Mészáros, A. A., & Kelemen-Erdős, A. (2023). Industrial espionage from a human factor perspective. *Journal of International Studies, 16*(3), 97-116. doi:10.14254/2071-8330.2023/16-3/5

Journal of International Studies

Centre of Sociological Research

Scientific Papers

Industrial espionage from a human factor perspective

Alexandra Ágnes Mészáros
Óbuda University,
Budapest, Hungary
meszaros.alexandra@uni-obuda.hu
ORCID 0000-0003-3652-0203

Anikó Kelemen-Erdős
Budapest University of Technology and Economics,
Budapest, Hungary
kelemen-erdos.aniko@gtk.bme.hu
ORCID0000-0001-7202-5870

Abstract. Industrial espionage is a significant threat in a fiercely competitive environment which increases the risk of information security and safety being compromised and leads to concerns about business ethics. The main aim of this paper is to examine industrial espionage from the perspective of the insider human factor, explore the motivations that may lead to industrial espionage, and identify ways of maintaining information security and safety to reduce insider threats. The research involved qualitative in-depth interviews among twenty-one stakeholders from seven European countries. The transcripts were analysed using grounded theory methodology. Results show that main factors that may lead to industrial espionage include intensifying market competition, financial compensation offered in exchange for information, decreasing loyalty among the younger generation, psychological issues of personal grievance and psychological disorders, and poorly developed information-security infrastructure. This study recommends that managers and policymakers plan and implement protection and prevention measures, undertake risk analyses to reduce the potential consequences of insider threats, and establish a critical business information tracking system. Further recommendations include maintaining an appropriate company culture, ensuring employee satisfaction, and fostering information safety education while creating adequate security infrastructure.

Keywords: information security policy, information security culture, information security and safety, insider threat, grounded theory, European countries

JEL Classification: F16, F23, M54

Received: February, 2023
1st Revision: May, 2023
Accepted: September, 2023

DOI: 10.14254/2071-8330.2023/16-3/5

1. INTRODUCTION

Industrial espionage is one of the oldest business-related activities and is still a crucial issue in the modern economy. In the past few years, the frequency and negative impact of industrial espionage incidents have increased worldwide (Shelupanov et al., 2021; Konopatsch, 2020; Thorleuchter & Van den Poel, 2013), while the technological revolution has created more opportunities for the misuse of information (Kuzmenko et al., 2021). It is one of the most severe dangers in a country's industry and poses a significant threat long-term economic development (Heickerö, 2019) and to companies everywhere, making security challenges a global concern (Williams et al., 2023).

Industrial espionage is a complex issue with no standard generally accepted definition (Button, 2020; Hou & Wang, 2020; Carl, 2017). An interdisciplinary approach is required to address it. In this research, **industrial espionage** is considered as any activity organized by an actor in the international competitive market (Thorleuchter & Van den Poel, 2013) that aims to misappropriate critical business information from another actor (Button, 2020; Nasheri, 2005) to further their economic interests (Sutherland & Jones, 2008) without the direct involvement of any governmental actor (Button, 2020; Nasheri, 2005). Critical business information is essential for organizations active in the global competitive market. The most common types of the former affected by industrial espionage are intellectual property (consisting of patents, inventions, manuscripts, formulas, production details) and information about an organization's strategic, financial, and marketing activities (Nasheri, 2005; Rothke, 2001). Circumstances may invite companies to gather business information using unethical or illegal methods such as industrial espionage. When industrial espionage is suspected, it is important to identify whether the perpetrator is internal or external to the company because offenders are often trusted employees: a large proportion of such incidents globally are internally driven (Button, 2020; Zaytsev et al., 2017). Insiders who enjoy an organisation's confidence but act against it are a critical threat to any organization.

According to statistics, industrial espionage committed by insiders is rare, but even when companies have clear evidence of this, they are more reluctant to report such incidents to authorities (Button, 2020; Sadok et al., 2020; Bedford & Van Der Laam, 2016), thus the latter seldom become public (Sadok et al., 2020; Solberg Søilen, 2016). Consequently, few documented cases are known, so the problem of industrial espionage is hard to research and associated with very little academic curiosity (Lyan & Frenkel, 2022; Button, 2020; Knickmeier, 2020; Elifoglu et al., 2018; Solberg Søilen, 2016; Omar, 2015; Brancik & Ghinita, 2011). Many companies have invested in cyber defence systems to secure critical business information and focus only on information-technology-related outsider threats, ignoring the significant insider threat (Homoliak et al., 2020; Saxena et al., 2020). The novelty of this research is its focus on the internal threat posed by the human factor, whereas prior articles (Hou & Wang, 2020; Ashenden, 2018; Bedford & Van Der Laam, 2016; Brancik & Ghinita, 2011) predominantly examined the issue of industrial espionage from the perspectives of legal, technical, and external threats. Furthermore, the uniqueness of this research is that the findings are derived from empirical data collected through expert in-depth interviews, thus providing a framework that may help organizational leaders mitigate the risk of internal threats effectively.

The study focuses on industrial espionage in the competitive market, typically involving espionage between two competitors (Schiller, 2019). The research uses a multidisciplinary approach to analyse industrial espionage from the perspective of the insider human factor, examines the source of motivation for industrial espionage, and identifies how to reduce insider threat through the implementation of safety and security systems. The problem is approached using a comprehensive perspective. The literature review presents the role of the human element in industrial espionage, distinguishing unintentional and intentional incidents and describes potential means of protecting against insider threats based on a body of systematically analysed literature. The following section explains the research methodology. The empirical

results and discussion present the factors involved in the increasing number of industrial espionage incidents, with a focus on the human factor, and suggest preventive measures that can support companies to decrease the risk of industrial espionage committed by insiders. In the conclusions, the practical implications of the results are presented.

2. LITERATURE REVIEW

In cases of industrial espionage, the important question arises whether the perpetrator is internal or external, as offenders are not always unknown strangers but may be trusted employees of organizations (Knickmeier, 2020). Different forms of industrial espionage categorised according to perpetrator and intention are documented in Table 1.

Table 1

Forms of industrial espionage

Affiliation of perpetrator	**Mode of perpetration**	
	Intentional	**Indirect ('unintentional')**
Outsider	○ Acquires trade secrets from companies to knowingly benefit another company ○ Illegal and unethical activities undertaken by economic entities to systematically gather, analyse, and manage information on competitors ○ Cyberattacks, forms of social engineering ○ The clandestine obtaining of confidential information without permission ○ Bribing	○ Obtaining data, information, and market analysis of competitors if trade secrets are detected ○ Informal and formal conversations and other interactions with employees of a competitor without any ulterior motive
Insider	○ Data mishandling ○ Negligence ○ Clandestine obtaining of confidential information without permission ○ Inadequate training ○ Negligence of security policy; IT sabotage	○ Current or former employee, contractor, or business partner who has authorized access to an organization's system or business information ○ Lack of security policies ○ Lack of training programs
Both (outsider and insider)	○ Appropriation of intellectual property ○ Fraud ○ Unauthorized access to information	○ Mistakes

Source: authors' construction.

2.1. The role of the human element in industrial espionage

Industrial espionage committed by an insider who enjoys the confidence of an organization and has access to business secrets is the most unforeseen and sensitive form of economic crime, so the decision-makers of companies need to be aware of the nature of this threat. **Insider threat** refers to any individual who has or had authorized access to the assets of an establishment whose actions or inactivity, intentions, or carelessness have the potential to negatively affect the organization (Elifoglu et al., 2018; Bedford & Van Der Laam, 2016). The insider threat takes two different forms: intentionally committed malicious acts and unintentional acts, such as mistakes that have adverse impacts on the organization (Williams et al., 2019; Ashenden, 2018; Elifoglu et al., 2018; Hills & Anjali, 2017; Omar, 2015). Both forms can have devastating consequences for the information resources of an organization.

The **unintentional insider threat** refers to a current or former employee, contractor, or business partner who has authorized access to information and acts with no malicious intention yet causes harm to an organization's system or business information (Williams et al., 2019). Unintentional incidents happen due to a wide range of employee activities. In some cases, employee negligence (Ashenden, 2018) or the basic human tendency to make mistakes (Goel et al., 2017) lead to security gaps. In other cases, unacceptable attitudes toward security policy, inadequate or non-existent training programs, stress, carelessness, loss of devices, a desire to help others, vulnerability to blackmail or other unintentional acts negatively affect companies' economic interests (Williams et al., 2019; Elifoglu et al., 2018; Goel et al., 2017; Omar, 2015).

An **intentional insider threat** may be evoked by a current or former stakeholder of the company who has authorized access to the system of the organization or business information and intentionally uses their access in a manner that negatively affects the company (Williams et al., 2019; Patil & Meshram, 2018). As a consequence of their insider knowledge, the activities of internal offenders can be particularly damaging (Knickmeier, 2020). For example, Omar (2015) and Brancik & Ghinita (2011) have shown that deliberate insider attacks usually originate in the malicious intentions of skilled employees with good knowledge of the internal security measures of an organization. In contrast, Elifoglu and co-authors (2018) found that malicious insiders are not typically hackers equipped with special technical tools but are often employees who undertake authorized tasks with malicious intent.

The reasons for the intentional acts of insiders range widely. Some of the strongest sources of motivation are a desire for money, loss of loyalty, anger towards the organization, an ad hoc occasion to steal for personal gain, and the possession of the professional skills required to spy (Mitchell, 2020; Solberg Søilen, 2016). Employee dissatisfaction caused by poor management practices, insufficient communication, or a poor company culture also increases the risk of an insider incident (Sadok et al., 2020), as employees' motivation and commitment are influenced by how well their personal identity and perceptions of the justice and fairness of a company are aligned (Collier & Esteban, 2007). In other cases, insiders are bribed or blackmailed by an outsider actor to misappropriate information (Button, 2020). Participation in industrial espionage against an organization can also be influenced by a personal health predisposition, such as clinical depression, which involves the individual's personality and personal history (Noonan, 2018).

Researching unintentional and intentional threats is important because effective protection measures can be developed only against threats whose nature is thoroughly understood.

2.2. Potential protection against insider threat

To keep confidential business information secure, many organizations focus only on addressing information-technology-related outsider threats when fortifying their networks and do not pay close attention to the significant insider threat personified by stakeholders, although insider threat is one of the most challenging cybersecurity issues (Homoliak et al., 2020; Saxena et al., 2020). This approach is rooted in a lack of understanding of insider threat, leading policymakers to focus on strengthening technological protection when the real solution is not technological (Lara et al., 2020). To protect an organization from malicious insider threats, a holistic approach should be pursued that requires significant expertise (Dokko et al., 2021).

Insider threats continue to evolve in complexity and sophistication (Lehto, 2022) as technological advances make committing industrial espionage easier (Barrachina et al., 2021), leading to inexpensive access to other actors' critical information (Maican, 2019). Business organizations try to protect themselves by predicting potential insider incidents of industrial espionage before they actually happen (Elifoglu et al., 2018). Coordinating employee activity, processes, technology, and organizational strategy helps companies foresee and prevent potential incidents (Bedford & Van Der Laam, 2016). A multi-layered defensive system

that can proactively protect information infrastructure (Omar, 2015), monitor the weak signals of employee behaviour (Hills & Anjali, 2017), observe social media activity (Carstens et al., 2021), analyse warning signs associated with employees (Noonan, 2018) and employee profiling (Lee, 2015) may also help to prevent and foresee potential incidents. However, many of these approaches require careful application as they may encroach on personal freedom, and intensive employee monitoring creates distrust in the workplace (Chan, 2004).

Forthcoming developments will create more complex security challenges for managers and policymakers. The need for security responses to increasingly diverse attempts at hacking, the increase in innovative new services and devices that have many advantages but need to be managed appropriately to reduce the risk of them being used against companies, the emergence of autonomous entities (devices, agents, and robots) that will require identification, authentication, and authorization just like humans, and the new security threats posed by employees working from home or other locations are all factors that will make managers and their efforts to protect companies more important than ever (Wilson & Hingnikar, 2023). As smart systems are being integrated into companies' daily operations, integrating physical systems with cyber technology has led to more cyber-physical attacks (Williams et al., 2023); consequently, improving cyber security requires better and faster responses through targeted security updates (Nejad, 2023).

3. METHODOLOGY

3.1. In-depth interviews

The study was designed to explore the reasons, supporting circumstances, primary forms, and opportunities for implementing industrial espionage committed by the stakeholders of a company. According to the statistics, industrial espionage incidents committed by insiders are rare, but the probability that suspected incidents are reported is low, and quantitative methods alone cannot provide a full picture of such issues (Button, 2020; Sadok et al., 2020; Bedford & Van Der Laam, 2016).

In this study, participants were selected through purposive sampling, allowing individuals with relevant characteristics to be identified based on their relevance to the researched problem (Andrade, 2021). Data collection was conducted through expert in-depth interviews, typically performed with executives or professionals possessing exceptional knowledge in a defined field (Gáti & Bauer, 2017). In this research, the interviews were conducted with twenty-one individuals in leadership positions at innovative companies whose activities involve the daily use of critical information. The semi-structured, in-depth interviews were assisted by a guide to support the conversation flow. On average, each interview lasted 45-60 minutes. The interviews were personal discussions, during which the participants were encouraged to share their thoughts openly, knowing that every contribution could add to the success of the research.

In-depth interviews are the most appropriate method for examining sensitive issues (Delannon & Raufflet, 2021; Brannen, 1988) because they are similar to a situation when two individuals discuss a topic of mutual interest, in which the discussion is ideally open and honest (Mason, 2002). When using this flexible and free-flowing method, the moderator allows the respondent to freely express their thoughts on the subject while the interviewer discreetly leads the conversation (Morris, 2015). This method permits the deep exploration of the comments of the interviewee. It provides a way of assessing the perspectives of the respondents, their personal understanding, values, beliefs, experiences, and perceptions. This way, a deeper understanding of matters of interest may be obtained, and these nuanced accounts may become a primary source of knowledge (Scanlan, 2020). The main strengths of semi-structured in-depth interviews are that they allow access to rich personal data, as this extremely versatile method enables the interviewee to talk

about what they think is important and permits the understanding of the context and motivation of the latter (Morris, 2015).

The interviews started with explaining to the interviewee that no personal or confidential information about them or their company would be collected because of the subject's sensitivity and information security reasons. However, the interviewees were assured that every thought they could share could be very helpful in the course of the research. The phases of the interviews were structured based on the formulated research questions. First, the reasons for the increasing number of industrial espionage incidents were investigated utilizing the respondents' personal experiences. Then, the employees' attitudes toward confidential business information and respondents' experiences and opinions about unintentional incidents were explored. The issue of intentional business information leaks and the drivers of such acts were then analysed. The last phase of the interview involved exploring how to handle detected cases of espionage.

3.2. Grounded theory

Grounded theory methodology was used for the data analysis. Grounded theory is a widely acknowledged, scientifically based qualitative research methodology that can increase comprehension of the subject of the study (Delannon & Raufflet, 2021; Bratianu, 2020). This systematic methodology is often applied in exploratory research on sensitive topics (Mitev, 2012; Yin, 2001). The original grounded theory methodology was developed by Glaser and Strauss in 1967. Grounded theory can be defined as a qualitative research methodology that allows the researcher to observe an area of study and extract theory from data that is systematically collected (Glaser & Strauss, 1967). This research applies the further developed constructive grounded theory, which is abductive in nature as data is derived from the investigation and compared to previous literature, thus, contains inductive and deductive elements (Charmaz, 2014). Its primary purpose is to help construct a theory that represents an abstract understanding of one or more core elements of the area under study and offers useful strategies for developing researchers' theoretical analyses (Charmaz & Thornberg, 2021).

The data analysis was supported by NVivo 12 Software, which is suitable for supporting the data extraction process and enhances data reliability and accuracy; however, manual data reduction work cannot be omitted (Zamawe, 2015). Thus, every code, subcategory, and core category must be encoded manually.

Constructing theory from the gathered material requires coding the data at different levels (Bhal & Leekha, 2008). The related coding strategies involve classifying data into different conceptual areas and then compiling it into new ideas that lead to the emergence of theory (Corbin & Strauss, 1990). Figure 1 provides a detailed overview of the grounded theory process.

One of the most important criteria for assessing the validity of qualitative research is its trustworthiness (Riegger et al., 2021; McGinley et al., 2021), consisting of *credibility, transferability, dependability*, and *confirmability* (Guba & Lincoln, 1989), and a deeper exploration of the latter factor: integrity (Wallendorf & Belk, 1989). To ensure the trustworthiness of the results, the present research takes these aspects into account. However, *dependability* is a limitation of the research, as ensuring this would require a longitudinal study. At the same time, integrity may only be partially claimed due to the topic's sensitive nature. Furthermore, any concealment or embellishment of cases may distort data. However, the independent interviewees contributed to exploring and understanding real problems.

Confirmability (triangulation) is supported by the fact that both authors conducted the interviews. Thus, their a priori knowledge, views, and attitudes differed.

The *credibility* of the grounded theory methodology is based on rigorous documentation of analytical processes from research planning to evaluation (Glaser & Strauss, 1967). Thus, each step of the procedure is described in detail. The first step in the process is open coding – when the data embodied in transcripts

is broken down into 'thought units' that can range from a simple phrase to several sentences (Bhal & Leekha, 2008). The second step is axial coding, whereby the thought units are regrouped into developing categories, helping discover and specify their similarities and differences (Baskerville & Pries-Heje, 1999). The third step is defining propositions, which involves determining relationships between a category and its concepts and among different categories (Bhal & Leekha, 2008). Finally, the results are interpreted in line with previous theories to ensure external validity (Charmaz, 2014).

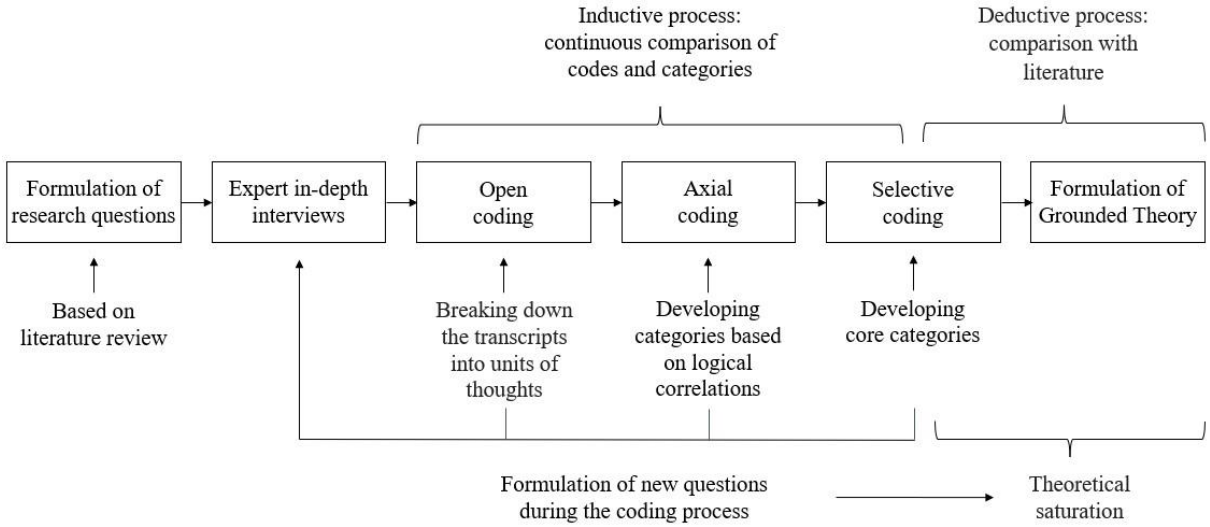

Figure 1. Stages of grounded theory methodology

Source: authors' construction based on Glaser & Strauss (1967) and Charmaz (2014)

Credibility and the triangulation of the qualitative approach can also be ensured by using multiple sources and intercoding (Denzin, 1978; Strauss & Corbin, 2008). In this context, relevant interviewees with various backgrounds were selected (see Sample subsection), and the authors simultaneously encoded transcripts. The first phase of the data analysis of this research involved an inductive approach to the initial coding to extract as much information as possible from the transcripts. The dual analysis, evaluated by using Cohen's Kappa ($\varkappa$) $\varkappa$= 0.79, resulted in almost perfect agreement between the encoders insofar as this indicator is interpreted by Everitt (1996). The Prevalence Index, which refers to the probability of the same and different codes emerging during the coding procedure (Byrt et al., 1993), had a relatively small effect on $\varkappa$ in this research (PI=0.50). Likewise, the bias of the coders appeared to have a negligible effect, as the Bias Index (BI=0.06) was small. However, it should be noted that Cohen's Kappa is not entirely reliable (Delgado & Tibau, 2019; Chicco et al., 2021). For this reason, Matthews' Correlation Coefficient (MCC) was also calculated. The result was MCC=0.21, suggesting that encoding resulted in the generation of almost random codes (Chicco et al., 2021), suggesting that bias played a minor role; other coders would probably have arrived at a similar result.

The second stage of the coding process was classifying the initial codes into axial codes based on the logical context. The third step was classifying the axial codes into theoretical codes, which resulted in the emergence of core categories. Finally, the result of the research, the grounded theory, was defined, and a model describing the relationships among the identified variables was built.

Associated with external validity, transferability was ensured by soliciting responses from stakeholders from twenty-one companies operating in seven different European countries.

3.3. Research questions

According to the grounded theory methodology, the final grounded theory should emerge from empirical data supported by research questions rather than hypotheses – this is also the case for ensuring an abductive process, thus avoiding limiting the research (Strauss & Corbin, 2015). This is an important step because the approach can generate the theoretical sensitivity that supports data fidelity (Charmaz, 2014). Based on the theoretical framework, the main knowledge gaps and dimensions of the research were identified and outlined, and the following research questions (RQ) were formulated:

RQ1: What are the main reasons for insider industrial espionage?
RQ2: What circumstances can lead to unauthorized business-information-outflow incidents?
RQ3: How and in what form do insider threats occur?
RQ4: How can companies manage and prevent insider industrial espionage?

Data were collected through semi-structured, in-depth interviews using open-ended questions that allowed respondents to reflect on their own experiences about the issue. The transcripts were analysed with NVivo 12 software. During the interviews, the questions in the guide were derived from the primary research questions. However, every interview differed slightly to foster the emerging theory and theoretical sensitivity. In accordance with the principles of abductivity and enhancing creditability (internal validity), the results are evaluated in relation to the scientific literature (see the Discussion and Recommendations section).

3.4. Sample

Theoretical sampling was applied, and interviewees were selected according to their experience to increase research validity. Examining different companies in seven diverse countries and industries may contribute to *transferability*. The nature and degree of the destructive potential of the insider threat strongly depend on the affected sector or industry (Hills & Anjali, 2017). The most threatened areas are the aerospace, telecommunications, automobile, biotechnology, energy, electrical, and defence industries (Kim, 2020; Pellegrino, 2015). Therefore, the sample was selected based on these industries to ensure relevancy. Data was collected through semi-structured, in-depth interviews with stakeholders in executive positions in the second quarter of 2022. The interviews for the research were undertaken with companies with a high level of innovation that operate in Austria, Bulgaria, England, Germany, Hungary, Poland, and Serbia.

Twenty-one in-depth interviews were conducted with five female and sixteen male respondents between the ages of 35 and 60. (Table 2 contains details about the main features of the respondents.) The data collection occurred during the fourth quarter of 2021 and the first quarter of 2022. Theoretical saturation was reached at the eighteenth interview (after this point, no more novel information emerged). The questions focused on the nature and frequency of the business information outflow incidents and distinguished between intentional and unintentional occurrences from the perspective of the human element.

Table 2

Features of respondents

Interview	Position of respondent	Profile of company	Company size	Country
1.	Owner/CEO	Defence wholesaler	Small	Bulgaria
2.	Lead Developer	IT/ Software engineering	Small	England
3.	Owner/CEO	Defence R&D&I and manufacturing	Medium	Austria
4.	Owner/CEO	Machining part manufacturer	Medium	Austria
5.	Owner/CEO	Defence R&D&I and manufacturing	Medium	Bulgaria
6.	Owner/Engineer	Defence R&D&I and manufacturing	Medium	Hungary
7.	Owner/Engineer	Information safety system developer	Medium	Hungary
8.	CEO	Private security company	Medium	Hungary
9.	Engineer	Defence equipment manufacturing	Medium	Poland
10.	Engineer	Defence R&D&I and manufacturing	Medium	Poland
11.	Owner/CEO	Defence R&D&I and manufacturing	Medium	Serbia
12.	Engineer	Aerospace R&D&I and manufacturing	Large	England
13.	Engineer	Car industry	Large	Germany
14.	Marketing Manager	FMCG	Large	Germany
15.	Engineer	Military vehicle manufacturing	Large	Germany
16.	Marketing Manager	Pharmaceutical industry	Large	Germany
17.	Senior Portfolio Manager	Asset and investment management	Large	Hungary
18.	Engineer	Car industry	Large	Hungary
19.	Financial Manager	FMCG	Large	Hungary
20.	Lead developer	IT/ Software engineering	Large	Hungary
21.	CEO	Pharmaceutical industry	Large	Hungary

Source: authors' construction

4. EMPIRICAL RESULTS AND DISCUSSION

In the course of the research, the experiences of respondents concerning industrial espionage were investigated. The data was collected through in-depth interviews and analysed with grounded theory methodology. The core categories of this research and the relationship among them are depicted in Figure 2.

Two external factors were identified behind the industrial espionage incidents committed by insiders and outsiders among the investigated companies: economic factors, which are connected with the intensifying competition in a competitive market, and financial factors, which refer to the monetary compensation offered by an outsider in exchange for confidential business information. According to the interviewees, a **competitive market environment** is one of the main reasons for the increasing incidence of industrial espionage. The competitive market environment is the result of the globalized nature of the international economy and factors such as the "*increasing value of intellectual property*" (I17), the "*increasing use of outsourcing*" (I5), "*more competitors*" (I9), "*acts of rival companies*" (I18), the fact that "*new technologies emerge every day*" (I21), and the "*growing complexity of communication technologies*" (I12) are all external circumstances that contribute to the increasing number of incidents. Companies gather information and forecast market trends, but to secure their positions, they require information about the plans and activities of rival companies, which they may obtain through industrial espionage. The results show that **financial compensation**, another external factor behind industrial espionage, motivates internal stakeholders to act against a company. This category was classified as an external factor because it usually involves an outsider entity that intends to exchange misappropriated information for financial compensation, as one of the interviewees explained: "*external actors [are] willing to pay for the information*" (I7). The internal stakeholder may participate in this transaction voluntarily, or the external agent may force/encourage the former to cooperate through

"*bribery*" or "*blackmail*", and some of the interviewees also mentioned "*corruption*". Most respondents explained that they regularly educate employees about recognising and protecting themselves against these issues. While this study focuses on internal threats, the effective prevention of industrial espionage requires continuous monitoring of the external environment. Events occurring in the external environment can indirectly or directly impact internal threats.

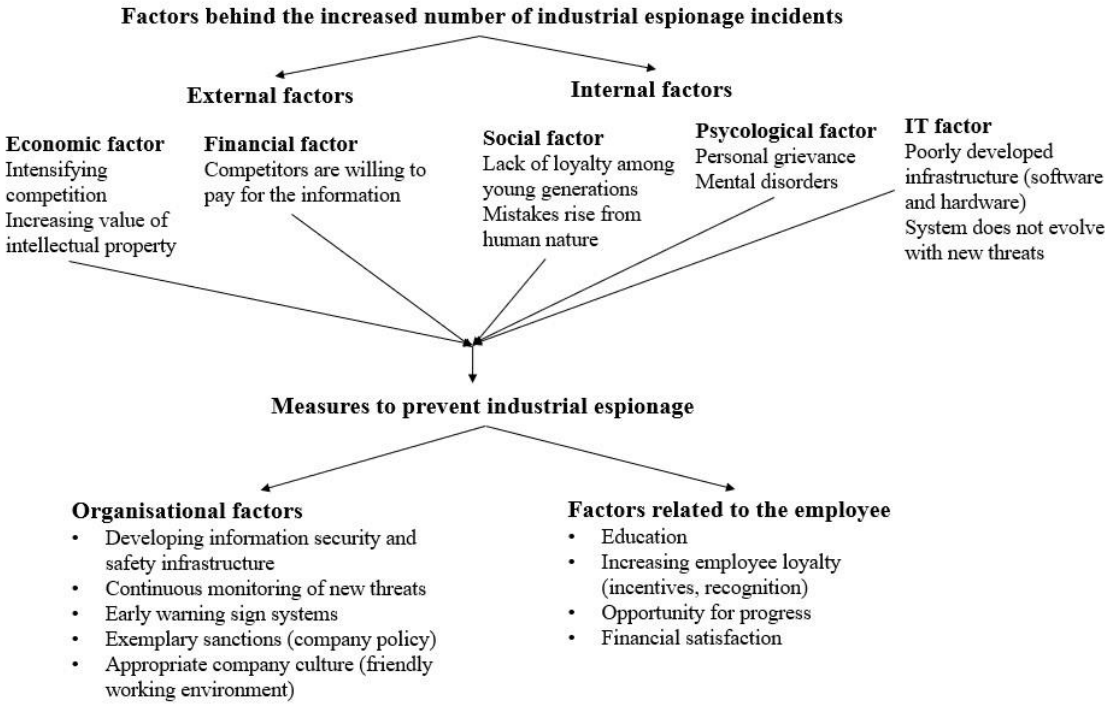

Figure 2. Core categories associated with insider industrial espionage

Source: authors' elaboration based on results

Three internal factors were identified from the perspective of industrial espionage committed by insiders. First, the **social factor** refers to a lack of loyalty among young generations and employee mistakes that arise from human nature. Results indicate that the respondents believe that loyalty among young employees is declining, representing a significant information security and safety issue for their companies. According to the findings, members of the younger generation change workplaces frequently and want to obtain experience at many notable firms within a short period, which poses a risk factor for a company. "*They observe the work process at our company, then some months later they quit and share the knowledge with another company*" (I16). "*It doesn't really matter that we signed a confidentiality contract or a paper saying that they cannot work in the same industry for a few years – they cannot be sanctioned, especially if they go abroad*" (I11). The respondents also reported that *"younger employees expect very high salaries with little work"* (I15), they "*have unrealistic expectations about rapid career progress"* (I7), and "*recent graduates have unreal expectations about the labour market*" (I20). Although the interviewees did not specify exactly which generation they were referring to, they spoke of the "*new generation*" or the "*young generation*", so it can be assumed that the referents were mainly members of generations Y and Z. In contrast, the older generations (presumably Generation X) were socialized in a society where fidelity was considered more valuable. This statement was made by most respondents, regardless of other distinctive features. Understanding young employees' characteristics is crucial for decision-makers so they can implement the appropriate activities to address the issue.

Unintentional **human mistakes** occur because "*employees are only human, and sometimes make mistakes*" (I18). Employees can make mistakes due to "*fatigue*", "*stress*", "*overwork*", "*inattention*", or "*multitasking*", often

because of "*pressure*" from bosses or a competitive environment. In this category, respondents also shared factors such as "*carelessness*", "*negligence*", "*naivety*", and "*gossiping*". Accidental incidents can manifest in various ways, such as sending an email to the wrong recipient or losing an unprotected smart device. In relation to unintentional incidents, whether information outflow events are unintentional or due to employee mistakes they have tried to cover up is a relevant distinction. These factors make it very difficult to deal with and sanction accidental incidents of industrial espionage. Specific information security gaps can be uncovered by investigating cases arising from human errors, necessitating further measures.

The **psychological aspect** involves personal grievance and psychological disorders. The former may develop during an employee's time with a company, while the latter may arise from an earlier trauma or personal issue. The respondents noted factors such as "*repressed anger*", "*revenge*", and "*frustration*" related to personal grievance, which, for example, can arise as a consequence of unethical practices by leadership. Associated with mental disorders, they highlighted "*egoistic*", "*sociopathic*", "*narcissistic*" personalities, "*depression*", and the problems of "*early burnout*" and "*poor upbringing*", which, for example, may be a consequence of childhood trauma. According to the interviewees, the motives for participating in industrial espionage against the company include personal gain, greed, revenge, cultural/ideological differences, or pressure from another individual inside or outside the company. The **information-technology (IT)** factor applies to poorly developed infrastructure and involves the issues of hardware and software information security. The deficiencies of the IT infrastructure may include the "*lack of access and entry control solutions*" (I17), "*lack of continuous development of the system*" (I6), or the absence of "*authentication*" and/or "*authorization*". System vulnerability increases if the company's information infrastructure does not evolve with the new threats that emerge in the environment. From the perspective of insider risk, inadequate security infrastructure increases the possibility of employee mistakes that may lead to unauthorized information outflow. This factor is closely related to the '**human mistakes**' factor, and investigating the vulnerabilities of the IT system may also uncover information security gaps.

During the data collection period, remote work became prevalent in many companies due to the COVID-19 pandemic, presenting a new information security threat from the perspective of industrial espionage. According to the respondents, the home office is expected to remain a part of normal working practice. This compels companies to enable remote access to their information infrastructure. Employees engaged in remote work tend to be "*less attentive to security*" (I2) and "*typically lack network-level security knowledge*" (I7), posing significant risks in terms of both internal threats and external attacks as employees take critical information outside the company.

The above-presented factors have increased **the number of industrial espionage incidents**, which is a significant information security and safety risk. However, companies have means of decreasing and preventing insider risk through organizational and employee-related factors. The risk of industrial espionage needs to be fundamentally addressed on three levels: managing threats posed by internal stakeholders, defining a comprehensive information security policy, and addressing external environmental threats. From the perspective of this research, the first factor is relevant; however, the other two factors are also closely related to the topic.

The organizational factor involves the development of smart and user-friendly **information security and safety** terms and conditions, continuous monitoring of new threats, and proper education about the utilization of such systems. **Monitoring** employee behaviour for **early warning signs** can also provide information that helps to reduce insider threat risk. Defining **sanctions** and penalties associated with company regulations represents one legal approach. These solutions may reduce insider threat risk, but only if employees acknowledge the potentially negative consequences thereof. However, sanctions may negatively impact employees' behaviour and attitude due to increasing pressure and stress. Respondents stated that this form of managing compliance is grounded in intimidating employees. It is necessary to define

organizational factors in the information security policy, which will only be effective if communicated clearly to internal stakeholders.

To reduce insider risk, employees desire a **friendly and convenient working environment** that will help them develop a positive attitude toward the company. "*A person always has some kind of attitude toward the firm, either positive or negative. If positive, they are more likely to act loyally*" (I2). Based on the findings, a positive and stimulating organizational culture involves a friendly and supportive working environment that contributes to employee satisfaction, including a positive relationship between fellow employees and their leaders and effective two-way communication. This requires respect for employees with different cultural backgrounds and providing opportunities for further development. For leaders of innovative companies, establishing an information security culture within the organization can offer significant support for information safety. This involves forming an internal group whose members are loyal to and respect the company and are aware of the potential risks and negative consequences of industrial espionage, thus making information protection a natural aspect of their daily work. Employee education is the most crucial factor in achieving an information security culture.

From the perspective of reducing risk, factors that increase employee loyalty include proper **training and education**, using an **incentive system**, and **ensuring financial satisfaction**. Educating employees about information security, using security systems and handling confidential information can decrease the risk of human mistakes. The results indicate that the appraisal and recognition of employees can support their positive attitude towards a company, thereby increasing loyalty and satisfaction. In addition, the risk of internal attacks can be reduced by providing financial and non-financial incentives to employees. Respondents explained that, from the perspective of internal industrial espionage attacks, monetary incentives play a notable role, as in most cases, an outside entity offers financial compensation for misappropriated information. Figure 3 compares intentional and unintentional cases using categories and subcategories emerged from grounded theory.

The factors identified as behind the global increase in industrial espionage cases have been categorized into external and internal ones. The external factors encompass economic aspects, including intensifying competition and the growing value of intellectual property, and the financial factor, which pertains to an external entity willing to pay for misappropriated information. Although the current study focused on internal threats, understanding external factors is necessary for obtaining more comprehensive insight. The identified internal categories cover social, psychological, and IT factors. Social factors involve the issue of loyalty among younger generations and human-nature-driven errors. Psychological factors involve personal grievances and mental disorders. The IT factor includes deficiencies in digital information security systems. The three identified internal factors are interconnected, either indirectly or directly. For instance, inadequate IT systems can lead to an increase in human errors, and poor management practices can result in deficient IT systems or internal stakeholders becoming resentful. Activities for mitigating the risk of industrial espionage include organizational and employee-related factors. Organizational factors involve tools that leaders can implement that must be incorporated into the information security policy. Employee-related factors increase loyalty among internal stakeholders, with the primary supporting factor being establishing an information security culture. The key findings are summarized in Figure 2 at the beginning of the section.

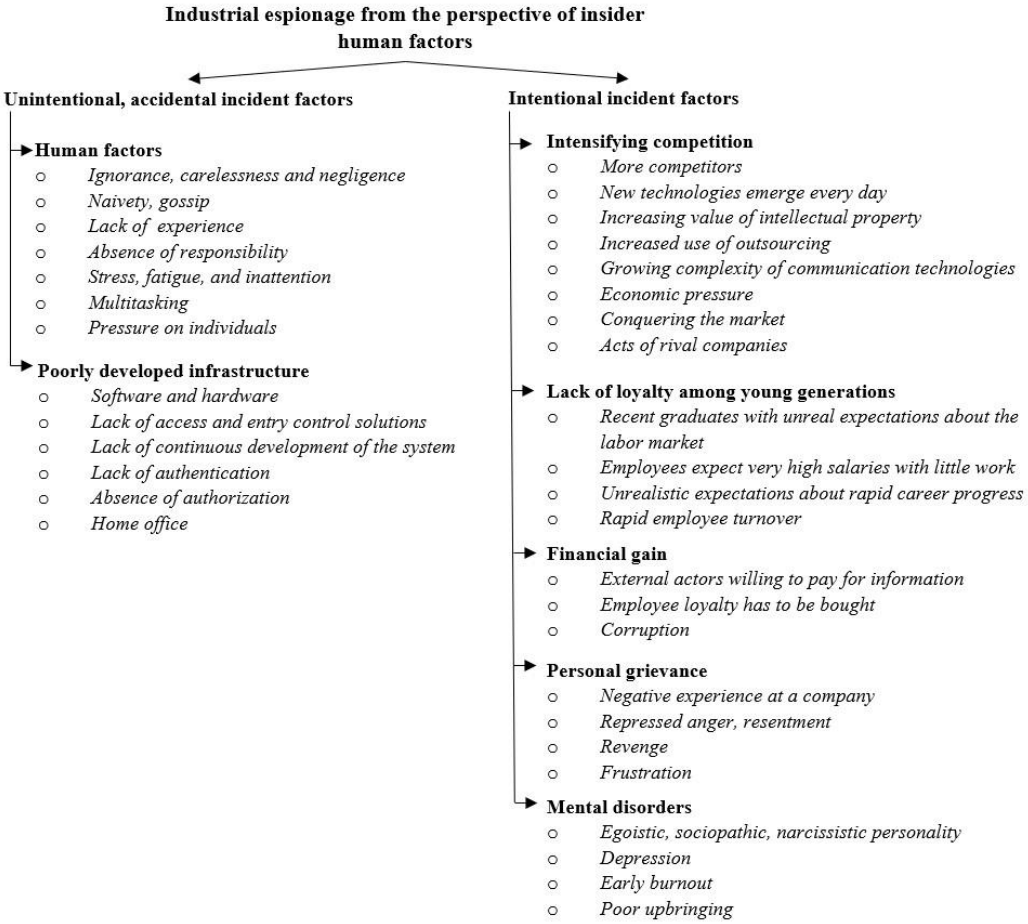

Figure 3. Categories and subcategories analysed with grounded theory methodology

Source: authors' elaboration based on results from using NVivo 12

The deductive nature of the applied grounded theory methodology allows for the comparison of the findings with those of pre-existing literature, ensuring the credibility of the research. The findings confirm that industrial espionage is a complex issue that requires an interdisciplinary approach. The results show that industrial espionage involves economic, social, and psychological factors, corresponding to the findings of Button (2020), Hou and Wand (2020), and Carl (2017). Despite its significant contemporary importance, industrial espionage has received little attention in the academic literature (Brancik & Ghinita, 2011; Button, 2020; Knickmeier, 2020; Elifoglu et al., 2018; Lyan & Frenkel, 2022; Solberg Søilen, 2016; Omar, 2015), perhaps due to its complexity. This paper investigates industrial espionage from the viewpoint of internal human factors, as opposed to a technical, information technology, or legal perspective (Hou & Wang, 2020; Ashenden, 2018; Bedford & Van Der Laam, 2016; Brancik & Ghinita; 2011).

One of the main reasons for the increasing number of industrial espionage incidents is the pressure created by a rapidly changing competitive market (**RQ1**). Market actors may gather information from other competitors using unethical or illegal means, considering this a cost and time-effective approach compared to initiating an internal research and development process. Due to its exceptional industrial and academic research and development, Europe is particularly vulnerable to industrial espionage and attracts interest from emerging countries and competitors. The issue of a dynamically changing competitive market is not directly related to the human factor but significantly impacts events of industrial espionage. Thus, the authors have included this factor in the analysis. The dynamic evolution of market competition puts pressure

on both leaders and employees. The negative behaviour of leaders impacts employees, potentially evoking feelings of anger or a desire for revenge. Under the influence of pressure and stress, internal stakeholders are more prone to making mistakes.

Although there is usually malicious intent behind most intentional acts of insider industrial espionage, according to the literature (Williams et al., 2019; Ashenden, 2018; Elifoglu et al., 2018; Hills & Anjali, 2017; Omar, 2015), the findings of the present study did not confirm this claim. Respondents highlighted that the intention behind industrial espionage incidents is mainly financial compensation or employees' characteristics and attitudes toward a company. The influence of monetary compensation was specified as an external factor (involving an external entity offering monetary compensation for embezzled information) and an insider factor (regarding how a company can reduce the risk of an incident). One example of industrial espionage is when Starwood Hotels accused Hilton Hotels of the latter, grounding their case on a breached employment contract involving two executives. Consequently, Hilton was prohibited from establishing a boutique hotel chain as part of the settlement stemming from an industrial espionage lawsuit by competitor Starwood Hotels (Jameson, 2011). Another case is when a former Google employee allegedly pilfered 14,000 files with information about Google's self-driving technology. He subsequently utilised this information to establish his own self-driving truck venture, which he later sold to Uber (Hou & Wang, 2020). Both cases involved employees acting in exchange for financial reward and causing significant damage to the competitor organization.

The interviewees reported that external actors are increasingly willing to pay for misappropriated information, significantly amplifying the risk of industrial espionage. However, companies can enhance the loyalty of internal stakeholders by providing competitive compensation.

Two psychological factors that lead to industrial espionage are personal grievance and psychological disorders, which are critical issues for companies, being difficult to identify and complex to manage (**RQ2 & RQ3**). The findings of Noonan (2018) also support this statement. From this research perspective, grievances are considered to occur due to the perception of an adverse event experienced at a company. At the same time, psychological disorders may develop prior to employment.

Two reasons were identified behind unintentional acts of industrial espionage: a poorly developed security infrastructure and human mistakes, which can be reduced through smart and user-friendly safety and security systems, along with the ongoing education of employees (**RQ3**). Unintentional incidents happen due to human nature, such as ignorance, carelessness, stress, or fatigue. According to the literature, employee negligence (Ashenden, 2018), mistakes (Goel et al., 2017), unacceptable attitudes, vulnerability to blackmail, stress, carelessness, the loss of devices, and a desire to help others (Williams et al., 2019; Elifoglu et al., 2018; Goel et al., 2017; Omar, 2015) are all factors that arise due to human nature and increase the risk of accidental information outflow. These factors can be managed with frequent warnings and the education of employees about their responsibility to work appropriately with confidential information. However, respondents indicated that the unintentional nature of many incidents was questionable.

The research finds that the social factor behind increasing industrial espionage incidents is exiguous loyalty among younger generations (**RQ3**). However, the authors wish to emphasize that this research focused on individuals specifically predicted to become involved in acts of industrial espionage against a company. Not every 'young' individual should be considered untrustworthy. According to the research of Baran and Kłos (2014), intergenerational cooperation within a company can lead to more diverse teams, which can potentially improve employee performance. Vilčiauskaitė and co-authors (2020) reported that older talents may promote performance, but they have some specific needs compared to younger talents, especially in terms of training and working conditions.

As companies are experiencing more incidents of industrial espionage (Konopatsch, 2020), they must consider how to reduce the risk of insider attacks (**RQ4**). One of the most crucial activities is the definition

of an information security policy that is extended to all organizational processes and is clearly communicated to all internal stakeholders. To protect the company from insider industrial espionage, security measures should be implemented, such as utilizing a reliable information security system and ensuring that strong passwords are used, and sensitive data is encrypted. In addition, the authentication and authorization of users should be guaranteed because this supports a higher level of protection. Limiting access to sensitive information ensures that only authorized persons can access it, and monitoring their access ensures that information is being used appropriately. The information security activities of a company may involve monitoring employee behaviour and employees' computer activity and background checks when recruiting. Employee or document tracking with GPS or RFID technologies can be justified occasionally. Implementing physical security measures such as security cameras, access control systems (such as card access systems or biometric scanners), and other measures can also reduce the risk of insider industrial espionage.

Establishing an information security culture is a crucial instrument for information protection, increasing the loyalty of internal stakeholders and integrating conscious and subconscious information safeguarding into their work. Education serves as the primary means for shaping this culture. Educating employees on protecting critical business information and the consequences of sharing it without authorization can reduce the risk of insider incidents. Proper training should include using security systems, safely handling confidential information and physical documents, secure communication, password management, and protection against bribery or blackmail. During such education, employees should understand the importance of protecting critical business information, which includes explaining why certain information is confidential and how its loss may damage the company. In addition, the sensitive and confidential nature of information should be clearly indicated to employees.

Increasing employee loyalty is also an important factor in decreasing insider risk. Appreciating employees' dedication and hard work, using a recognition system, and providing opportunities for personal growth significantly increase employee loyalty. Ensuring a positive and comfortable working environment and offering competitive compensation and benefits are also essential. In an intercultural working environment, respect for cultural background can contribute significantly to employee loyalty. When analysing employee loyalty, organisational trust also needs to be explored deeply. The question of trust in various social and economic relations has become a subject of wide debate (Krot & Rudawska, 2016). Organisational trust is associated with the enhanced reliability of employees who do not fear making mistakes. The latter may be free to be honest with one another without criticism; this supports innovation and enhances job satisfaction (Bencsik & Juhász, 2020). The main characteristics of a welfare-oriented organization involve a clear focus on well-being creation, committed leadership, a goal-oriented strategy, and the use of multidimensional measures of success that contribute to maintaining and increasing a positive attitude and loyalty to a company (Shrivastava & Zsolnai, 2022). Discretely handling employee failures and avoiding public humiliation is also recommended for preventing negative attitudes or even anger against a company.

The main result of the application of the grounded theory methodological approach is the grounded theory itself. The external factors of intensifying market competition, financial compensation offered for business information, and the internal aspects of the lack of loyalty among young generations, mistakes committed by employees, personal grievances, and psychological disorders have increased the number of industrial espionage incidents. A company can decrease, prevent, or forecast the risk of industrial espionage through organizational processes such as developing an information security infrastructure, creating conditions for improving safety, implementing an employee-behaviour-related monitoring system, defining sanctions in company policy, and creating the conditions for appropriate company culture; additionally, through education and a well-structured compensation system that includes competitive salaries, incentives,

and a recognition system. These initiatives can ensure social, professional, and financial satisfaction, increasing employee loyalty.

5. CONCLUSION

The results of this study provide a deeper understanding of industrial espionage for organizations, managers, and policymakers. It is impossible to define a universally effective information security system that works well in all situations and circumstances, as different internal and external factors can simultaneously affect businesses. However, the research provides a framework for decision-makers that enables them to identify the specific characteristics of different situations and apply the most suitable tools in these contexts. The findings represent a frame for planning and implementing appropriate prevention and protection measures. According to the collected data, managers and policymakers generally do not classify industrial espionage as high risk, so their attention must be drawn to this issue because they play a crucial role in protecting organizations and keeping sensitive information safe from insider industrial espionage. In the future, the role of managers and policymakers in protecting companies will increase further because of constantly evolving security threats. A company's organizational and technological development should be integrated with its human resource development, which may help prevent industrial espionage incidents.

The grounded theory approach applied here may contribute to exploring the problem, although further research is needed to identify the additional features underpinning the complex phenomenon of industrial espionage. For example, further research could explore the methods companies use to deal with the aftermath of an industrial espionage incident, including damage control and employee relations. Additional research can examine the factors behind the declining loyalty to the place of work of the Y and Z generations. Another interesting issue is the impact of employee training on the likelihood of industrial espionage incidents. How managers and policymakers can prepare for ever-changing threats to information security can also be examined.

This qualitative research has limitations due to the sensitive nature of the topic. For the interviews, individuals were contacted who have significant experience in the field of business information security and safety and could share their valuable practical thoughts to enrich the academic literature on this topic. However, the answers provided by the interviewees may sometimes not reflect reality, as they may have wished to keep some information confidential; thus, integrity could only partially be ensured. Many cases of espionage are concealed, and incidents may not be noticed or, if recognized, are seldom reported because of the potential repercussions. When authorities investigate an industrial espionage incident, the results are usually confidential and unavailable for scientific use. The limited scope of this paper and the interdisciplinary nature of this topic hinder the authors from delving deeper into the phenomenon. The topic should be analysed more deeply from several perspectives, such as psychology, jurisprudence, information technology and safety, and security sciences. For these reasons, some aspects of insider industrial espionage may remain hidden. Despite these limitations, the authors have tried their best to explore this problem in depth.

REFERENCES

Andrade, C. (2021). The Inconvenient Truth About Convenience and Purposive Samples. *Indian Journal of Psychological Medicine*, 43(1), 86–88.

Ashenden, D. (2018). In their own words: employee attitudes towards information security. *Information and Computer Security*, *26*(3), 327–337. https://doi.org/10.1108/ICS-04-2018-0042

Baran, M., & Klos, M. (2014). Managing an intergenerational workforce as a factor of company competitiveness. *Journal of International Studies*, *7*(1), 94–101. https://doi.org/10.14254/2071-8330.2014/7-1/8

Barrachina, A., Tauman, Y., & Urbano, A. (2021). Entry with two correlated signals: The case of industrial espionage and its positive competitive effects. *International Journal of Game Theory*, *50*, 241–278. https://doi.org/10.1007/s00182-020-00748-8

Baskerville, R., & Pries-Heje, J. (1999). Grounded action research: a method for understanding IT in practice. *Accounting, Management and Information Technologies*, *9*(1), 1–23. https://doi.org/10.1016/S0959-8022(98)00017-4

Bedford, J., & Van Der Laam, L. (2016). Organizational vulnerability to insider threat. In Stephanidis C. (Ed.), HCI International 2016 – Posters' Extended Abstracts. HCI 2016. *Communications in Computer and Information Science*, *617*, 465–470. https://doi.org/10.1007/978-3-319-40548-3_77

Bencsik, A., & Juhasz, T. (2020). Impacts of informal knowledge sharing (workplace gossip) on organisational trust. *Economics and Sociology*, *13*(1), 249–270. https://doi.org/10.14254/2071-789X.2020/13-1/16

Bhal, K. T., & Leekha, N. D. (2008). Exploring cognitive moral logics using grounded theory: The case of software piracy. *Journal of Business Ethics*, *81*(1), 635–646. https://doi.org/10.1007/s10551-007-9537-7

Brancik, K., & Ghinita, G. (2011). The optimization of situational awareness for insider threat detection. *CODASPY '11: Proceedings of the first ACM conference on Data and application security and privacy*, 231–236. San Antonio, TX, USA. https://doi.org/10.1145/1943513.1943544

Brannen, J. (1988). The study of sensitive subjects. *The Sociological Review*, *36*(3), 552–563. https://doi.org/10.1111/j.1467-954X.1988.tb02929.x

Bratianu, C. (2020). Toward understanding the complexity of the COVID-19 crisis: A grounded theory approach. *Management & Marketing*, *15*(Special Issue), 410–423. https://doi.org/10.2478/mmcks-2020-0024

Button, M. (2020). Editorial: Economic and industrial espionage. *Security Journal*, *33*, 1–5. https://doi.org/10.1057/s41284-019-00195-5

Byrt, T., Bishop, J., & Carlin, J. B. (1993). Bias, prevalence and kappa. *Journal of Clinical Epidemiology*, *46*(5), 423–429. https://doi.org/10.1016/0895-4356(93)90018-v

Carl, S. (2017). An unacknowledged crisis – economic and industrial espionage in Europe. In Spinellis C. D., Billis, N. T. E. & Papadimitrakopoulos, G. (Eds.), *Europe in Crisis: Crime, Criminal Justice and the Way Forward. Essays in Honour of Nestor Courakis*, *2017*(2), 1315–1326.

Carstens, D. S., Miller, J. R., Mahlman, J. A., & Shaffer, M. J. (2021). Internet, social media, and mobile device addiction effects on a workplace. *International Journal of Social Media and Online Communities*, *13*(1), 37–50. https://doi.org/10.4018/IJSMOC.2021010103

Chan, M. (2004). Corporate espionage and workplace trust/distrust. *Journal of Business Ethics*, *42*(1), 45–58. https://doi.org/10.1023/A:1021611601240

Charmaz, K. (2014). Constructing grounded theory. *Sage Publications,* Thousand Oaks, California.

Charmaz, K., & Thornberg, R. (2021). The pursuit of quality in grounded theory. *Qualitative Research in Psychology*, *18*(23), 305–327. https://doi.org/10.1080/14780887.2020.1780357

Chicco, D., Warrens, M. J., & Jurman, G. (2021). The Matthews correlation coefficient (MCC) is more informative than Cohen's Kappa and Brier score in binary classification assessment. *IEEE Access,* 9, 78368–78381. https://doi.org/10.1109/ACCESS.2021.3084050

Collier, J., & Esteban, R. (2007). Corporate social responsibility and employee commitment. *Business Ethics: A European Review*, *16*(1), 19–33. https://doi.org/10.1111/j.1467-8608.2006.00466.x

Corbin, J. M., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative Sociology*, *1990*(13), 3–21. https://doi.org/10.1007/BF00988593

Delannon, N., & Raufflet, E. (2021). Impeding corporate social responsibility: Revisiting the role of government in shaping business—Marginalized local community relations. *Business Ethics, the Environment & Responsibility, 30*(4), 470–484. https://doi.org/10.1111/beer.12378

Delgado, R., & Tibau, X. A. (2019). Why Cohen's Kappa should be avoided as performance measure in classification. *PloS one, 14*(9), e0222916. https://doi.org/10.1371/journal.pone.0222916

Denzin, N. K. (1978). Triangulation: A case for methodological evaluation and combination. In Denzin, N.K. (Ed.), *Sociological methods: A sourcebook*. New York: McGraw-Hill, 339–357.

Dokko, J., Shin, M., & Park, S. Y. (2021). An intelligence criminal tracker for industrial espionage. *Digital Forensics and Cyber Crime*, *351*, 224–230. https://doi.org/10.1007/978-3-030-68734-2_12

Elifoglu, I., Abel, I., & Taşseven, Ö. (2018). Minimizing insider threat risk with behavioral monitoring. *Review of Business: Interdisciplinary Journal on Risk and Society*, *38*(2), 61–73.

Everitt, B. (1996). Making sense of statistics in psychology: A second-level course. Oxford, UK: Oxford University Press.

Gáti, M. & Bauer, A. (2017). Kvalitatív megközelítés a kis- és középvállalatok marketingdöntéseinek szervezeti értelmezéséhez, kiemelten kezelve a vállalatvezető szerepét. *Vezetéstudomány - Budapest Management Review*, 48(12), pp. 41–49. https://doi.org/10.14267/VEZTUD.2017.12.05

Glaser, B. G., & Strauss, A. L. (1967). *The Discovery of Grounded Theory: Strategies for Qualitative Research*. London: Weidenfed and Nicolson.

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems*, *18*(1). 22–44. https://doi.org/10.17705/1jais.00447

Guba, E. G., & Lincoln, Y. S. (1989). *Fourth generation evaluation*. Sage Publication, Newbury Park, California

Heickerö, R. (2019). Cyber espionage and illegitimate information retrieval. *Multigenerational Online Behavior and Media Use: Concepts, Methodologies, Tools, and Applications*, 1725–1736. https://doi.org/10.4018/978-1-5225-7909-0.ch091

Hills, M., & Anjali, A. (2017). A human factors contribution to countering insider threats: Practical prospects from a novel approach to warning and avoiding. *Security Journal*, *2017*(30), 142–152. https://doi.org/10.1057/sj.2015.36

Homoliak, I., Toffalini, F., Guarnizo, J. D., Elovici, Y., & Ochoa, M. (2020). Insight into insiders and IT: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Computing Surveys*, *52*(2), 1–40. https://doi.org/10.1145/3303771

Hou, T., & Wang, V. (2020). Industrial espionage –A systematic literature review (SLR). *Computers & Security*, *98*, 1–12. https://doi.org/10.1016/j.cose.2020.102019

Jameson, D. A. (2011). The rhetoric of industrial espionage: The case of Starwood v. Hilton. *Business Communication Quarterly*, *74*(3), 289–297. https://doi.org/10.1177/1080569911413811

Kim, S.-K. (2020). Intellectual property right infringement, state involvement in industrial espionage, and North-South trade. *Economic Modelling*, *91*, 110–116. https://doi.org/10.1016/j.econmod.2020.05.026

Krot, K., Rudawska, I. (2016), The Role of Trust in Doctor-Patient Relationship: Qualitative Evaluation of Online Feedback from Polish Patients, *Economics and Sociology*, *9*(3), 76–88. https://doi.org/10.14254/2071-789X.2016/9-3/7

Knickmeier, S. (2020). Spies without borders? The phenomena of economic and industrial espionage and the deterrence strategies of Germany and other selected European countries. *Security Journal*, *33*, 6–26. https://doi.org/10.1057/s41284-019-00199-1

Konopatsch, C. (2020). Fighting industrial and economic espionage through criminal law: lessons to be learned from Austria and Switzerland. *Security Journal*, *33*, 83–118. https://doi.org/10.1057/s41284-019-00200-x

Kuzmenko, O., Cyburt, A., Yarovenko, H., Yesh, V., & Humenna, Y. (2021). Modeling of "information bubbles" in the global information space. *Journal of International Studies*, *14*(4), 270-285. https://doi.org/10.14254/2071-8330.2021/14-4/18

Lara, E., Aguilar, L., Sanchez, M. A., & García, J. A. (2020). Lightweight authentication protocol for M2M communications of resource-constrained devices in industrial Internet of Things. *Sensors (Basel, Switzerland)*, *20*(2), 1–22. https://doi.org/10.3390/s20020501

Lee, C. M. (2015). Criminal profiling and industrial security. *Multimedia Tools and Applications*, *74*(5), 1689–1696. https://doi.org/10.1007/s11042-014-2014-2

Lehto, M. (2022). Cyber-attacks against critical infrastructure. *Computational Methods in Applied Sciences*, *54*, 3–42. https://doi.org/10.1007/978-3-030-91293-2_1

Lyan, I., & Frenkel, M. (2022). Industrial espionage revisited: Host country–foreign multinational corporation legal disputes and the postcolonial imagery. *Organization*, *29*(1), 30–50. https://doi.org/10.1177/1350508420928517

Maican, O. H. (2019). Legal aspects of economic espionage. *Perspectives of Law and Public Administration*, *8*(2), 385–392.

Mason, J. (2002). *Qualitative Researching* (2nd ed.). London: Sage Publications.

McGinley, S., Wei, W., Zhang, L., & Zheng, Y. (2021). The state of qualitative research in hospitality: A 5-year review 2014 to 2019.*Cornell Hospitality Quarterly*, *62*(1), 8–20. https://doi.org/10.1177/1938965520940294

Mitchell, B. (2020). Corporate cyberespionage: identification and prevention part 1. *Edpacs*, *62*(5), 1–14. https://doi.org/10.1080/07366981.2020.1798594

Mitev, A. Z. (2012). Grounded theory, a kvalitatív kutatás klasszikus mérföldköve. *Vezetéstudomány*, 43(1), 17–30. https://doi.org/10.14267/VEZTUD.2012.01.02

Morimoto, R., Ash, J., & Hope, C. (2005). Corporate social responsibility audit: From theory to practice. *Journal of Business Ethics*, *2005*(62), 315–325. https://doi.org/10.1007/s10551-005-0274-5

Morris, A. (2015). A Practical introduction to in-depth interviewing (First ed.). London: SAGE Publications Ltd.

Nasheri, H. (2005). *Economic Espionage and Industrial Spying*. Cambridge: Cambridge University Press.

Nejad, B. (2023). Cyber Security. In: *Introduction to Satellite Ground Segment Systems Engineering*. Space Technology Library, *41*. Springer, Cham. https://doi.org/10.1007/978-3-031-15900-8_16

Noonan, C. F. (2018). Spy the lie: Detecting malicious insiders. *United States: Pacific Northwest National Lab (PNNL)*, Richland, WA, United States. https://doi.org/10.2172/1452870

Omar, M. (2015). Insider threats: Detecting and controlling malicious insiders. In Dawson, M. (Ed.), *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*, 162–172. https://doi.org/10.4018/978-1-4666-8345-7.ch009

Patil, D., & Meshram, B. (2018). Network packet analysis for detecting malicious insider. *2018 3rd International Conference for Convergence in Technology I2CT*, 1–8. https://doi.org/10.1109/I2CT.2018.8529451

Pellegrino, M. (2015). The threat of state-sponsored industrial espionage. *2021, European Union Institue for Security Studies. 26*. Retrieved from https://www.iss.europa.eu/content/threat-state-sponsored-industrial-espionage

Riegger, A. S., Klein, J. F., Merfeld, K., & Henkel, S. (2021). Technology-enabled personalization in retail stores: Understanding drivers and barriers. *Journal of Business Research*, *123*, 140–155. https://doi.org/10.1016/j.jbusres.2020.09.039

Rothke, B. (2001). Corporate espionage and what can be done to prevent it. *Information Systems Security*, *10*(5), 1–7. https://doi.org/10.1201/1086/43315.10.5.20011101/31716.3

Sadok, M., Welch, C., & Bednar, P. (2020). A socio technical perspective to counter cyber enabled industrial espionage. *Security Journal*, *2020*(33), 27–42. https://doi.org/10.1057/s41284-019-00198-2

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K.-K. R., & Burnap, P. (2020). impact and key challenges of insider threats on organizations and critical businesses. *Electronics*, *9*(9), 1460. https://doi.org/10.3390/electronics9091460

Scanlan, C. L. (2020). *Preparing for the Unanticipated: Challenges in Conducting Semi-Structured, In-Depth Interviews* (First ed.). London: SAGE Publications Ltd. https://dx.doi.org/10.4135/9781529719208

Schiller, C. A. (2019). Counter-economic espionage. In Tipton, H.(Ed.). Information Security Management Handbook: Volume IV, 67–88. (1st ed.). Auerbach Publications. https://doi.org/10.1201/9781351073547

Shelupanov, A., Nemirovich-Danchenko, M., & Glukhareva, S. (2021). Decision-making in the recommendation system of personnel security of the company. *Journal of Physics: Conference Series, 33*(5) 1–5. https://doi.org/10.1088/1742-6596/1989/1/012045

Shrivastava, P., & Zsolnai, L. (2022). Wellbeing-oriented organizations: Connecting human flourishing with ecological regeneration. *Business Ethics, the Environment and Responsibility*, *31*(2), 386–397. https://doi.org/10.1111/beer.12421

Solberg Søilen, K. (2016). Economic and industrial espionage at the start of the 21st century - Status quaestionis. *Journal of Intelligence Studies in Business*, *6*(3), 51–64. https://doi.org/10.37380/jisib.v6i3.196

Strauss, A., & Corbin, J. (2015). Basics of qualitative research: Techniques and procedures for developing grounded theory. 4th ed. *Sage Publications,* Thousand Oaks trustworthiness in naturalistic consumer research. In SV - Interpretive Consumer Research, Hirschman, E. C. (Ed.) California.

Thorleuchter, D., & Van den Poel, D. (2013). Protecting research and technology from espionage. *Expert Systems with Applications*, *40*(9), 3432–3440. https://doi.org/10.1016/j.eswa.2012.12.051

Vilčiauskaitė, B., Savanevičienė, A., & Navickas, V. (2020). Managing older talents in the context of aging society. *Economics and Sociology*, *13*(4), 213–226. https://doi.org/10.14254/2071-789X.2020/13-4/13

Wallendorf, M., & Belk, R. W. (1989). Assessing *Association for Consumer Research special volumes*. Provo, USA, 69–84.

Williams, M. L., Levi, M., Burnap, P., & Gundur, R. V. (2019). Under the corporate radar: Examining insider business cybercrime victimization through an application of routine activities Theory. *Deviant Behavior*, *40*(9), 1119–1130. https://doi.org/10.1080/01639625.2018.1461786

Williams, B., Soulet, M., & Siraj, A. (2023). A Taxonomy of Cyber Attacks in Smart Manufacturing Systems. In Knapčíková, L. & Peraković, D. (Eds.), 6th EAI International Conference on Management of Manufacturing Systems. *EAI/Springer Innovations in Communication and Computing*. Springer, Cham. https://doi.org/10.1007/978-3-030-96314-9_6

Wilson, Y., Hingnikar, A. (2023). Looking into the Crystal Ball. In: Solving Identity Management in Modern Applications. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-8261-8_21

Yin, R. K. (2001). Qualitative Research Methods. *Designing case studies*, 5(14), p. 359–386.

Zamawe, F. C. (2015). The implication of using NVivo software in qualitative data analysis: Evidence-based reflections. *Malawi Medical Journal*, *27*(1), 13–15. http://dx.doi.org/10.4314/mmj.v27i1.4

Zaytsev, A., Malyuk, A., & Miloslavskaya, N. (2017). Critical analysis in the research area of insider threats. *2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud)*, 288–296. https://doi.org/10.1109/FiCloud.2017.16