid in threat modeling efforts.

Facebook also contributed to the exposure of information, particularly through personal and visual content. Although less structured than LinkedIn, it remains widely publicly accessible. Among the 184 profiles analyzed, 170 had an identifiable Facebook account, and 159 of them (approximately 94% of the identified Facebook users) were publicly accessible. These profiles frequently confirmed employment affiliations and occasionally showcased work related images capturing the office environment or shared professional events. In a limited number of cases, Facebook also revealed work email addresses, either within static posts or temporary content such as stories. According to Hayes and Cappa [1], the presence of PII about employees on social media enables adversaries to reconstruct organizational hierarchies and determine internal workflows. This is especially dangerous when job roles, contact information, and platform linkages are disclosed across multiple sources. The 2020 SolarWinds breach, attributed to the APT group "Nobelium" (also known as APT29), involved a supply chain compromise where attackers inserted malware (SUNBURST) into updates for the Orion network monitoring platform. Before launching this sophisticated campaign, the threat actors reportedly engaged in extensive reconnaissance, including the analysis of employee social media profiles. These were

used to identify system administrators and IT staff, whose credentials were later targeted through spear phishing. Once inside, attackers gained persistent access to internal systems of over 18,000 organizations, including U.S. federal agencies and Fortune 500 companies. The breach led to widespread policy reviews and highlighted the critical role of OSINT in pre-compromise reconnaissance [34]. Open source intelligence can be instrumental in these specific cases for an attacker's information gathering phase, helping them identify individuals with access to critical systems. Similarly, in this study, employees' use of Facebook and LinkedIn enabled the confirmation of workplace affiliation, internal tools, and even personal identifiers, which could be used for targeted impersonation or lateral movement planning. Such information can potentially be used to compromise individual workstations through social engineering tactics. The hybrid nature of the platform, where personal and professional identities often intersect, makes Facebook, like LinkedIn, particularly exploitable for visual and relational OSINT.

Platforms such as GitHub revealed minimal exposure overall but still presented potential for insight into the technological environments of technical staff. The small number of developers using GitHub were not explicitly tied to their employers, but their code repositories may reflect the technology stacks familiar to banking institutions, adding value for attackers performing long term infrastructure mapping.

Conversely, Instagram, Twitter/X, and TikTok played a negligible role in corporate data disclosure. Most of the identified profiles were either inactive or used for non professional purposes. This supports the risk classification summarized in Table 1, where LinkedIn and Facebook were rated as high risk, GitHub as medium risk, and the remaining platforms as low to very low risk.

This analysis supports the argument that social media based OSINT risks are not uniformly distributed but instead platform specific, necessitating differentiated mitigation strategies.

9.5 Contextual OSINT risks in the Estonian banking sector (SRQ3)

The third sub-research question (SRQ3), *"What are the specific OSINT risks for the banking sector in Estonia compared to other industries?"*, is addressed by contextualizing the findings within Estonia's digitally advanced financial ecosystem. Estonia's strong national digital identity framework, reliance on e-governance infrastructure, and a highly interconnected banking sector contribute to an environment where OSINT related vulnerabilities are particularly significant.

Compared to findings from other regions, such as the Croatian banking sector analyzed by

Matvej, Morić, and Papić [3], Estonian banks exhibit a more digitally mature exposure landscape. The level of a country's digital advancement plays a significant role in determining its exposure to OSINT based information gathering. According to this assumption, Akın [18] highlights that digital proliferation, characterized by the widespread use of social media, interconnected platforms, and Internet of Things (IoT) devices, exponentially increase the amount of behavioral and organizational data that becomes available in the public domain. As Akın notes, digitally advanced societies produce more granular, exploitable data, enabling both state and non state OSINT analysts to access vast and continuously growing pools of behavioral information [18]. This reinforces the argument that nations like Estonia, recognized for their digital governance face disproportionately higher risks of OSINT reconnaissance compared to the least digitalized countries. This is further evidenced by the strong culture of online engagement, particularly the widespread digital presence of employees and the frequent use of professional networking platforms.

Although the internal social media or OSINT policies of Estonian banks are not publicly disclosed, this thesis includes a direct inquiry sent to RIA, the national cybersecurity authority. In their written response, received via email on April 16, 2025, RIA confirmed: "We do not currently have any banking-specific OSINT activities" in place. This clarification supports the conclusion that current sectoral governance does not sufficiently address human driven information exposure and highlights a significant oversight in addressing OSINT-related vulnerabilities in Estonia's financial sector.

This institutional gap highlights the relevance of the findings in this study. The absence of explicit OSINT policy guidelines leaves responsibility for risk mitigation largely in the hands of individual organizations. Without sector specific frameworks, the pervasive use of platforms like LinkedIn increases the attack surface for reconnaissance. As shown through the OSINT findings in Chapter 8, many employees share metadata, project milestones, and references to internal tools that could support adversarial targeting. This study therefore emphasizes the need for organizations to proactively define internal communication boundaries and adapt existing cybersecurity frameworks to reflect real world human behavior.

The risks observed within Estonia's banking sector are demonstrated by recurring patterns such as cross platform identity linkage, public disclosure of job related details, and widespread availability of indexed contact information. In particular, Swedbank, LHV, and Coop Pank exhibited higher levels of OSINT exposure due to references to internal tools, mentions of enterprise technologies, and public facing visual content showing workplace environments. These behaviors, though often underestimated, can provide actionable intelligence for malicious actors engaged in reconnaissance, infrastructure profiling, or

targeted spear phishing campaigns [2].

However, when comparing Estonia's case with similar research conducted in Croatia [3], key differences emerge. The Croatian banking sector showed a higher prevalence of basic contact information disclosure (e.g., emails and phone numbers), often lacking references to internal tools or technologies. Estonian banks, by contrast, are more digitally advanced and operate in a mature e-governance context, which promotes online transparency and professional visibility. This digital maturity leads to more complex forms of OSINT exposure, not just contact data, but layered disclosures that include internal system references.

While both countries show that employee behavior is a contributing factor to information leakage, the Estonian context amplifies the risk through its digital culture and the high volume of online professional engagement. The data generated by Estonian employees is richer and more multidimensional, making it easier for attackers to construct detailed threat models. Therefore, Estonia's exposure is not merely a matter of quantity, but of qualitative depth, and that presents a more serious challenge for threat mitigation.

The findings do not suggest that the banking sector is uniquely vulnerable due to employee behavior alone. Rather, the results point to a risk landscape shaped by the convergence of professional digital engagement and sector specific operational visibility. The cumulative evidence reinforces that, as with other critical infrastructure sectors, the financial industry must remain vigilant against OSINT driven threats. As emphasized by Lee and Shon [4], industries of strategic importance require proactive cyber threat inspection frameworks to anticipate and counter adversarial activities.

Estonia's advanced digital environment demonstrates both innovation and efficiency but also introduces a significantly expanded OSINT attack surface. This duality highlights the pressing need for a consistently high security posture, supported by robust employee cyber hygiene practices. Considering that Estonian banks manage highly sensitive financial and personal data, the overlap between employee digital activity and organizational visibility necessitates a proactive mitigation strategy. Awareness initiatives, particularly concerning social media use, should be prioritized. This is consistent with ENISA's recommendations for critical infrastructure sectors, which emphasize the human element as a persistent vector for targeted cyberattacks [8].

9.6 Framework adaptation and the integration of OSINT (SRQ4)

The final sub-research question (SRQ4), *"How can cybersecurity frameworks be adapted to mitigate OSINT risks in specific industries?"*, addresses the gap between established

cybersecurity standards and the practical challenges posed by human-driven information exposure. Security frameworks such as ISO 27001 and the NIST Cybersecurity Framework, can provide strong guidance on technical controls. However, such frameworks lack of specific controls regarding publicly available information leakage. This is particular evident when leakage is generated by employee behavior and digital footprints.

In the context of the NIST SP 800-53 framework [10], although OSINT is not directly addressed, several control families can be adapted to mitigate human driven exposure. A particularly relevant one is the Awareness and Training (AT) family, which outlines how to develop a security conscious workforce capable of recognizing and avoiding behavior that could lead to unintentional data disclosures. This family emphasizes education and targeted awareness activities, especially for individuals in high-risk roles. Controls such as AT-2 (Literacy training and awareness) promote general knowledge about the risks of metadata exposure and improper use of public platforms. AT-3 (Role-based training) provides tailored instruction for sensitive positions, such as executives or system administrators, who are more likely to be targeted in OSINT reconnaissance. AT-4 (Training records) ensures these efforts are measurable and maintained over time. Since many OSINT risks arise from casual digital engagement or poor social media practices, this control family offers an actionable starting point for risk mitigation aligned with recognized international standards.

As introduced earlier, the Personnel Security (PS) control family from NIST SP 800-53 includes mechanisms to manage insider risk and external exposure [10]. For instance, PS-6 (Access Agreements) and PS-7 (External Personnel Security) help define expectations and enforce compliance among both staff and contractors regarding data sharing, online conduct, and social media use. These controls play a preventive role in managing behavioral risks associated with public digital footprints.

From a technical perspective, the System and communications protection (SC) family includes SC-12 (Cryptographic key establishment) and SC-28 (Protection of information at rest). Both of these controls help preventing the leakage of sensitive data, including files unintentionally shared on public platforms or code repositories such as GitHub.

Building on the principles introduced earlier, the Risk Assessment (RA) control family offers key support for OSINT related risk monitoring [10]. Specifically, RA-3 (Risk Assessment) enables organizations to evaluate how public digital footprints, including work related emails, system references, or visual project indicators may expand their external attack surface. This allows the integration of OSINT visibility into existing risk models and helps to prioritize response efforts. RA-5 (Vulnerability Monitoring and Scanning) further

complements this approach by extending monitoring capabilities to passive reconnaissance techniques, such as Google Dorking. Although traditionally associated with technical scans, this control can be interpreted to include OSINT based methods, thus encouraging institutions to proactively audit their publicly accessible information before it is exploited by adversaries.

Furthermore, the Planning (PL) family can also address OSINT concerns. PL-4 (Rules of behavior) may be adapted to define social media use policies and outline expected online behavior. This control ensures staff to understand the implications of sharing work related details.

The overall maturity of an institution, when evaluated through NIST, would depend on how comprehensively it adopts and integrates these controls into daily operations and governance practices.

Currently, the Estonian Information System Authority does not offer banking specific guidance for mitigating OSINT related threats. This absence reinforces the relevance of this research and highlights a gap in sector specific cybersecurity governance. Based on the empirical findings, the most prominent vulnerabilities arise from employee driven disclosures, such as the mention of internal tools, publication of work related visuals, or cross platform linkage of personal and professional identities. These behaviors significantly contribute to the unintentional expansion of an organization's digital footprint.

To mitigate these risks, institutions should adopt a multi-layered strategy. This includes embedding OSINT considerations into existing frameworks like NIST SP 800-53 [10], enhancing employee awareness training (AT family), enforcing access control and personnel management policies (PS family), and performing routine OSINT audits (RA family) to monitor external exposure. The integration of behavioral guidelines, privacy-setting education, and technical scanning should collectively form the foundation of a resilient institutional posture. Without addressing OSINT as a strategic vulnerability, critical financial institutions risk leaving exploitable gaps in an otherwise well-fortified cybersecurity perimeter.

The research conducted here suggests that cybersecurity programs should be enhanced to reflect the evolving OSINT threat landscape. This is also in line to Henricks [27] and Boyson, Corsi, and Paraskevas [25], who stress the need for frameworks to evolve and reflect real-world behaviors. Beyond technical protections, organizations could establish behavioral guidelines regulating what employees may disclose online. Security awareness efforts should include education on metadata leakage and the risks associated with

combining personal and professional identities online. Additionally, employees should be informed about the appropriate use of privacy settings on social media platforms to reduce exposure to these types of risks.

Routine OSINT audits, employing techniques such as passive Google Dorking, can provide valuable insight into public-facing vulnerabilities. The resulting exposure levels should be translated into risk indicators or KPIs to monitor institutional posture over the time. The failure to address OSINT as a strategic vulnerability risk, undermine cybersecurity governance altogether [14].

OSINT must be viewed not as a limited issue but as an integral dimension of cybersecurity management. Frameworks that lack to combine the human behavior component with organizational culture, and digital exposure, are likely to miss the mitigation of sophisticated information gathering tactics employed by modern threat actors.

9.7 Linkage to research objectives

This chapter interpreted the empirical results of the OSINT investigation in light of the research objectives established in Chapter 3. Each research question was addressed not only through primary findings but also by drawing connections to existing academic literature and known industry practices.

The central research question **(MRQ)** explored how human factors contribute to the unintentional exposure of corporate data. The results strongly support previous studies, such as Capano [7] and Hayes [1], who documented how online behaviors and digital footprints serve as vectors for exploitation. Consistent with this literature, this study confirms that employees frequently reveal organizational metadata and internal tool references across publicly accessible platforms.

SRQ1, examining how threat actors exploit such data, finds validation in Mitchell [13] and Decusatis [2], both of whom emphasize the role of OSINT in reconnaissance phases of advanced attacks. The observed use of Google Dorking and professional network mining in this thesis confirms their findings on pre-attack profiling methods.

SRQ2 focused on platform specific exposure patterns. The differentiation of risk levels between LinkedIn, Facebook, and platforms like GitHub was supported by both academic sources and threat intelligence reports such as Proofpoint [31], which detail how attackers use professional social platforms for phishing and social engineering campaigns.

SRQ3 addressed the specific OSINT risk landscape within Estonia's banking sector. Compared to previous cases such as the Croatian banks discussed by Matvej [3], Estonia presents higher visibility risks due to digital maturity, a factor supported by Ünver's [18] argument that increased digitalization expands the OSINT surface.

Finally, **SRQ4** investigated how existing cybersecurity frameworks can be adapted to mitigate these risks. This study extends the recommendations of Henricks [27] and Boyson [25], who advocate for evolving cybersecurity strategies that incorporate human behavior and digital presence. The NIST SP 800-53 framework was mapped onto the OSINT threat landscape to provide a structured response through controls related to training, access agreements, risk evaluation, and behavior management.

This cross validation of empirical evidence and academic literature strengthens the reliability of the findings and underlines the critical need for sector specific, behavior-informed cybersecurity strategies to address OSINT risks in modern digital environments.

10. Challenges and limitations

This chapter reflects on the methodological, analytical, and practical limitations encountered during the study. While the investigation successfully uncovered OSINT related vulnerabilities in Estonia's banking sector, several constraints shaped the depth and scope of the findings. These include limitations inherent in the data collection process, the tools and techniques used, the scope of the systematic literature review, and the ethical choices made throughout the research.

10.1 Ethical Scope

Ethical considerations, including GDPR compliance, anonymization, and responsible handling of publicly available data, were discussed in detail in Chapter 7. These principles also shaped the methodological boundaries of this study and influenced the decision to exclude certain OSINT tools and data types from the analysis.

10.2 Sample Limitations

Although 184 profiles were examined, this sample cannot be considered statistically representative of the entire workforce in Estonia's banking sector. Therefore, the findings should not be interpreted as a definitive assessment of how each institution contributes to data leakage. Rather, they provide a general indication of the types and frequency of sensitive information disclosures observed within specific banks. It is not possible to determine with certainty whether the absence of significant findings in a particular institution reflects effective internal policies or awareness campaigns.

However, the analysis revealed meaningful patterns and recurring behaviors that reflect common OSINT vulnerabilities. These insights, while not exhaustive, offer valuable indicators of how employee behavior can expose sensitive organizational metadata.

10.3 Risk Categorization

Most findings could be categorized as low to moderate risk because they involved indirect or contextual information, such as mentions of enterprise tools, public facing contact details, or vague visual content rather than confidential documents or system credentials. While not immediately critical, these disclosures support adversarial profiling, which can

serve as a foundation for more targeted social engineering or phishing campaigns. As the research focused on passive OSINT collection, high-risk findings (such as credential leaks or internal documents) were outside its legal and ethical scope.

10.4 Tool and Technique Limitations

The investigation relied on passive OSINT methods, particularly manual analysis of digital footprints across social media platforms. Hashtag-based searches, automated scraping tools, and image recognition techniques were excluded due to ethical and resource constraints. Despite these methodological limits, the study demonstrated that even basic techniques, including manual LinkedIn reviews and targeted Google Dork queries were sufficient to uncover employee affiliations, references to internal systems, and metadata of potential intelligence value. This reinforces how low complexity OSINT can produce high-impact results when applied systematically.

11. Recommendations

This chapter presents a set of practical and strategic recommendations resulting from the findings of the OSINT based investigation into data exposure risks across five major Estonian banks. As demonstrated in Chapter 8, publicly available information, particularly from employee social media profiles, can unintentionally reveal sensitive organizational insights. These findings support the growing concern that human behavior and digital presence are key enablers of cyber threats in critical infrastructure sectors.

The recommendations in this chapter are divided into three parts: (1) institutional governance and internal policy, (2) technical and operational practices, and (3) regulatory and sectoral coordination. Each recommendation aims to support financial institutions, cybersecurity professionals, and policymakers in improving the resiliency against cyber threats amplified by OSINT. In line with recent literature on behavioral cybersecurity and organizational exposure [13, 1], this chapter emphasizes the need of strategic and operational planning, through the integration OSINT techniques into both threat intelligence and cyber risk governance.

11.1 Recommendations for financial institutions

Estonian financial institutions face a specific set of risks deriving from employee behavior on digital platforms. This study revealed a pattern of exposure across LinkedIn and Facebook, where employees routinely disclosed their job roles, tool usage, team affiliations, and, in some cases, work related visual content. This information, mainly innocent if considered individually, can be aggregated by threat actors to map internal systems, engineer pretexting campaigns, or identify individuals with privileged access.

To mitigate these risks, financial institutions should develop some guidelines focused on employees' digital behavior. These guidelines shouldn't only focus on generic IT security awareness campaigns. Instead, they should directly address social media conduct. Clear boundaries should be established concerning what can be publicly shared about tools, roles, or team structures. Employees in technical and leadership roles should receive tailored awareness training reflecting their elevated risk of exposure. This aligns with NIST's AT-3 (Role-Based Training) control [10], which emphasizes that personnel with specific security responsibilities or access to critical systems must receive customized training relevant to their role. In the context of OSINT, such employees are often the most exposed through

public metadata and job descriptions. For example, LinkedIn profiles frequently disclose managerial hierarchies and technical specializations, which can be exploited by adversaries to craft spear phishing campaigns or impersonation attacks.

Integrating OSINT-based auditing into red teaming and internal security assessments is strategically significant because even basic techniques, such as manual LinkedIn reviews or Google Dorking were shown in this study to reveal valuable organizational data. Emulating threat actor information gathering methods, security teams can proactively identify the same vulnerabilities adversaries would exploit. This allows institutions to address weak points before they are targeted. Including OSINT tasks in red teaming deliverables also enables a more realistic simulation of pre-attack stages, reinforcing both technical defenses and employee behavioral awareness. The same passive information gathering techniques employed in this study, such as LinkedIn profiling, Google Dorking, and visual content analysis, can be introduced into security programs for internal simulation exercises. These activities not only enhance situational awareness but also generate measurable insights for strengthening the organization's security posture over time [14].

11.2 Enhancing OSINT capabilities in threat intelligence

One of the key contributions of this research is the demonstration of how publicly accessible social metadata can support adversarial profiling. Threat actors can identify technology stacks, organizational hierarchies, and likely phishing targets through platforms such as LinkedIn and Facebook. As Bizouarn, Abdulnabi, and Tan [14] emphasize, OSINT provides adversaries with low cost data, that has a high impact into corporate structures. The same insights can also provide defenders with better understanding of their own risk.

Therefore, financial institutions should integrate OSINT outputs into their threat intelligence activities. This includes creating internal watchlists of job titles or keywords that are frequently associated with internal systems (e.g., ServiceNow, Jira, Ansible, Apache Tomcat, Splunk Enterprise Server) and monitoring their public mention. Furthermore, security operations centers should develop the indicator of exposure derived by OSINT activities. This helps to integrate their existing indicators of compromise. The combination of threat intelligence activities and the use of the data resulted from the OSINT activity can feed the SOC/SIEM team with greater understanding of their indicator of exposure. This can help financial institutions to prevent and detect cyber threats. It also helps to establish priorities needed for the protection of critical assets based on risk analysis of vulnerabilities and known threats to the critical assets [13].

11.3 Integration of OSINT into policy and training programs

The present work support the necessity to embed OSINT awareness into security policy frameworks and employee training. Many employees are still unaware of how their public content may trigger vulnerabilities for the own organizations. As demonstrated in this thesis, even a minor disclosures, such as screenshots, role confirmation, or event participation, can provide threat actors with data used in social engineering campaigns. As noted by Capano [7], adversaries often exploit personal and organizational details disclosed online to craft pretexting scenarios or phishing emails that appear highly credible. These attacks leverage information such as event participation, team affiliations, or tool usage to impersonate colleagues or vendors, thereby increasing the likelihood of successful compromise. The findings in this study reflect this dynamic: seemingly minor disclosures on platforms like LinkedIn or Facebook enable threat actors to develop convincing narratives that bypass generic security filters.

Security policies should explicitly address online conduct, defining both acceptable use of corporate references and the implications of metadata exposure. These policies should be reviewed and updated annually, reflecting changes in platform behavior and threat tactics. For awareness programs to be meaningful, they must simulate OSINT-driven attack scenarios, such as phishing attempts based on LinkedIn metadata. This approach translates theoretical simulations into real world consequences of unintentional information disclosure.

11.4 Sector wide coordination and governance recommendations

While many OSINT risks are present in individual institutions, the patterns identified in this thesis indicate a more systemic vulnerability across Estonia's banking sector. Platforms like LinkedIn and Facebook contain a vast amount of aggregated data sufficient to map technical environments, personnel structures, and inter-organizational relationships. Given this wide interconnection of the financial sector and its role within national digital infrastructure, this exposure type of risk cannot be mitigated by a single institution alone. For instance, the Estonian Financial Supervisory Authority or the Information System Authority should translate this activity into specific OSINT related guidelines for a better digital risk management.

12. Conclusions

This thesis has demonstrated that employee driven OSINT exposure is not only possible but increasingly likely in highly digitalized environments such as Estonia's banking sector. While the research employed only passive, ethically aligned techniques, it revealed a consistent pattern of professional and personal disclosures that could aid adversaries during reconnaissance and pretexting stages. The key takeaway is that the human element through social media activity, platform linkage, or metadata leakage can unintentionally expand the attack surface of critical infrastructure institutions.

Rather than offering just a descriptive mapping of digital behaviors, this work critically examined how threat actors might weaponize such publicly available data. It also argued for the integration of OSINT perspectives into cybersecurity frameworks, red teaming exercises, and policy development moving beyond traditional perimeter focused models of cyber defense.

Importantly, the lack of sector specific guidance was revealed by the response received from Estonia's national Information System Authority - RIA, which confirmed that there are currently no OSINT mitigation strategies tailored for the financial sector. This gap validates the contribution of this thesis and signals an urgent need for regulatory engagement in this area.

The findings also affirm that OSINT is not merely a threat vector but a diagnostic tool for defenders. Financial institutions and policymakers should not only be concerned with what attackers might see but should begin using these same tools to monitor their digital footprint proactively.

While limited in scale, this study offers an exploratory foundation for assessing institutional vulnerability driven by digital behavior. Future research should expand the scope through interviews, automation tools, or real-time monitoring systems to quantify exposure more comprehensively.

In summary, the boundary between internal cybersecurity and external digital visibility is increasingly blurred. In sectors handling sensitive data, managing human behavior online must become as important as securing the systems those employees operate. OSINT should be treated as a core element of strategic cybersecurity governance, not an edge case.

13. Future work

This thesis has demonstrated how employee driven digital exposure can introduce significant cybersecurity risks through publicly accessible data, particularly within Estonia's banking sector. However, several areas remain open for further exploration and refinement.

13.1 Advanced technical OSINT and automation

While this study focused primarily on social OSINT, future research could incorporate more advanced technical reconnaissance techniques, such as DNS and subdomain enumeration, infrastructure exposure mapping through tools like Shodan or Censys, and the analysis of unsecured public APIs. Moreover, automation through natural language processing, scraping frameworks, and machine learning models may significantly enhance the scalability and accuracy of OSINT monitoring, enabling near real-time detection of emerging exposure indicators.

13.2 Hashtag and keyword exposure analysis

A method logical limitation of this study was the exclusion of hashtag and keyword based content analysis. Future investigations could examine the use of hashtags (e.g., `#bankname`) or contextual keywords such as "promotion," "hiring," or "project" across platforms like LinkedIn, Instagram, and X (formerly Twitter). Such analysis may reveal broader institutional exposure trends, including indirect disclosures made by former employees, clients, or third-party partners.

13.3 Behavioral and policy oriented research

Further research is granted into the behavioral factors driving unintentional disclosure of sensitive metadata by employees. Qualitative approaches, such as surveys or semi-structured interviews could offer insight into motivational, cultural, or organizational dynamics influencing digital behavior. Additionally, future work could examine how OSINT related threats are addressed (or neglected) within evolving regulatory frameworks such as NIS2 and DORA. Exploring how institutions interpret and implement these directives could inform the development of sector specific best practices for managing digital exposure.

References

[1] D. R. Hayes and F. Cappa. "Open-source intelligence for risk assessment". In: *Business horizons* 61.5 (2018), pp. 689–697. DOI: 10.1016/j.bushor.2018.02.001.

[2] C. DeCusatis et al. "Red team ethical physical penetration testing simulations using open source intelligence". In: *2023 IEEE 13th annual computing and communication workshop and conference*. 2023. DOI: 10.1109/CCWC57344.2023.10099053.

[3] E. Matvej, Z. Morić, and S. Papić. "Croatian Bank security analysis by publicly available data". In: *Annals of DAAAM & proceedings*. 2020. DOI: 10.2507/31st.daaam.proceedings.024.

[4] S. Lee and T. Shon. "Open source intelligence base cyber threat inspection framework for critical infrastructures". In: *FTC 2016 - proceedings of future technologies conference*. 2016. DOI: 10.1109/FTC.2016.7821730.

[5] Information System Authority (RIA). *September in Estonian Cyberspace: People Lost Thousands of Euros Due to Phishing*. Accessed: 29-04-2025. 2023. URL: https://www.ria.ee/en/news/september-estonian-cyberspace-people-lost-thousands-euros-due-phishing.

[6] Information System Authority (RIA). *Situation in Cyberspace – March 2024*. Tech. rep. Accessed: 29-04-2025. Estonian Information System Authority, Apr. 2024. URL: https://www.ria.ee/sites/default/files/documents/2024-04/Situation-in-cyberspace-march-2024.pdf.

[7] D. Capano. "Cybersecurity: human assets". In: *Control engineering* 66.11 (2019). [Accessed: 18 October 2024], pp. 41–43. URL: https://research.ebsco.com/linkprocessor/plink?id=96582321-3729-3b11-a7b1-9a8abfdadd38.

[8] Marianthi Theocharidou et al. *ENISA Threat Landscape: Finance Sector (January 2023 – June 2024)*. European Union Agency for Cybersecurity (ENISA). Feb. 2024. DOI: 10.2824/5410466. URL: https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf.

[9] National Institute of Standards and Technology. *Security and Privacy Controls for Information Systems and Organizations*. Accessed: 15-04-2025. 2020. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[10] Cybersecurity framework tools. *NIST SP 800-53 controls reference*. https://csf.tools/reference/nist-sp-800-53/. Accessed 19 April 2025. 2025.

[11] International Organization for Standardization (ISO). *ISO 27001 Annex A.7 and A.8: Human Resource Security and Operational Security*. https://iso-docs.com/blogs/iso-27001-standard/iso-27001-annex-a-7-human-resource-security?srsltid=AfmBOoqSuZfoEaqzJq-uXzkXUt0jORhhkP46zqg9zWGQazNlgKTtK6uYv. Accessed: 21-04-2025. 2025.

[12] European Union Agency for Cybersecurity (ENISA). *European Cybersecurity Skills Framework (ECSF)*. https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles. Accessed: 21-04-2025. 2022.

[13] B. Mitchell. "Corporate cyberespionage: identification and prevention part 1". In: *EDPACS: the EDP audit, control & security newsletter* 62.5 (2020), pp. 1–14. DOI: 10.1080/07366981.2020.1798594.

[14] K. M. Bizouarn, M. Abdulnabi, and M. J. Tan. "OSINT and AI: a powerful combination for company vulnerability detection". In: *2023 IEEE 21st student conference on research and development*. Dec. 2023. DOI: 10.1109/SCOReD60679.2023.10563226.

[15] Md. Adil Raza et al. "Evaluating the Human Factor in Bank Cybersecurity: Strategies for Improving Employee Awareness and Reducing Insider Threats". In: *Indonesian Journal of Advanced Research (IJAR)* 4.1 (2025), pp. 1–20. DOI: 10.55927/ijar.v4i1.13399. URL: https://journal.formosapublisher.org/index.php/ijar/article/view/13399.

[16] T. O. Browne, M. Abedin, and M. J. M. Choudhury. "A systematic review on research utilising artificial intelligence for open source intelligence (OSINT) applications". In: *International journal of information security* 74.4 (2024), pp. 2911–2938. DOI: 10.1007/s10207-024-00868-2.

[17] T. Sasaki, K. Yoshioka, and T. Matsumoto. "Who are you? OSINT-based profiling of infrastructure honeypot visitors". In: *International symposium on digital forensics and security*. 2023. DOI: 10.1109/ISDFS58141.2023.10131856.

[18] Ü. H. Akın. *Digital open source intelligence and international security: a primer*. Centre for economics and foreign policy studies, [accessed: 10-10-2024]. 2018. URL: https://www.jstor.org/stable/resrep21048.

[19] C. Eldridge, C. Hobbs, and M. Moran. "Fusing algorithms and analysts: open-source intelligence in the age of 'big data'". In: *Intelligence & national security* 33.3 (2018), pp. 391–406. DOI: 10.1080/02684527.2017.1406677.

[20] LHV Bank. *About LHV*. https://www.lhv.ee/en/about. Accessed: 18-04-2025. 2025.

[21] Swedbank AS. *Swedbank in numbers*. https://swedbank.ee/about. Accessed: 18-04-2025. 2025.

[22] SEB Pank. *About SEB*. https://www.seb.ee/en/about-seb/about-seb. Accessed: 18-04-2025. 2025.

[23] Coop Pank AS. *About Coop Pank*. https://www.cooppank.ee/en/coop-pank/about-coop-pank. Accessed: 18-04-2025. 2025.

[24] K. Smith. "Digital espionage". In: *Best's review* 119.4 (2018). [Accessed: 07-10-2024], pp. 56–59. URL: https://research.ebsco.com/linkprocessor/plink?id=63c992ee-d206-3418-96f8-7c2fb4c81f4d.

[25] S. Boyson, T. M. Corsi, and J. P. Paraskevas. "Defending digital supply chains: evidence from a decade-long research program". In: *Technovation* 118 (2022), pp. 1–13. DOI: 10.1016/j.technovation.2021.102380.

[26] European Commission. *NIS2 Directive: new rules on cybersecurity of network and information systems*. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive. Accessed 15-04-2025. 2025.

[27] S. C. Henricks. "Social media, publicly available information, and the intelligence community". In: *American intelligence journal* 34.1 (2017), pp. 21–31. URL: https://www.jstor.org/stable/26497113.

[28] A. Yadav, A. Kumar, and V. Singh. "Open-source intelligence: a comprehensive review of the current state, applications and future perspectives in cyber security". In: *Artificial intelligence review* 56.11 (2023), pp. 12407–12438. DOI: 10.1007/s10462-023-10454-y.

[29] MITRE Corporation. *CVE-2025-30219: RabbitMQ Management UI XSS via Virtual Host Name*. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-30219. Available at: CVE database maintained by MITRE. 2025.

[30] MITRE Corporation. *CVE-2024-8924: ServiceNow Blind SQL Injection Vulnerability*. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-8924. Common Vulnerabilities and Exposures (CVE) Record. 2024.

[31] Proofpoint, Inc. *State of the Phish 2023 – Rapport France*. https://go.proofpoint.com/rs/309-RHV-619/images/Proofpoint_Rapport-State_of_the_Phish_2023_en_France_Mar8.pdf. Accessed: 15-04-2025. 2023.

[32] Luminor. *About Luminor*. Accessed: 18-04-2025. 2025. URL: https://luminor.ee/about.

[33] ServiceNow Support. *ServiceNow Common Vulnerabilities & Exposures (CVE)*. Accessed April 2025. 2023. URL: https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1226057.

[34] Lindsay Sterle and Suman Bhunia. "On SolarWinds Orion Platform Security Breach". In: *2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI)*. IEEE, 2021, pp. 635–641. DOI: 10.1109/SWC50871.2021.00094. URL: https://doi.org/10.1109/SWC50871.2021.00094.

[35] e-Estonia Briefing Centre. *2023: Estonia facing advanced cybersecurity threats*. Accessed: 2025-05-08. 2023. URL: https://e-estonia.com/2023-estonia-advanced-cybersecurity-threats/.

Appendix 1 – Non-Exclusive License for Reproduction and Publication of a Graduation Thesis[1]

I Marco Fontana

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis "Human aspects of OSINT in corporate espionage: how employees unknowingly leak critical information", supervised by Ricardo Gregorio Lugo
   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.

27.05.2025

[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 – Overview of analyzed OSINT articles

Article	Authors	Year	OSINT focus	Sector	Human factors	Key findings	Relevance to thesis	MRQ	SRQ1	SRQ2	SRQ3	SRQ4
Digital open source intelligence and international security: a primer	Ü. H. Akın	2018	Strategic implications	International Security	Yes	OSINT reshapes secrecy and digital governance.	High	Yes	–	–	–	Yes
Management of open source information in the management of current cyber threats and ways to fight fraud at financial companies	C. S. Bădele and L. Ivan	2021	Fraud prevention	Finance	Yes	Emphasizes employee awareness and fraud prevention.	Very High	Yes	Yes	–	Yes	–
OSINT and AI: a powerful combination for company vulnerability detection	K. M. Bizouarn et al.	2023	AI-based vulnerability detection	Corporate	Yes	AI finds vulnerabilities from public employee data.	Very High	Yes	Yes	Yes	–	–

Article	Authors	Year	OSINT focus	Sector	Human factors	Key findings	Relevance to thesis	MRQ	SRQ1	SRQ2	SRQ3	SRQ4
Defending digital supply chains: evidence from a decade-long research program	S. Boyson et al.	2022	Supply chain risk management	Supply Chain	Indirect	Human-originated risks in digital ecosystems.	Medium	Yes	–	–	–	Yes
Eight reasons why your business may get hacked	W. Bonheim	2024	Common cyber risks	Business	Yes	Human errors (password reuse, oversharing) exploited.	Medium	Yes	Yes	Yes	–	–
Red team ethical physical penetration testing simulations using open source intelligence	C. De-Cusatis et al.	2023	Red teaming and simulation	Education / Training	Yes	OSINT helps simulate realistic social engineering.	High	Yes	–	–	–	Yes
Fusing algorithms and analysts: open-source intelligence in the age of 'big data'	C. Eldridge et al.	2018	Big data and intelligence	National Security	Yes	Human judgment complements algorithmic OSINT.	Very High	Yes	–	Yes	–	Yes
Open-source intelligence for risk assessment	D. R. Hayes and F. Cappa	2018	Risk prediction via LinkedIn	Critical Infrastructure	Yes	Employee OSINT can predict internal threats.	Very High	Yes	Yes	Yes	–	Yes
Social media, publicly available information, and the intelligence community	S. C. Henricks	2017	Social media profiling	Government	Yes	Social media is a lawful data source for profiling.	High	Yes	Yes	Yes	–	–

Article	Authors	Year	OSINT focus	Sector	Human factors	Key findings	Relevance to thesis	MRQ	SRQ1	SRQ2	SRQ3	SRQ4
Analysis and overview of information gathering & tools for pentesting	A. S. L. Kowta et al.	2021	OSINT toolkits overview	General	Yes	Tools like Google Dorking, Shodan help data mining.	High	Yes	Yes	Yes	–	–
Open Source Intelligence Base Cyber Threat Inspection Framework for Critical Infrastructures	S. Lee and T. Shon	2016	Framework design	Critical Infrastructure	Indirect	Presents OSINT threat detection framework.	Very High	Yes	–	–	Yes	Yes
Croatian Bank security analysis by publicly available data	E. Matvej et al.	2020	Passive OSINT footprinting	Banking	Yes	Discovered sensitive bank data through OSINT.	Very High	Yes	Yes	Yes	Yes	–
Corporate cyberespionage: identification and prevention part 1	B. Mitchell	2020	Insider threats and info leaks	Corporate	Yes	OSINT aids insider threat identification.	High	Yes	Yes	–	–	Yes
Evaluating the Human Factor in Bank Cybersecurity	M. A. Raza et al.	2025	Insider threat and awareness	Banking	Yes	Training mitigates employee-driven vulnerabilities.	Very High	Yes	Yes	–	Yes	Yes
Who are you? OSINT-based profiling of infrastructure honeypot visitors	T. Sasaki et al.	2023	Honeypot profiling	Infrastructure / Cybersecurity	Yes	OSINT tracks attacker behavior via Telnet.	Very High	Yes	Yes	Yes	–	Yes

Article	Authors	Year	OSINT focus	Sector	Human factors	Key findings	Relevance to thesis	MRQ	SRQ1	SRQ2	SRQ3	SRQ4
Digital espionage	K. Smith	2018	Corporate IP theft via OSINT	Corporate / Insurance	Yes	Employees unintentionally enable long-term risks.	High	Yes	Yes	–	–	Yes
Open-source intelligence: a comprehensive review of the current state, applications and future perspectives in cyber security	A. Yadav et al.	2023	OSINT systems and misuse	Cross-sector	Yes	Describes risks, methods, future directions.	High	Yes	Yes	Yes	–	–
Governing cyber espionage threats via the integration of the risk society-cyber securitisation theory	R. Wan et al.	2021	Theory integration	Government / Policy	Yes	Risk society theory aligns with OSINT mitigation.	Very High	Yes	–	–	–	Yes
A systematic review on research utilising artificial intelligence for open source intelligence (OSINT) applications	T.O.Browne et al.	2024	AI tool survey for OSINT	General	Yes	AI enhances OSINT processing and targeting.	High	Yes	Yes	Yes	–	–

Article	Authors	Year	OSINT focus	Sector	Human factors	Key findings	Relevance to thesis	MRQ	SRQ1	SRQ2	SRQ3	SRQ4
Cybersecurity: human assets	D. Capano	2019	Insider behavior	Industrial / Engineering	Yes	Human error is the root of many cyber incidents.	Medium	Yes	–	–	–	–
Mapping tools for open source intelligence with cyber kill chain for adversarial aware security	M. Y. Muhammad et al.	2022	OSINT mapped to kill chain	Cybersecurity / Military	Yes	OSINT supports attack lifecycle stages.	High	Yes	Yes	–	–	Yes