ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 9 Number 1 (September)
http://doi.org/10.9770/jesi.2021.9.1(8)

Publisher
http://jssidoi.org/esc/home

ICT SECURITY IN BUSINESSES – EFFICIENCY ANALYSIS

Ágnes Kemendi [1], Pál Michelberger [2], Agata Mesjasz-Lech [3]

[1] Doctoral School of Safety and Security Science, Óbuda University, Népszínház utca 8, 1081 Budapest, Hungary
[2] Donát Bánki Faculty of Mechanical and Safety Engineering, Óbuda University, Népszínház utca 8., 1081 Budapest, Hungary
[3] Faculty of Management, Czestochowa University of Technology, Dabrowskiego 69, 42-201, Czestochowa, Poland

E-mails: kemendi.agnes@uni-obuda.hu; michelberger.pal@bgk.uni-obuda.hu; agata.mesjasz-lech@wz.pcz.pl

Received 10 March 2021; accepted 26 May 2021; published 30 September 2021

Abstract. The purpose of this paper was to identify ICT security measures and to assess the level of ICT security in small, medium and large enterprises in spatial terms. The measures in the ICT security area were identified based on secondary data of European Union member states retrieved from the Eurostat database. The research used the CCR Date Envelopment Analysis (CCR-DEA) model to meet the research purpose.The research identifies countries where ICT security results were achieved with the optimum combination of expenditures, i.e. the so-called fully efficient countries. The authors demonstrate that the countries participating in the optimal shared technology are aligned to non-fully efficient countries and they can achieve their results at lower expenditures. In the optimal technologies of all non-fully efficient countries the volume of the achieved results of enterprises is slightly higher than the actual volume. Research conducted in the area of enterprise ICT security rarely focuses on the efficiency of actions undertaken. The authors of this paper examine the technical efficiency in the area of enterprise information security in spatial terms and formulate conclusions about enterprises in the EU member states. The application of the expenditure-oriented CCR-DEA model identifies countries that achieve their results fully utilising their expenditures and those that are able to achieve at least the same results as achieved by non-fully efficient countries but at lower expenditures. The technical efficiency analysis of actions undertaken represents the starting point for defining good practices and success factors in the area of ICT security, both at enterprise and country levels.

Keywords: businesses; efficiency analysis; ICT security; ICT risk management

Reference to this paper should be made as follows: Kemendi, A., Michelberger, P., Mesjasz-Lech, A. 2021. ICT security in businesses – efficiency analysis. *Entrepreneurship and Sustainability Issues*, 9(1), 123-149. http://doi.org/10.9770/jesi.2021.9.1(8)

JEL Classifications: C80, C67, M15

Additional disciplines information and communication, mathematics

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 9 Number 1 (September)
http://doi.org/10.9770/jesi.2021.9.1(8)

1. Introduction

Modern-day organisations are operating in the age of continuous real-time exchange of information. As information is the foundation of the decision-making process, effective competition requires organisations to have access to information and to be able to disseminate information among their stakeholders (Naicker et al., 2019). For this reason, it is necessary to ensure information security so that information can be used for making key business decisions. Indeed, while bringing numerous advantages to organisations, information technology has also made information security the main problem for organisations relying on the technology (Safa et al., 2018). Better understanding and acceptance of safeguards is an inherent element of the information security practice (Burdon & Coles-Kemp, 2019). Identification of good practices is needed (Brunner et al, 2020; Hoffmann et al, 2020; Tøndel et al, 2014), the more so as enterprises still fail to learn from security incidents (Ahmad et al, 2015). Security of computer information systems, commonly termed as cybersecurity, is an important operational issue for nearly each organisation (Solak & Zhuo, 2020). Security-related tasks can be very complex (Sönmez, 2019). For this reason, the literature on the subject includes models, which support the enterprise management process in terms of information security by raising awareness on security factors, which need to be taken into account in the decision-making process (Diesch et al, 2020). Furthermore, information security research focuses on information security data exchange, threat intelligence sharing or information security data sources, like vulnerability databases (Sauerwein et al, 2019).

However, there have been no studies assessing the level of enterprise security in geographical and structural terms in the context of the efficiency of the actions taken. Therefore, the following research questions have been asked:
Q1: How do the development of information society and digital economy affect the enterprise information security?
Q2: Does the available data allow defining measures which reflect the level of enterprise ICT security expenditure and achieved results in spatial terms?
Q3: Are there any tools which provide for assessing enterprise ICT security in spatial terms taking into account effects in this respect and expenditure incurred to achieve those effects?
Q4: Are there any differences in the level of the information security methods in small, medium and large enterprises?

To answer the questions, the following research hypotheses have been formulated:
H1: The ICT security methods in enterprises provide for creating a system of measures for assessing the ICT security in the context of expenditures and results in enterprises in terms of geography.
H2: An assessment of the enterprise ICT security level in spatial terms carried out with appropriate tools will allow identifying the countries where the enterprise ICT security level requires improvement and, most importantly, finding reference objects in the test group.

The proposed research method allows ranking EU countries in terms of ICT security taking into account the efficiency of actions taken respectively. The country ranking may in turn be used to facilitate best practices sharing which can constitute the foundation of national or international information security policies, to set priority goals in the area of ICT security practices and to identify the best means of achieving the goals. Furthermore, the analyses conducted will allow assessing the level of ICT security of enterprises active in specific markets, which can enhance trust in economic transactions made in those markets.

Considering the level of development and use of information and communication technologies, a comprehensive and scientific system needs to be created which will enhance technical breakthroughs, develop system recovery technologies and take various effective measures to prevent and respond to security risks (Guo & Wang, 2020). Best practices of enterprises with sound ICT security measures will serve as role models for other entities.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 9 Number 1 (September)
http://doi.org/10.9770/jesi.2021.9.1(8)

The study contributes to the literature on the subject in three following respects. Firstly, the variables that determine the outlays and effects in the area of ICT security of enterprises have been identified.

Correct identification of variables is a key stage in the efficiency analysis and ensures its credibility. Secondly, the usefulness of the set of variables in the diagnosis of information security activities of enterprises in individual states of the European Union was verified. A set of variables that measure inputs and outputs in information security was used to assess the efforts of enterprises to achieve results in the area of ICT security. Thirdly, research to date in the field of ICT security in enterprises rarely focuses on the effectiveness of actions taken. Moreover, technical efficiency in the area of information security in enterprises was examined, but in spatial terms, which allowed for formulating conclusions regarding enterprises operating on the markets of individual European Union countries.

2. Literature review

Context of the Information society and digital economy

The digital spread was revolutionary in the last decades with a wide range of opportunities that are available through the new technologies, the rapid growth of the internet, WAN. Information and communication technology (ICTs) sector is the pioneer of the digital economy. New technologies, particularly artificial intelligence (AI) reshape the labour market that comes on one hand, with creation of jobs in some sector but on the other hand, with disappearance of others.

Digital advances have generated enormous but concentrated wealth around minor number of individuals, companies and countries. New key risk areas have been created: cybersecurity, privacy concerns, facilitation of illegal economic activities or digital disruptions are amongst the major concerns (UNCTAD, 2019).

Information has become swiftly available and there is actual oversupply of information. Beyond the obvious positive impacts, this carries also some negative aspects. The quality of information might be questionable, the origin of sources may lead to confusion and as such can cause indecisiveness; overall this can result in higher information costs. The so called TIME markets – telecommunication, information technology, media technology, and entertainment – form the basis of the network economy or Net Economy. This Net Economy now coexists with and evolves next to the - physical products and/or services focused - Real Economy (Kollmann, 2006).

The orientation of information, communication and transaction processes within Net Economy have evolved from the supply-orientated Web 1.0, then to the membership-orientated Web 2.0, and to the demand-oriented Web 3.0. (Kollmann et al, 2016).

In the digital age, information and knowledge have central role; the concept of both information and knowledge society have been created. Information society describes the technological options related to the electronic age; knowledge society gives prominence to the problems and strategies of making sense of information (Krohn, 2001).

The concept of the new social structure promoted by Castells is the so-called network society: society made of networks in all the key dimensions of social organization and social practice. This network society is considered as a global system (Castells, 2010).

The Industry 4.0 refers to the fourth technological revolution and follows the third revolution known as “Information Age” that developed to “knowledge-based economy” (Pereira et al, 2017).

The term information society is defined in the EUR-Lex, European Union Law Glossary as a „society where a significant degree of activity focuses on the creation, distribution, use and reuse of information.” This happens through the means of Information and communication technology (ICTs) (EUR-Lex Glossary, n.d.).

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 9 Number 1 (September)
http://doi.org/10.9770/jesi.2021.9.1(8)

„ICT covers all technical means used to handle information and aid communication. This includes both computer and network hardware, as well as their software" as defined in the European Commission Eurostat database (Eurostat Glossary, n.d.). ICT has economic contribution to growth (Goodridge et al, 2019).

ICTs – defined as the combination of all company's audio-visual, telephone, and computing networks – used to be costly and were deployed by companies carefully, however, advances in connectivity, cloud computing, and other technologies are easier to be adopted. Services can turn IT into an affordable resource, regardless of company size (Bossert & Laartz, 2018).

In harmony with the requirements of the information economy an industrial enterprise need to define a strategy that consider automation, robotization and business processes (Kwilinski, 2018). This new era has brought numerous positive impacts, however, a number of challenges and new risks still are to be addressed. These challenges are basically round the digital vulnerabilities and the digital divide that arose as a result of the digital transformation. The digital sphere has opened up new opportunities for criminals; new security threats appear such as cyber-crime, data theft. The role of security measures and relevant control procedures at the enterprises focusing on mitigating these risks are fundamental and inevitable to maintain a stable operation.

With regards information society the inclusion and exclusion exists meaning that participation is not available unconditionally. In addition to the access to online information, the digital divide is about the different uses, misuses and abuses of information (Segev, 2010).

Identification of the ICT security problem - definition of ICT security

ICT is an extremely developing, innovative sector, which fulfils strategic role in the European Union. In the context of today's knowledge-based, resp. information society, the management and use of information has become the key to success, which can lead to competitive advantages in the market. The use of the ICT services is becoming more and more widespread amongst businesses. By now ICTs have become fundamental infrastructure and promote the knowledge-based digital society. The spread of information with the means of information communication has almost no boundaries. Networking is general. Information flows in and out. ICT systems are naturally vulnerable to security threats. In the digitalized world the connection is built through ICTs and this is a key concern if the system is compromised, misused or attacked (OSCE Cyber/ICT security, n.d.). The Internet threat landscape have changed, there is a significant shift toward well-organized cyber-crime carried out in a targeted manner circumventing common security measures (Skopik et al, 2016). Enterprises constantly experience information security related incidents, which are very likely to disrupt their business operations and threaten the information security (Ahmadian et al, 2020; Evans et al, 2019; Bartnes et al, 2016).

Internet of things (IoT) – that refers to Internet-connected devices such as sensors, radio frequency identification (RFID) chips that are embedded in objects enabling them to send and receive various kinds of data (Digital McKinsey, 2018) – is built on the basis of the Internet, thus security problems of the Internet will also show up in IoT devices. This requires customized security and privacy levels to be guaranteed, and solutions that ensure confidentiality, access control, and privacy for users and things, trustworthiness among devices and users, compliance with de-fined security and privacy policies (Tewari & Gupta, 2020). „Security is like a chain. It is as strong as its weakest link. Security depends on people more than on technology. Employees are far greater threat to information security than outsiders" (Technical Department of ENISA, 2006). The threat of humans to information protection can be minimized by ideal or strong information security culture (Veiga et al, 2020).

Information technology has widened the scope of management; in addition to organizational performance, productivity and human resources perspectives, information security should be considered as a responsibility of management, which has also an impact on the market position (Soomro et al, 2016). Entities need to build resilience to ensure smooth operation: to provide appropriate response to these threats, adequate control measures are necessary. The use of ICT services can generate value added in the operation of a business. However, all this

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 9 Number 1 (September)
http://doi.org/10.9770/jesi.2021.9.1(8)

requires special attention from security point of view; security measures ensuring proper control are needed. Security measures play an important role in the security system of businesses, which are highly exposed to security risks related to ICT.

The e-commerce segment of business channels - depending on the volume of segment - underpin the need for adequate protection. The parameters of the process on ICT security measures can be described through a typical action plan – who does what, when, where and what evidence this – with the help of control operations. These security elements can be automatic, manual, or semi-automatic, semi-manual operations. The planning of activities shows who / what does it.

The implementation of the process is supported by an appropriate process documentation and operation, as well as by providing appropriate information to the stakeholders.

The model of information security factors for decision makers shows that there are key security-indicators, which directly impact the security-status of an organization while other indicators are only indirectly connected.

The identified key security-indicators are

- "Physical security" (in practice: physical protection of buildings, offices, servers, and hardware),
- "Vulnerability" (in practice: known vulnerabilities within systems and software),
- "Access control" (in practice: the management and regulation of access to systems, applications, data, and infrastructure),
- "Infrastructure" (in practice: knowing all systems, software and the connections between them and if they are secured or not; „strengthening" of all available systems, prepare threat models and secure the infrastructure in each network layer),
- "Awareness" (in practice: all topics that concern people and cannot be treated with technology) (Diesch et al, 2020).

The Castle Model that has „the defence as walls" approach on cybersecurity – with a safe inside and a dangerous outside – is also worth to be mentioned here. This approach leaves namely a blind spot. Organizations open up their walls and make their gateways more „leaky" so that they can do more, faster and better. Walls from the outside are increasingly destroyed by technological developments. The Millennial generation tend to mix professional and private life. All these factors call for a new approach to cybersecurity (Leuprecht et al, 2016).

„ICT security refers to relevant incidents as well as measures, controls and procedures applied by enterprises in order to ensure integrity, confidentiality and availability of their data and ICT systems" as defined by the Eurostat database. A set of security measures is also compiled to describe this (Eurostat, n.d.). Good practices are required to ensure that the processes of the enterprise are designed and operated in a way that the enterprise is resilient towards the ICT challenges.

Control measures related to ICT security

There is sound European approach on digital transformation that is covered underneath not exhaustively. The adoption of Regulation 1025/2012 on European standardization emphasised „the fast evolution of ICT and the way in which new products and services, such as 'smart' or connected devices (referred to as the 'Internet of Things' or IoT) or the Cloud, transform markets (Regulation (EU) No 1025/2012, 2012). The Commission has identified the following priority areas as the essential technology building blocks of the Digital Single Market: cloud computing, the internet of things (IoT), 5G communications, cybersecurity and (big) data technologies (European Commission, 2016). The so-called 2020 Rolling plan for ICT standardisation has a unique link between EU policies and standardization activities in the field of ICT (European Commission, 2020).

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 9 Number 1 (September)
http://doi.org/10.9770/jesi.2021.9.1(8)

The Directive on security of network and information systems (NIS Directive) is the first EU level legislation on cybersecurity. The deadline for the transposition into national legislation was by 9 May 2018, and by 9 November 2018 for the identification of operators of essential services. Energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure count among the sectors that heavily rely on ICTs. Businesses identified as operators of essential services have to take appropriate security measures and notify serious incidents to the relevant authority.

This is applicable also for search engines, cloud computing services and online market places as well as they are key digital service providers. A culture of security across sectors is in the focus (European Commission, NIS Directive, 2020).

Data has been defined as the fuel of digital economy. In the context of ICT the role of data protection becomes key issue. The EU directive 2016/679 – known as GDPR – meant to protect natural persons with regard to the processing of personal data and on the free movement of such data (REGULATION (EU) 2016/679, 2016).

The EU's digital strategy "A Europe fit for the digital age" count among the six Commission priorities for 2019-24 with policy areas of Data protection; Better access to online goods for consumers and businesses; The right environment for digital network and services; Economy and Society and the European Data Strategy. New rules on e-commerce were introduced which are key elements of the Digital Single Market Strategy: the revised Payment Services Directive and new rules on cross-border parcel delivery services (already in force), new rules to stop unjustified geo-blocking (entered into force on 3 December 2018), revised consumer protection rules (will enter into force in 2020), new VAT rules for online sales of goods and services (will enter into force in 2021) (European Commission, 2021).

The Organization for Security and Co-operation in Europe (OSCE) - that has 57 participating States from Europe, Central Asia and North America (OSCE, n.d.). - names the key challenge that ICTs made the offence easy and defence difficult. This organization has a special role in strengthening cyber/ICT security with particular focus on reducing the risks of conflict arising from the use of ICTs - with the so-called confidence-building measures (CBMs) - between its participating States. Protecting ICT-enabled critical infrastructure as part of enhancing cyber resilience in the OSCE region for the favour of all. The OSCE also pays particular attention to tackling cyber/ICT security threats such as organized criminals and terrorists (OSCE, n.d.).

Information security standards such as ISO/IEC 27001:2013 mark information security policies as mandatory. Albeit, there is little guidance on how to develop good and effective policies. Currently organization-specific information security needs are in the focus of information security policy development (Paananen et al, 2020).

ICT risks in the context of manufacturing industry, service-oriented organizations and e-commerce

The new technological solutions are usually associated with unexpected risks due to security vulnerabilities.

The different entity sizes – small, medium or large enterprises – and businesses may face and address the risks differently. The more so as the findings of studies conducted to date show that the current perception of information risk and readiness to take such risk are low, especially among small economic entities (Line et al, 2016).

Proper risk management process is necessary for each companies to ensure the stable operation. Due to their significant role, the author covers the risk areas of the manufacturing industry, the service-oriented organizations and the e-commerce business model.

ICT activities are adopted in most of the industry activities, but especially in logistics and production operations (Barreto et al, 2017).

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 9 Number 1 (September)
http://doi.org/10.9770/jesi.2021.9.1(8)

The *manufacturing industry* – with its processes well supported by ICT - face increased security risks due to the new technologies, the spread of Industry 4.0, cloud-based systems, IoT, Big Data, BYOD (Bring Your Own Device) and CYOD (Choose Your Own Device) trends. The security implications of the evolving smart systems should be addressed. Employees need to be properly trained. The interconnected organizational systems pose significant security risks. Hackers with malicious intent benefit from software vulnerabilities. The era of Industry 4.0 is greatly exposed to cyber-espionage. High value assets should be protected with a security approach that contains data loss prevention solutions as well as encryption algorithms. The industrial sector run the risk of Denial-of-Service (DoS) causing that a system or an application is unavailable (for instance, overloading a server with massive number of requests to consume the available system sources); DoS attacks are very difficult to control; are often unforeseeable. These attacks cause not only operational issues but the remediation is usually expensive (Pereira et al, 2017).

In *service-oriented systems* the key issues of the security management process are identity management; proper security controls management; security management sovereignty; seamless connection to other organizations on a real-time basis (security of the communication protocols of the services) and protection of data in transit and rest (Dudziak-Gajowiak et al, 2019).

E-commerce is one of the components of the digital economy (UNCTAD, 2019). In the e-commerce context, the critical and vulnerable points of system security are hardware, software and environment. The basic security threats are

- Denial-of-Service (DoS) – see above
- SQL Injection – let a malicious user execute commands in the application's database by using the privileges granted to the application's login
- Price Manipulation – very common whereby the final payable price is manipulated by the attacker using a web application proxy.
- Session Hijacking – takes control of a user session after successfully obtaining or generating an authentication session ID.
- Cross-site script (XSS) – special case code injection; the hacker fold malicious content into the content being delivered from the compromised site which appears at the client-side web-browser as it has been delivered from the trusted source.

Viruses, worms, Trojan horse, bots, EXE file, browser parasites, adware, and spyware etc. are also used by attackers to compromise the security of the e-commerce systems. Secure site design – to be both proactive and reactive in handling security threats - is up to the development team and up to the shopper (Singh, 2014).

3. Research methodology

Data description

In order to verify the hypotheses, a database was constructed consisting of the following variables:

1. variables characterizing the results of DEA:
   - Enterprises did not experience any problem due to ICT security incident: unavailability of ICT services (OUT_ unavailability),
   - Enterprises did not experience any problem due to ICT security incident: destruction or corruption of data (OUT_destruction),
   - Enterprises did not experience any problem due to ICT security incident: disclosure of confidential data (OUT_disclosure),
2. variables characterizing DEA inputs:
   - Enterprises using any ICT security measure (IN_measure),
   - Enterprises having insurance against ICT security incidents (IN_insurance),

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 9 Number 1 (September)
http://doi.org/10.9770/jesi.2021.9.1(8)

- The enterprise's ICT security policy was defined or most recently reviewed within the last 12 months (IN_policy),
- Enterprises make persons employed aware of their obligations in ICT security related issues (IN_obligations),
- In the enterprises the ICT security related activities are carried out by own employees or external suppliers (IN_suppliers).

The "Enterprises did not experience any problem due to ICT security incidents: unavailability of ICT services" (OUT_unavailability) variable shows the share of enterprises which use computers and which in 2019 did not report any unavailability of ICT services due to overloads, failures and human errors occurring during introduction of updates (including in networks, applications, configuration). Continuous availability of ICT services can be ensured by means of adequately efficient hardware and systems as well as through creating redundant configurations, where key computer system components (including inter alia servers, network and security devices) are composed of many elements, so that when one element fails, another operational element can take over its tasks.

The "Enterprises did not experience any problems due to ICT security incidents: destruction or corruption of data" (OUT_destruction) variable shows the share of enterprises which use computers and which in 2019 did not report any destruction or corruption of data due to, mainly, software or physical destruction or damage of data carriers. Since the methods of destruction or corruption employed do not always allow recovery of data, enterprises should avoid situations which may lead to loss of data.

The "Enterprises did not experience any problems due to ICT security incidents: disclosure of confidential data" (OUT_disclosure) variable shows share of enterprises which use computers and which in 2019 did not lose any confidential data. Safeguarding information which is critical to further operations and the future of an enterprise is fundamental to running a business.

Confidentiality most often covers commercial and financial information, business development plans and strategies, customer and contractor databases, product and service information as well as the related know-how. The obligation to keeping such information confidential rests on employees as well as contractors and clients to whom it is provided when establishing cooperation (e.g. during negotiations) and thereafter.

Therefore, the effect-related variables express the security level achieved by enterprises for their computer systems with respect to individual functions of these systems as well as confidential information gathered and processed there. These effects are ensured by putting in place appropriate procedures and deploying methods and technologies which ensure correct and efficient implementation of these procedures. The expenditure-related variables express capabilities of enterprises on the expenditure front. One should remember that perpetrators of security incidents (including insider criminals) can use the cyberspace only to a limited extent to generate threats by using gaps and vulnerabilities in security systems (Szczepaniuk et al, 2020). Therefore, actions taken can reduce the number of security incidents even further.

The "Enterprises using any ICT security measure (IN_measure)" variable shows the share of enterprises which use computers and which in 2019 used any ICT security measure, in particular: keeping the software (including operating systems) up-to-date; user identification and authentication via biometric methods implemented by the enterprise; encryption techniques for data, documents or e-mails; data backup to a separate location (including backup to the cloud); network access control (management of access by devices and users to the enterprise's network); VPN (Virtual Private Network extends a private network across a public network to enable secure exchange of data over public network); maintaining log files for analysis after security incidents; ICT risk assessment, i.e. periodically assessment of probability and consequences of ICT security incidents; ICT security tests.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 9 Number 1 (September)
http://doi.org/10.9770/jesi.2021.9.1(8)

The "Enterprises having insurance against ICT security incidents" (IN_insurance) variable shows the share of enterprises which use computers and which in 2019 implemented the security method involving transfer of effects of security incidents onto other entities. Having such insurance allows minimisation of losses which may arise in the event of an incident or a series of incidents that directly jeopardise information security, especially such aspects as confidentiality, integrity and availability.

The "Enterprise's ICT security policy was defined or most recently reviewed within the last 12 months" (IN_policy) variable shows the share of enterprises which use computers and which in 2019 developed or verified their security policies. A key instrument to reduce information security threats is to create deploy and enforce information security policies (Jaeger et al, 2020). Information security policy is an internal document to ensure information asset and information technology security with a specific procedure to support the organization objectives (Angraini et al, 2019). A security policy includes a list if physical and technical safeguards, data processing locations, information on personal data processing software. A security policy includes also the assessment of information security threats, which is among key obligations of decision-makers in the area of information security (Schmitz & Pape, 2020), and it should take into account stakeholder feedback regarding the security methods deployed (Samonas et al, 2020). Employees' non-compliance with organisational information security policy have become the main reason for continuous security incidents (Liu et al, 2020).

The "Enterprises make persons employed aware of their obligations in ICT security related issues" (IN_obligations) variable shows the share of enterprises which use computers and which in 2019 implemented practices aimed at increasing their employees' awareness in ICT security related issues, e.g. by organising voluntary training or disseminating information within the company; organising mandatory training or obliging employees to familiarise themselves with information prepared by the employer; signing clauses or commitments. Information security training allows organisations to raise awareness among employees about ICT security best practices (Abraham & Chengalur-Smith, 2019). Training is important for the development of employees' information security behaviour (Karjalainen et al, 2020). Currently, in information security, employee behavior and social factors are as important as the physical and logical resources of an organization (Shameli-Sendi, 2020).

The "In the enterprises the ICT security related activities are carried out by own employees or external suppliers" (IN_suppliers) variable shows the share of enterprises which use computers and which in 2019 employed ICT security personnel.

Enterprises can employ various strategies – they can either engage their own employees to take care of ICT security or commission this task to external entities. Whatever strategy is employed by an enterprise, personnel adequately trained in security procedures ensures the security of its ICT assets.

The analyses were made for the year 2019 for small, medium and large enterprises. The enterprise structure approach will allow observing changes in the level of ICT security of enterprises depending on their size. Due to the availability and completeness of data, 28 EU countries for small and large enterprises and 27 EU countries for medium enterprises (excluding Portugal) will be analysed.

Stages of DEA modelling

Data Envelopment Analysis (DEA) is a non-parametric method for the measurement of efficiency in multi-dimensional situations. It allows evaluating the performance of a set of units called decision-making units (DMUs), which are characterised by multiple inputs and outputs (Zu et al, 2018).

DEA provides for finding the best combination of resources held within a specific technology (Anokhin et al, 2011) - i.e. determining the technical efficiency. At present, DEA is considered as one of the most effective approaches to evaluating unit efficiency (Chen, 2018; Premachandra et al, 2011).

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 9 Number 1 (September)
http://doi.org/10.9770/jesi.2021.9.1(8)

DEA is a non-parametric method for the assessment of the efficiency of each set of comparable decision-making variants (Saen, 2010). DEA models provide for determining the efficiency of an object on the basis of an efficiency indicator taking into account multiple expenditures and results at the same time (Song et al, 2011).

In order to assess the technological efficiency European Union countries, the author has:

1. defined set *J* of objects assessed $O_1, \ldots, O_j$, J=28,
2. defined set *R* of the results to be the basis for the efficiency assessment of the objects examined, R=3,
3. determined set *N* of expenditures which allow achieving the pre-determined results, N=5,
4. defined the volume of the object-specific results y_{rj} ($r = 1, 2, 3, j = 1, \ldots, 28$) and expenditures x_{nj} ($n = 1, \ldots, 5, j = 1, \ldots, 28$),
5. defined the relative technological efficiency for respective objects.

One must bear in mind that expenditures are the amounts, which allow achieving certain operating results and do not have to be considered in terms of accounting, finances or productivity analysis. In other words, they are a physical quantity, which should *ceteris paribus* be increased in order to increase the result. In turn, the term "technological efficiency" means the effectiveness of transforming expenditures into results. The technology of an object will therefore be its vector of empirical expenditures and results.

The technological efficiency has been assessed on the basis of the indicator understood as the ratio of the results to the value of expenditures, calculated in accordance with the following formula:

$$E_j = \frac{\sum_{r=1}^{R} u_r y_{rj}}{\sum_{n=1}^{N} v_n x_{nj}},$$

where: E_j – the efficiency indicator of the *j* object,

u_r – valuation of the unit of the *r* result (the unit value of the *r* result where the market prices of the result are known),

v_n – valuation of the unit of the *n* expenditure (the unit value of the *n* expenditure where the market prices of the expenditure are known).

The resulting efficiency indicator:

- is standardised in the range [0;1],
- its upper value represents the higher efficiency,
- determines at least the relative efficiency of an object.

With the expenditure and result sets defined, the efficiency of individual countries in terms of ICT security has been determined. The country efficiency ($\hat{\theta}_o$) has been determined by the optimal expenditure level factor with the use of the CCR model. The model assumes minimisation of expenditures of the o object realised by minimisation of the so-called expenditure level factor $\hat{\theta}_o$. The CCR model data includes the expenditures xnj and results ryj (j=1,…,J; r=1,…,R; n=1,…,N), while the decision-making variables includes the weights of intensity in the shared technology oriented to the o object λo1, λo2,…, λoJ and the expenditure factor θo.

The target function takes the form: θo→min, and the boundary conditions are as follows:

$$\sum_{j=1}^{J} x_{nj}\lambda_{oj} \le \theta_o x_{no} \qquad n = 1,\ldots,N,$$

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 9 Number 1 (September)
http://doi.org/10.9770/jesi.2021.9.1(8)

$$\sum_{j=1}^{J} y_{rj}\lambda_{oj} \geq y_{ro} \qquad r = 1,...,R,$$

$$\theta_o \leq 1,$$

$$\theta_o, \lambda_{o1}, \lambda_{o2}, ..., \lambda_{oJ} \geq 0.$$

Therefore, the CCR model involves finding such non-negative numbers θ_o and λ_{oJ} so that:

- the expenditures of the shared technology represent the lowest possible portion of the actual expenditures of the *o* object,
- the results of the shared technology are at least the same as the ones actually achieved by the *o* object,
- the shared technology is acceptable.

4. Results

The results for the assumed variables are presented in Table 1. Due to the interpretation possibilities, only the optimal values of the expenditure level factor are given.

Table 1. Results of the expenditure-oriented CCR for small, medium and large enterprises

EU countries	Efficiency ($\hat{\theta}_o$)		
	Small enterprises	Medium enterprises	Large enterprises
Belgium	0,8948	0,909	0,9289
Bulgaria	1	1	1
Czechia	0,8853	0,8998	0,9298
Denmark	0,8791	0,9239	0,9524
Germany	0,8857	0,9508	0,9539
Estonia	1	1	1
Ireland	0,8904	0,9189	0,9297
Greece	1	1	1
Spain	0,911	0,9413	0,9594
France	0,9241	0,9091	0,9085
Croatia	1	1	1
Italy	0,9564	0,99	0,9815
Cyprus	1	0,9291	0,9707
Latvia	0,8421	0,9092	0,9193
Lithuania	0,9551	0,9775	0,9708
Luxembourg	0,9372	0,9364	0,9336
Hungary	1	1	0,971
Malta	0,875	0,9075	1
Netherlands	0,8971	0,9414	0,9396

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 9 Number 1 (September)
http://doi.org/10.9770/jesi.2021.9.1(8)

Austria	0,9629	0,9481	0,985
Poland	0,9914	0,9453	0,9563
Portugal	0,9247	-	0,9923
Romania	1	1	1
Slovenia	1	1	1
Slovakia	0,9156	0,9373	0,9585
Finland	0,8876	0,9091	0,9001
Sweden	0,9042	0,9184	0,9011
United Kingdom	1	0,9737	0,9898

Source: own calculations.

The value of the optimal factor $\hat{\theta}_o$ lower than one means that the optimal expenditures of the shared technology necessary to achieve results at the level corresponding to those achieved by the object examined are not greater than the expenditures actually incurred by that object. Therefore, one can say that the object examined has achieved given results with the use of more expenditures than required, and thus it is not fully efficient.

The object's non-efficiency level can be defined as $1-\hat{\theta}_o$. Where the optimal factor $\hat{\theta}_o$ equals one, the optimal expenditures necessary to achieve the effects which occurred in the object concerned are the same as the actual expenditures of that object, which means that the object is fully efficient. One can therefore say that the optimal expenditures are the expenditures of a fully efficient object.

On analysing efficiency indicators small, medium and large enterprises, one can say that most EU countries are non-fully efficient in the area of ICT security. The lowest value of the efficiency indicator is observed for small enterprises, where it ranges from 0.8421 to 0.9914, and therefore is close to one. However, it is the expenditures and results in small enterprises where the largest amount of fully efficient states can be observed. For all types of enterprises, fully efficient countries include Bulgaria, Estonia, Greece, Croatia, Romania and Slovenia. One can therefore assume that enterprises in those countries achieve their results in the area of ICT security through the optimal use of expenditures. Tables 2 – 4 show optimal technologies minimising expenditures in small, medium and large enterprises in non-efficient countries.

\

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 9 Number 1 (September)
http://doi.org/10.9770/jesi.2021.9.1(8)

Table 2. Optimal technology (the optimal value as percentage of the empirical value) for small enterprises in non-efficient countries

Non-fully efficient countries		Belgium	Czechia	Denmark	Germany	Ireland	Spain	France	Italy	Latvia	Lithuania	Luxembourg	Malta	Netherlands	Austria	Poland	Portugal	Slovakia	Finland	Sweden
Variable		%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%
Inputs	IN_measure	89,5	88,5	87,9	88,6	89	91,1	92,4	95,6	84,2	95,5	93,7	87,5	89,7	96,3	99,1	92,5	91,6	88,8	90,4
	IN_insurance	71,1	88,5	8,7	64,1	12,9	34,2	24,3	77,3	84,2	95,5	52,3	21,4	61,4	31,9	99,1	92,5	91,6	15,9	9,8
	IN_policy	76,6	88,5	39,2	88,6	41,3	84,7	90,1	64,1	84,2	71,1	67	75,9	45,3	58,5	98,7	86,9	91,6	45,2	53,9
	IN_obligations	89,5	64,3	77,5	80	66,6	91,1	92,4	72	75,9	78,6	93,7	87,5	89,7	85,4	99,1	92,5	81,5	81,9	79,4
	IN_suppliers	89,1	88,5	87,9	88,6	89	91,1	92,4	95,6	80,3	95,5	93,7	87,5	89,7	96,3	89,9	82,5	91,6	88,8	90,4
Outputs	OUT_ unavailability	114,6	105,9	101	100	110,5	100,5	102,7	100	100,3	100	104,1	109,9	103	100	100	100	102,5	104,6	130,6
	OUT_destruction	100	101,4	100	100	100	100	100	100	100	102,4	100	100	100	100	101,8	100	100	100	100
	OUT_disclosure	100	100	100,2	100	100	100	100	100	100	101,3	100	100	100,1	100	101	103,5	100	100,7	100

Source: own calculations.

Table 3. Optimal technology (the optimal value as percentage of the empirical value) for medium enterprises in non-efficient countries

Non-fully efficient countries		Belgium	Czechia	Denmark	Germany	Ireland	Spain	France	Italy	Cyprus	Latvia	Lithuania	Luxembourg	Malta	Netherlands	Austria	Poland	Slovakia	Finland	Sweden	United Kingdom
Variable		%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%
Inputs	IN_measure	90,9	90	92	93	91,9	94,1	90,9	92,9	92,9	90,9	97,7	92,8	89	93,6	92,8	94,5	93,7	90,9	91,8	93,9
	IN_insurance	33	63,6	50	62	17,5	24,2	17,6	65,5	82,3	69,9	97,7	26,8	24,9	94,1	63,5	92	82,7	29	21,2	39,3
	IN_policy	40,5	46,9	39,9	46,1	30,8	52,3	58,1	44,8	53,1	60,6	84,1	53,7	49,9	50,6	47,3	66,4	56,8	32,7	29,7	37,5
	IN_obligations	84,5	70,4	70,2	74,4	73,5	92,1	85,3	76,4	85	80,8	84,5	93,6	78,5	81,8	76,6	92,3	81,8	74,4	74,5	72,3
	IN_suppliers	90,7	89,8	92,4	95,1	91,7	93,1	90,7	99	91,1	88,9	97,3	93,6	90,8	94,1	94,8	93,6	92,6	90,7	90,7	97,4
Outputs	OUT_ unavailability	110,7	113,7	100	100	106,1	100	101,2	100	100	101	100	106,2	104,3	100	100	100	101	104,9	150,2	100
	OUT_destruction	100,1	104,6	100	102,2	100	103,7	100	100	103,4	104,4	100,6	100	100,2	100,8	100	107,6	103,2	100	101,2	100
	OUT_disclosure	100	100	100,7	100	102,1	100	102,1	101,5	100	100	100	102,1	100	100,3	100,4	100	100	105,4	100	102,8

Source: own calculations

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 9 Number 1 (September)
http://doi.org/10.9770/jesi.2021.9.1(8)

Table 4. Optimal technology (the optimal value as percentage of the empirical value) for large enterprises in non-efficient countries

Non-fully efficient countries		Belgium	Czechia	Denmark	Germany	Ireland	Spain	France	Italy	Cyprus	Latvia	Lithuania	Luxembourg	Hungary	Malta	Netherlands	Austria	Poland	Portugal	Slovakia	Finland	Sweden	United Kingdom
Variable		%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%
Inputs	IN_measure	92,9	93	95,2	94,8	93	95,4	90,8	96,4	97,1	91,9	97,1	93,4	96	97,9	94	98,5	95,6	99,2	95,9	90	90,1	98
	IN_insurance	91,2	93	95,2	95,4	57,8	38,9	65,7	98,1	97,1	91,9	97,1	93,4	97,1	77,6	94	98,5	95,6	99,2	95,9	90	88,5	58,3
	IN_policy	51,5	62,1	48,8	64,5	43,6	65,3	63,6	67	61	66,8	96,5	80,8	97,1	48,1	58,6	73,1	75	82	70,4	50	42,3	47,1
	IN_obligations	75,8	80,9	75,2	79,4	71,9	87	74,9	82,5	84,7	83,7	92,3	82,8	96,7	75,8	83,4	85,7	88,2	95,4	86,7	72,2	70,4	77,4
	IN_suppliers	92,9	92	95,2	95,4	92,9	95,9	89,9	98,1	96	90,2	97,1	93,3	97,1	100	93,8	97,1	94	97,7	94	89,8	90,1	99
Outputs	OUT_ unavailability	127,3	116,9	109,4	101,9	121,7	103	113,2	110,4	100,9	108,8	100	115,3	111,9	137,3	102	104,8	100,1	103,3	108,9	117,5	227,4	103,2
	OUT_destruction	100	104,5	100	100	100	100	100	100	102,6	100,2	100,5	100	100	100	100	100	108,3	100	104,4	100	103,9	100
	OUT_disclosure	102	100	111,4	100	105,4	100	100,8	100,2	100	100	100	104,3	102,3	103,1	102,2	102,5	100	102,7	100	110,7	100	106,4

Source: own calculations

Countries which participate in an optimal shared technology oriented to non-fully efficient countries can together achieve their results at lower expenditures, while:

- In optimal technologies of all non-fully efficient countries, the physical quantity of results of small, medium and large enterprises is slightly higher than the actual quantity. In the said optimal technologies, most results are at the same level as the one observed, and this applies particularly to the enterprises which were not affected by disclosure of confidential data. Deployment of an optimal shared technology in non-fully efficient countries would in turn cause the highest increase in the share of enterprises which did not report any problems with availability of ICT services compared to the actual value of that share.
- Among non-fully efficient countries, the calculated optimal expenditures related to having insurance against ICT security incidents and defining or reviewing the security policy within the last 12 months account for less than 50% of the empirical expenditures in a number of countries. This is true mainly for small and medium enterprises in such countries as Denmark, Ireland, Spain, France, Malta, the Netherlands, Austria, Finland, Sweden (for small enterprises) and Belgium, the Czech Republic, Denmark, Germany, Ireland, Spain, France, Italy, Luxembourg, Malta, the Netherlands, Austria, Finland, Sweden, the United Kingdom (for medium enterprises).

Based on the optimal technology, the authors evaluated surpluses and deficits of results with respect to the optimal amounts in non-efficient states, and the findings are presented in Tables 5 – 7. Slacks mean the difference between the optimal expenditures and $\hat{\theta}_o$-proportional expenditures. The expenditure slacks for the acceptable and optimal technologies result of Pareto non-optimality. In turn, the surplus of empirical expenditures is the difference between the empirical expenditures and $\hat{\theta}_o$-proportional expenditures.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 9 Number 1 (September)
http://doi.org/10.9770/jesi.2021.9.1(8)

Table 5. Slacks and surpluses in expenditures of small enterprises in non-efficient countries.

Non-fully efficient countries	Slacks	Actual IN_measure	Actual IN_insurance	Actual IN_policy	Actual IN_obligation	Actual IN_supplier
Belgium	Expenditure slack	0,0064	4,4152	2,8456	0,0044	0,3868
	Surplus	9,79	6,94	5,16	5,58	9,96
	Surplus as percentage of optimal expenditures	0,117654	0,4068	0,306413	0,117672	0,122902
	Surplus as percentage of empirical expenditures	0,105269	0,289167	0,234545	0,105283	0,109451
Czechia	Expenditure slack	0,0035	-0,0029	-0,0034	17,9022	0,0064
	Surplus	10,9	0,8	2,52	26,39	10,1
	Surplus as percentage of optimal expenditures	0,129608	0,129032	0,129363	0,554295	0,129653
	Surplus as percentage of empirical expenditures	0,114737	0,114286	0,114545	0,356622	0,114773
Denmark	Expenditure slack	-0,0073	45,1687	18,5158	6,9897	-0,0028
	Surplus	11,72	52,06	23,11	15,09	11,12
	Surplus as percentage of optimal expenditures	0,13743	10,53846	1,552048	0,290695	0,137488
	Surplus as percentage of empirical expenditures	0,120825	0,913333	0,608158	0,225224	0,12087
Germany	Expenditure slack	-0,0014	4,6483	0,0011	5,5048	-0,0027
	Surplus	11,2	6,82	2,63	12,82	10,17
	Surplus as percentage of optimal expenditures	0,129032	0,559934	0,129111	0,250488	0,129012
	Surplus as percentage of empirical expenditures	0,114286	0,358947	0,114348	0,200313	0,11427
Ireland	Expenditure slack	-0,002	28,1748	18,6156	17,3108	-0,004
	Surplus	10,41	32,23	22,89	25,75	9,86
	Surplus as percentage of optimal expenditures	0,123064	6,756813	1,420857	0,502439	0,123035
	Surplus as percentage of empirical expenditures	0,109579	0,871081	0,586923	0,334416	0,109556
Spain	Expenditure slack	0,002	17,07	1,422	0,001	-0,003
	Surplus	8,19	19,74	3,38	4,54	7,74
	Surplus as percentage of optimal expenditures	0,097721	1,923977	0,181525	0,097718	0,097653
	Surplus as percentage of empirical expenditures	0,089022	0,658	0,153636	0,08902	0,088966
France	Expenditure slack	0,0013	25,1817	0,3515	0,005	0,0044
	Surplus	7,06	27,99	1,49	3,8	6,38
	Surplus as percentage of optimal expenditures	0,08215	3,106548	0,110289	0,082251	0,082195
	Surplus as percentage of empirical expenditures	0,075914	0,756486	0,099333	0,076	0,075952
Italy	Expenditure slack	-0,0048	2,1968	8,2064	17,2672	-0,0052
	Surplus	4,05	2,72	9,34	20,45	3,57
	Surplus as percentage of optimal expenditures	0,045531	0,293103	0,560624	0,389153	0,045518
	Surplus as percentage of empirical expenditures	0,043548	0,226667	0,359231	0,280137	0,043537
Latvia	Expenditure slack	0,0079	0,0052	0,0004	5,4886	3,89
	Surplus	15,64	1,9	3,79	15,91	19,68
	Surplus as percentage of optimal expenditures	0,18762	0,188119	0,187531	0,317628	0,24502
	Surplus as percentage of empirical expenditures	0,15798	0,158333	0,157917	0,241061	0,1968
Lithuania	Expenditure slack	-0,0008	-0,0047	4,882	10,6313	0,0033
	Surplus	4,13	0,13	5,78	13,46	3,73
	Surplus as percentage of optimal expenditures	0,047001	0,045296	0,40647	0,2717	0,047054

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 9 Number 1 (September)
http://doi.org/10.9770/jesi.2021.9.1(8)

	Surplus as percentage of empirical expenditures	0,044891	0,043333	0,289	0,213651	0,04494
Luxembourg	Expenditure slack	0,0024	9,9428	4,8096	-0,0016	0,0076
	Surplus	5,78	11,45	5,94	2,95	5,22
	Surplus as percentage of optimal expenditures	0,067038	0,912351	0,492537	0,066969	0,067112
	Surplus as percentage of empirical expenditures	0,062826	0,477083	0,33	0,062766	0,062892
Malta	Expenditure slack	-0,005	17,845	2,54	-0,005	0
	Surplus	11,62	21,22	5,29	6,87	11
	Surplus as percentage of optimal expenditures	0,142787	3,67128	0,316577	0,142738	0,142857
	Surplus as percentage of empirical expenditures	0,124946	0,785926	0,240455	0,124909	0,125
Netherlands	Expenditure slack	-0,0055	7,0675	11,9917	-0,005	-0,001
	Surplus	9,77	9,64	14,77	5,14	9,26
	Surplus as percentage of optimal expenditures	0,114631	0,627604	1,207686	0,114579	0,114689
	Surplus as percentage of empirical expenditures	0,102842	0,3856	0,547037	0,1028	0,102889
Austria	Expenditure slack	0,001	10,9493	9,4625	6,4011	0,0049
	Surplus	3,34	11,58	10,39	8,59	3,01
	Surplus as percentage of optimal expenditures	0,038541	2,136531	0,711157	0,170403	0,038595
	Surplus as percentage of empirical expenditures	0,037111	0,681176	0,4156	0,145593	0,03716
Poland	Expenditure slack	0,0032	0,004	0,071	0,0044	8,0518
	Surplus	0,76	0,09	0,2	0,4	8,8
	Surplus as percentage of optimal expenditures	0,008712	0,009082	0,013514	0,008772	0,112532
	Surplus as percentage of optimal expenditures	0,008636	0,009	0,013333	0,008696	0,101149
Portugal	Expenditure slack	0,0006	0,0023	0,9946	-0,0003	9,9053
	Surplus	7,38	0,68	2,35	3,84	17,36
	Surplus as percentage of optimal expenditures	0,081439	0,081731	0,15016	0,081425	0,212641
	Surplus as percentage of empirical expenditures	0,075306	0,075556	0,130556	0,075294	0,175354
Slovakia	Expenditure slack	0,0052	-0,0008	-0,0036	6,2372	0,0028
	Surplus	7,77	0,59	1,6	11,47	7,43
	Surplus as percentage of optimal expenditures	0,092247	0,092044	0,091954	0,226994	0,092218
	Surplus as percentage of empirical expenditures	0,084457	0,084286	0,084211	0,185	0,084432
Finland	Expenditure slack	0,0072	19,6652	13,068	4,1736	-0,0012
	Surplus	10,91	22,7	16,44	11,03	9,89
	Surplus as percentage of optimal expenditures	0,126728	5,27907	1,212389	0,220732	0,126616
	Surplus as percentage of empirical expenditures	0,112474	0,840741	0,548	0,18082	0,112386
Sweden	Expenditure slack	-0,0052	30,6496	12,787	6,7262	-0,003
	Surplus	9	34,29	16,14	12,57	8,14
	Surplus as percentage of optimal expenditures	0,105882	9,242588	0,855779	0,25955	0,105907
	Surplus as percentage of empirical expenditures	0,095745	0,902368	0,461143	0,206066	0,095765

Source: own calculations

.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 9 Number 1 (September)
http://doi.org/10.9770/jesi.2021.9.1(8)

Among small enterprises in countries which are not fully efficient in terms of ICT security, one can observe fairly large differences in the surpluses of individual expenditures understood as the difference between the empirical and optimal expenditures. The surplus peaks for expenditures related to insurance against ICT security incidents. In the case of such countries as Denmark, Ireland, France, Malta, Finland and Sweden they should be reduced by more than 70%.

Table 6. Slacks and surpluses in expenditures of medium enterprises in non-efficient countries.

Non-fully efficient countries	Slacks	Actual IN_measure	Actual IN_insurance	Actual IN_policy	Actual IN_obligation	Actual IN_supplier
Belgium	Expenditure slack	0,002	15,633	22,176	4,825	0,164
	Surplus	8,92	18,09	26,18	11,65	8,9
	Surplus as percentage of optimal expenditures	10,01%	203,03%	146,91%	18,39%	10,22%
	Surplus as percentage of empirical expenditures	9,10%	67,00%	59,50%	15,53%	9,27%
Czechia	Expenditure slack	0,0002	3,6872	16,3724	17,632	0,1806
	Surplus	9,92	5,09	20,18	26,65	9,9
	Surplus as percentage of optimal expenditures	11,14%	57,13%	113,24%	42,07%	11,37%
	Surplus as percentage of empirical expenditures	10,02%	36,36%	53,11%	29,61%	10,21%
Denmark	Expenditure slack	0,4261	21,175	29,8923	19,0854	-0,0017
	Surplus	7,96	24,98	34,23	25,63	7,38
	Surplus as percentage of optimal expenditures	8,74%	99,84%	150,33%	42,45%	8,23%
	Surplus as percentage of empirical expenditures	8,04%	49,96%	60,05%	29,80%	7,61%
Germany	Expenditure slack	2,0692	9,2724	22,036	17,588	0,006
	Surplus	6,94	10,65	24,25	21,77	4,68
	Surplus as percentage of optimal expenditures	7,54%	61,38%	116,87%	34,43%	5,18%
	Surplus as percentage of empirical expenditures	7,01%	38,04%	53,89%	25,61%	4,93%
Ireland	Expenditure slack	0,0011	38,6828	36,0251	16,1732	0,1833
	Surplus	8,03	42,9	40,81	23,31	8,05
	Surplus as percentage of optimal expenditures	8,83%	471,43%	224,35%	36,03%	9,05%
	Surplus as percentage of empirical expenditures	8,11%	82,50%	69,17%	26,49%	8,30%
Spain	Expenditure slack	0,0048	33,5424	15,0668	1,3997	0,9735
	Surplus	5,64	36,36	17,18	5,45	6,55
	Surplus as percentage of optimal expenditures	6,24%	312,37%	91,29%	8,58%	7,41%
	Surplus as percentage of empirical expenditures	5,88%	75,75%	47,72%	7,90%	6,89%
France	Expenditure slack	0,0009	37,3641	10,1821	4,1825	0,1827
	Surplus	9	42	13	11	9
	Surplus as percentage of optimal expenditures	10,00%	466,67%	72,22%	17,19%	10,23%
	Surplus as percentage of empirical expenditures	9,09%	82,35%	41,94%	14,67%	9,28%
Italy	Expenditure slack	6,05	7,03	23,86	19,02	0
	Surplus	7,04	7,24	24,3	19,86	0,91
	Surplus as percentage of optimal expenditures	7,66%	52,62%	123,35%	30,96%	1,01%

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 9 Number 1 (September)
http://doi.org/10.9770/jesi.2021.9.1(8)

	Surplus as percentage of empirical expenditures	7,11%	34,48%	55,23%	23,64%	1,00%
Cyprus	Expenditure slack	0,0027	2,112	15,1458	5,7843	1,7127
	Surplus	6,88	3,53	17,84	10,96	8,59
	Surplus as percentage of optimal expenditures	7,63%	21,43%	88,49%	17,67%	9,72%
	Surplus as percentage of empirical expenditures	7,09%	17,65%	46,95%	15,01%	8,86%
Latvia	Expenditure slack	0	2,7296	9,096	8,086	2,02
	Surplus	9,08	3,91	11,82	15,35	11,1
	Surplus as percentage of optimal expenditures	9,99%	43,01%	65,02%	23,74%	12,49%
	Surplus as percentage of empirical expenditures	9,08%	30,08%	39,40%	19,19%	11,10%
Lithuania	Expenditure slack	0,0075	0,005	3,9475	10,4625	0,375
	Surplus	2,19	0,14	4,6	12,24	2,49
	Surplus as percentage of optimal expenditures	2,31%	2,39%	18,85%	18,33%	2,72%
	Surplus as percentage of empirical expenditures	2,26%	2,33%	15,86%	15,49%	2,65%
Luxembourg	Expenditure slack	0,7972	23,394	13,5676	0,0016	-0,002
	Surplus	7,03	25,62	15,73	4,39	6,04
	Surplus as percentage of optimal expenditures	7,73%	273,13%	86,10%	6,79%	6,79%
	Surplus as percentage of empirical expenditures	7,17%	73,20%	46,26%	6,36%	6,36%
Malta	Expenditure slack	1,695	23,0425	14,3125	9,6525	-0,005
	Surplus	10,76	26,28	17,55	16,96	8,69
	Surplus as percentage of optimal expenditures	12,33%	301,38%	100,57%	27,34%	10,19%
	Surplus as percentage of empirical expenditures	10,98%	75,09%	50,14%	21,47%	9,24%
Netherlands	Expenditure slack	0,4972	-0,0008	20,0244	9,1236	0,0044
	Surplus	6,24	1,64	22,72	13,46	5,63
	Surplus as percentage of optimal expenditures	6,80%	6,22%	97,59%	22,23%	6,23%
	Surplus as percentage of empirical expenditures	6,37%	5,86%	49,39%	18,19%	5,86%
Austria	Expenditure slack	1,9238	6,5801	19,4621	15,1523	-0,0086
	Surplus	7,01	7,67	21,59	19,46	4,87
	Surplus as percentage of optimal expenditures	0,077041	0,575394	1,112313	0,306264	0,054639
	Surplus as percentage of empirical expenditures	0,071531	0,365238	0,526585	0,234458	0,051809
Poland	Expenditure slack	0,0041	0,4148	8,429	1,5457	0,8788
	Surplus	5,31	1,29	10,07	5,32	6,13
	Surplus as percentage of optimal expenditures	0,057913	0,087695	0,505268	0,083543	0,06821
	Surplus as percentage of empirical expenditures	0,054742	0,080625	0,335667	0,077101	0,063854
Slovakia	Expenditure slack	-0,0019	1,2203	11,8136	9,3967	1,0808
	Surplus	6,08	1,91	13,82	14,35	7,1
	Surplus as percentage of optimal expenditures	0,066872	0,210121	0,760176	0,221964	0,079865
	Surplus as percentage of empirical expenditures	0,06268	0,173636	0,431875	0,181646	0,073958
Finland	Expenditure slack	0,0009	19,1821	32,0005	14,1826	0,1827
	Surplus	9	22	37	22	9
	Surplus as percentage of optimal	0,1	2,444444	2,055556	0,34375	0,102273

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 9 Number 1 (September)
http://doi.org/10.9770/jesi.2021.9.1(8)

	expenditures					
	Surplus as percentage of empirical expenditures	0,090909	0,709677	0,672727	0,255814	0,092784
Sweden	Expenditure slack	0,0048	29,6628	37,284	14,714	1,0664
	Surplus	7,92	33,09	42,18	21,65	8,9
	Surplus as percentage of optimal expenditures	0,088909	3,713805	2,367003	0,341752	0,102181
	Surplus as percentage of empirical expenditures	0,081649	0,787857	0,703	0,254706	0,092708
United Kingdom	Expenditure slack	3,42	38,9279	37,7031	21,5682	0,0015
	Surplus	6,05	40,69	39,36	23,83	2,5
	Surplus as percentage of optimal expenditures	0,064396	1,54656	1,664975	0,383304	0,027027
	Surplus as percentage of empirical expenditures	0,0605	0,607313	0,624762	0,277093	0,026316

Source: own calculations.

Fairly large differences in the surpluses of individual expenditures can also be observed among medium enterprises in countries which are not fully efficient in terms of ICT security. It peaks for expenditures related to having insurance against ICT security incidents and ICT security policy. In such countries as Ireland, France, Spain, Luxembourg, Malta, Finland and Sweden the reduction should be relatively larger than in the case of other expenditures.

Table 7. Slacks and surpluses in expenditures of large enterprises in non-efficient countries.

Non-fully efficient countries	Slacks	Actual IN_measure	Actual IN_insurance	Actual IN_policy	Actual IN_obligation	Actual IN_supplier
Belgium	Expenditure slack	0,0011	0,6938	27,7563	15,5599	0,0322
	Surplus	7,04	3,68	32,52	22,03	7
	Surplus as percentage of optimal expenditures	0,076555	0,096033	0,943155	0,319414	0,076923
	Surplus as percentage of empirical expenditures	0,071111	0,087619	0,485373	0,242088	0,071429
Czechia	Expenditure slack	0	-0,0034	18,2282	11,5908	0,9202
	Surplus	7,02	1,19	22,37	18,33	7,87
	Surplus as percentage of optimal expenditures	0,0755	0,075269	0,610702	0,235998	0,08636
	Surplus as percentage of empirical expenditures	0,0702	0,07	0,379153	0,190938	0,079495
Denmark	Expenditure slack	0	-0,004	34,85	19,2604	0,0776
	Surplus	4,76	1,9	38,42	23,83	4,79
	Surplus as percentage of optimal expenditures	0,049979	0,049869	1,050301	0,330193	0,050844
	Surplus as percentage of empirical expenditures	0,0476	0,0475	0,512267	0,248229	0,048384
Germany	Expenditure slack	0,63	0,0048	18,2001	15,0266	0,0022
	Surplus	5,24	1,48	20,92	19,36	4,52
	Surplus as percentage of optimal expenditures	0,055298	0,048493	0,54937	0,259378	0,048353
	Surplus as percentage of empirical expenditures	0,0524	0,04625	0,354576	0,205957	0,046122
Ireland	Expenditure slack	0	23,5499	39,516	20,4509	0,0403
	Surplus	7,03	28,26	45,14	27,27	7
	Surplus as percentage of optimal expenditures	0,075616	0,729479	1,294894	0,39108	0,076087

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 9 Number 1 (September)
http://doi.org/10.9770/jesi.2021.9.1(8)

	Surplus as percentage of empirical expenditures	0,0703	0,421791	0,56425	0,281134	0,070707
Spain	Expenditure slack	0,5212	41,0568	16,867	7,639	0,0024
	Surplus	4,5	43,98	19,1	11,09	3,9
	Surplus as percentage of optimal expenditures	0,048128	1,569593	0,532033	0,150047	0,042345
	Surplus as percentage of empirical expenditures	0,045918	0,610833	0,347273	0,130471	0,040625
France	Expenditure slack	0,0015	14,3145	14,4205	14,315	0,9415
	Surplus	9,06	19,53	19,27	22,55	10
	Surplus as percentage of optimal expenditures	0,100734	0,521217	0,571302	0,334322	0,11236
	Surplus as percentage of empirical expenditures	0,091515	0,342632	0,363585	0,250556	0,10101
Italy	Expenditure slack	1,7185	-0,0035	18,9715	14,368	0,004
	Surplus	3,55	0,57	20,1	16,07	1,78
	Surplus as percentage of optimal expenditures	0,037192	0,018732	0,491443	0,211642	0,018892
	Surplus as percentage of empirical expenditures	0,035859	0,018387	0,329508	0,174674	0,018542
Cyprus	Expenditure slack	0	-0,0027	21,642	10,7509	1,11
	Surplus	2,93	1,14	23,4	13,3	4,04
	Surplus as percentage of optimal expenditures	0,030184	0,030111	0,639344	0,180461	0,042101
	Surplus as percentage of empirical expenditures	0,0293	0,029231	0,39	0,152874	0,0404
Latvia	Expenditure slack	0	-0,0033	13,5622	7,4963	1,76
	Surplus	8,07	1,53	17,92	14,84	9,83
	Surplus as percentage of optimal expenditures	0,087784	0,087579	0,496674	0,194853	0,109016
	Surplus as percentage of empirical expenditures	0,0807	0,080526	0,331852	0,163077	0,0983
Lithuania	Expenditure slack	0,02	-0,002	0,29	4,4644	-0,0016
	Surplus	2,94	0,29	1,75	7,18	2,86
	Surplus as percentage of optimal expenditures	0,030291	0,029866	0,036269	0,083663	0,030061
	Surplus as percentage of empirical expenditures	0,0294	0,029	0,035	0,077204	0,029184
Luxembourg	Expenditure slack	0	0,0004	5,642	9,1096	0,0964
	Surplus	6,64	2,59	8,63	14,82	6,67
	Surplus as percentage of optimal expenditures	0,071123	0,071134	0,237283	0,208205	0,072241
	Surplus as percentage of empirical expenditures	0,0664	0,06641	0,191778	0,172326	0,067374
Hungary	Expenditure slack	1,099	0,002	-0,002	0,336	-0,004
	Surplus	3,97	0,35	1,39	2,83	2,78
	Surplus as percentage of optimal expenditures	0,041776	0,030043	0,029822	0,034027	0,029822
	Surplus as percentage of empirical expenditures	0,040101	0,029167	0,028958	0,032907	0,028958
Netherlands	Expenditure slack	0	0,006	23,3636	9,3148	0,2004
	Surplus	6,04	2,12	27,35	14,63	6,18
	Surplus as percentage of optimal expenditures	0,064283	0,064477	0,707633	0,1994	0,06658
	Surplus as percentage of empirical expenditures	0,0604	0,060571	0,414394	0,16625	0,062424

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 9 Number 1 (September)
http://doi.org/10.9770/jesi.2021.9.1(8)

Austria	Expenditure slack	0,005	0,005	15,77	12,03	1,425
	Surplus	1,49	0,38	16,7	13,44	2,91
	Surplus as percentage of optimal expenditures	0,01528	0,015435	0,368653	0,166832	0,030284
	Surplus as percentage of empirical expenditures	0,015051	0,0152	0,269355	0,142979	0,029394
Poland	Expenditure slack	-0,0063	0,0012	10,0887	6,4781	1,6137
	Surplus	4,32	1,05	12,23	10,28	5,94
	Surplus as percentage of optimal expenditures	0,045627	0,045752	0,332608	0,133994	0,06383
	Surplus as percentage of empirical expenditures	0,043636	0,04375	0,249592	0,118161	0,06
Portugal	Expenditure slack	0	-0,0017	10,1357	3,3824	1,55
	Surplus	0,77	0,16	10,59	4,06	2,32
	Surplus as percentage of optimal expenditures	0,00776	0,007678	0,218756	0,048368	0,023751
	Surplus as percentage of empirical expenditures	0,0077	0,007619	0,179492	0,046136	0,0232
Slovakia	Expenditure slack	0,0015	0,003	13,5005	8,3435	1,8415
	Surplus	4,11	0,75	15,7	12,12	5,95
	Surplus as percentage of optimal expenditures	0,043313	0,043478	0,420912	0,153651	0,063944
	Surplus as percentage of empirical expenditures	0,041515	0,041667	0,296226	0,133187	0,060101
Finland	Expenditure slack	0	0,0034	29,9875	17,4998	0,2099
	Surplus	9,99	3,4	37,48	27,29	10,1
	Surplus as percentage of optimal expenditures	0,110988	0,111111	0,998934	0,385943	0,113611
	Surplus as percentage of empirical expenditures	0,0999	0,1	0,499733	0,278469	0,10202
Sweden	Expenditure slack	-0,0011	0,6762	37,7369	18,6945	0,0278
	Surplus	9,79	4,83	45,55	28,09	9,72
	Surplus as percentage of optimal expenditures	0,109741	0,129944	1,361734	0,419818	0,110104
	Surplus as percentage of empirical expenditures	0,098889	0,115	0,576582	0,295684	0,099184
United Kingdom	Expenditure slack	0,96	28,446	40,4444	20,511	0,0004
	Surplus	1,98	29,16	41,24	21,48	1
	Surplus as percentage of optimal expenditures	0,0202	0,714006	1,121872	0,292165	0,010309
	Surplus as percentage of empirical expenditures	0,0198	0,416571	0,528718	0,226105	0,010204

Source: own calculations.

Among large enterprises in countries which are not fully efficient in terms of ICT security, one can observe much smaller differences in the surpluses of individual expenditures than in the case of small and medium enterprises. The surplus peaks for expenditures related to having an ICT security policy and actions taken to make persons employed aware of their obligations in ICT security related issues.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 9 Number 1 (September)
http://doi.org/10.9770/jesi.2021.9.1(8)

Conclusions

Key findings

All sorts of enterprises - including small, medium and large ones - need to be resilient and manage the risks that the challenging market conditions and the associated risks pose. In the era of information society and digital economy the organizations have internal response how they approach and manage the risks. Information and communication technologies (ICTs) call for sound security measures that requires resources.

The authors positively verified, by means of empirical studies, the hypotheses regarding the possibility of identification of a system of measures for the assessment of ICT security in enterprises and the assessment of the ICT security level in enterprises in spatial terms with the use of appropriate tools that allow identifying countries where the level of ICT security in enterprises requires improvement and that provide for identifying the threshold objects in the test group. To assess ICT security in small, medium and large enterprises in geographical terms, the authors used DEA models which allowed assessing the enterprise security system in a number of terms, in particular with multiple expenditures and results based on the technical efficiency. The technical efficiency has been determined through the relation between the productivity of the object concerned and the productivity of the object considered as fully efficient. The efficiency thus determined showed the actual relation between the benefits and expenditures with reference to the maximum level that can be reached in specific technological conditions. The studies allowed the author to identify both DEA expenditures and achieved results. The expenditures and results have been referenced to the share of enterprises, which did not report any security incidents, and to the share of enterprises, which deployed specific methods to prevent such incidents. The share of enterprises which did not report any ICT risks has been considered as the result of deployment of information security systems in enterprises because - although an increasing number of more and more sophisticated safeguards are being applied - organisations still experience information security related incidents.

The research allowed identifying countries where ICT security results were achieved with the optimum combination of expenditures, i.e. the so-called fully efficient countries. Countries which are fully efficient in terms of ICT security in enterprises are in the Central and Eastern Europe, and therefore are less economically developed than other EU member states. This fact should not come as a surprise since enterprises active in economically developed countries more often apply much more advanced technologies than less developed countries, which makes them more vulnerable to cyberattacks (Li & Wu, 2020; Hughes et al, 2017; Jorgenson & Vu, 2016). Consequently, these enterprises are exposed to more security incidents, which translates into the need to incur much greater expenditures on information security.

The studies are also very important from the perspective of technical efficiency of ICT security actions. Identification of the possibilities of more effective planning of expenditures to achieve a specific level of ICT security can contribute to the improvement of their information risk management systems deployed.

Furthermore, the findings of the studies can be used for identifying the best practices in determining expenditures and results in the area of ICT security. Indeed, it is highlighted that DEA is the best tool for identifying the best practices or success, as it allows finding the best combination of resources held within a given technology.

The efficiency of ICT security measures undertaken by enterprises is key concern for the management of entities. Digital technologies are spreading and enterprises need to be continually watched out for ICT security matters. ICT technologies open up numerous new opportunities for enterprises. However, management should focus on designing and maintaining effective security procedures to ensure adequate protection for their organization.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 9 Number 1 (September)
http://doi.org/10.9770/jesi.2021.9.1(8)

Limitations and future research

The theoretical deliberations and analyses regarding the ICT security level in the context of technical efficiency presented in this paper cannot be considered as exhaustive and closed. The multitude and variety of information security problems in economic entities, coupled with the lack of clear solutions in this respect, require further research and studies. In the future, it would be advisable to identify barriers and possibilities regarding the development of ICT security systems in small, medium and large enterprises. It would also be appropriate to analyse the level of the results and expenditures in the context of technical efficiency over the last several years. Taken dynamically, it would provide for observing changes in the level of ICT security in enterprises over the years. Future studies should also focus on defining good practices to provide enterprises with adequate safeguards against data security breaches.

References

Abraham, S. and Chengalur-Smith, I. (2019), "Evaluating the effectiveness of learner controlled information security training", *Computers & Security*, Vol. 87 https://doi.org/10.1016/j.cose.2019.101586

Ahmad, A., Maynard, S.B. and Shanks, G. (2015), "A case analysis of information systems and security incident responses", *International Journal of Information Management*, Vol. 35, pp. 717-723 https://doi.org/10.1016/j.ijinfomgt.2015.08.001

Ahmadian, M.M., Shajari, M. and Shafiee, M.A. (2020), "Industrial control system security taxonomic framework with application to a comprehensive incidents survey", *International Journal of Critical Infrastructure Protection*, Vol. 29 https://doi.org/10.1016/j.ijcip.2020.100356

Angraini, Alias, R.A. and Okfalisa (2019), "Information Security Policy Compliance: Systematic Literature Review", Procedia Computer Science, Vol. 161, pp. 1216–1224 https://doi.org/10.1016/j.procs.2019.11.235

Anokhin, S., Wincent, J. and Autio, E. (2011), "Operationalizing opportunities in entrepreneurship research: use of data envelopment analysis", *Small Business Economics*, Vol. 37(1), pp. 39–57 https://doi.org/10.1007/s11187-009-9227-1

Barreto, L., Amaral, A. and Pereira, T. (2017), "Industry 4.0 implications in logistics: an overview", *Procedia Manufacturing*, Vol. 3, pp. 1245-1252 https://doi.org/10.1016/j.promfg.2017.09.045

Bartnes, M., Moe, N.B. and Heegaard, P.E. (2016), "The future of information security incident management training: A case study of electrical power companies", *Computers & Security*, Vol. 61, pp. 32-45 https://doi.org/10.1016/j.cose.2016.05.004

Bossert, O. and Laartz, J. (2018), "Modernizing IT for digital reinvention", *Digital McKinsey: Insights,*, available at: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Modernizing%20IT%20for%20digital%20reinvention/Modernizing-IT-for-digital-reinvention-Collection-July-2018.ashx (accessed 20 August 2020).

Brunner, M., Sauerwein, C., Felderer, M. and Breu, R. (2020), "Risk management practices in information security: Exploring the status quo in the DACH region", Computers & Security, Vol. 92 https://doi.org/10.1016/j.cose.2020.101776

Burdon, M. and Coles-Kemp, L. (2019), "The significance of securing as a critical component of information security: An Australian narrative", *Computers & Security*, Vol. 87 https://doi.org/101601. 10.1016/j.cose.2019.101601

Castells, M. (2010), *The Rise of the Network Society*, Wiley-Blackwell A John Wiley & Sons, Ltd. Publication, https://doi.org/10.1002/9781444319514

Chen, H. (2018), Average lexicographic efficiency for data envelopment analysis, Omega 74, pp. 82–91 https://doi.org/10.1016/j.omega.2017.01.008

Diesch, R., Pfaff, M. and Krcmar, H. (2020), "A comprehensive model of information security factors for decision-makers", *Computers & Security*, Vol. 92, 101747 https://doi.org/10.1016/j.cose.2020.101747

Dudziak-Gajowiak, D., Kolaczek, G. and Juszczyszyn, K. (2019), "Solving problems relating to ICT security management systems including various characteristics of the environment and system", *Scientific Journal of the Military University of Land Forces*, Vol. 1(2/192), pp. 321-334 https://doi.org/10.5604/01.3001.0013.2607

EUR-Lex Glossary. Information society, available at: https://eur-lex.europa.eu/summary/glossary/information_society.html (accessed 20 August 2020).

European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee And the Committee Of the Regions, ICT Standardisation Priorities for the Digital Single Market, Brussels, 19.4.2016, COM(2016) 176 final, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0176 (accessed 20 August 2020).

European Commission: 2020 Rolling plan for ICT standardisation, 2020 Rolling plan for ICT standardisation, available at: https://ec.europa.eu/docsroom/documents/41541 (accessed 20 August 2020).

European Commission: New EU rules on e-commerce, available at: https://ec.europa.eu/digital-single-market/en/new-eu-rules-e-commerce, 2021 (accessed 20 August 2020).

European Commission: Shaping Europe's digital future, Policy, The Directive on security of network and information systems (NIS Directive), 2020, available at: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive (accessed 20 August 2020).

Eurostat Glossary. Information and communication technology (ICT), available at: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Information_and_communication_technology_(ICT) (accessed 20 August 2020).

Eurostat. ICT security in enterprises, available at: https://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_security_in_enterprises#ICT_security_in_EU_enterprises (accessed 20 August 2020).

Evans, M., He, Y., Maglaras, L. and Janicke, H. (2019), "HEART-IS: A novel technique for evaluating human error-related information security incidents", *Computers & Security*, Vol. 80, pp. 74-89 https://doi.org/10.1016/j.cose.2018.09.002

Goodridge, P., Haskel, J. and Edquist, H. (2019), "The economic contribution of the "C" in ICT: Evidence from OECD countries", *Journal of Comparative Economics*, Vol. 47(4), pp. 867-880 https://doi.org/10.1016/j.jce.2019.07.001

Guo, J. and Wang, L. (2020), "Learning to upgrade internet information security and protection strategy in big data era", *Computer Communications*, Vol. 160, pp. 150-157 https://doi.org/10.1016/j.comcom.2020.05.043

Hoffmann, R., Napiórkowski, J., Protasowicki, T. and Stanik, J. (2020), "Measurement Models of Information Security Based on the Principles and Practices for Risk-Based Approach", *Procedia Manufacturing*, Vol. 44, pp. 647-654 https://doi.org/10.1016/j.promfg.2020.02.244

Hughes, B.B., Bohl, D., Irfan, M., Margolese-Malin, E. and Solórzano, J.R. (2017), "ICT/Cyber benefits and costs: Reconciling competing perspectives on the current and future balance", *Technological Forecasting and Social Change*, Vol. 115, pp. 117-130 https://doi.org/10.1016/j.techfore.2016.09.027

Jaeger, L., Eckhardt, A. and Kroenung, J. (2021), "The role of deterrability for the effect of multi-level sanctions on information security policy compliance: Results of a multigroup analysis", *Information & Management*, Vol. 58(3) https://doi.org/10.1016/j.im.2020.103318

Jorgenson, D.W. and Vu, K.M. (2016), "The ICT revolution, world economic growth, and policy issues", *Telecommunications Policy*, Vol. 40(5), pp. 383-397 https://doi.org/10.1016/j.telpol.2016.01.002

Karjalainen, M., Siponen, M. and Sarker, S. (2020), "Toward a stage theory of the development of employees' information security behaviour", *Computers & Security*, Vol. 93 https://doi.org/10.1016/j.cose.2020.101782

Kollmann, T. (2006), "What is e-entrepreneurship? – fundamentals of company founding in the net economy", *International Journal of Technology Management*, Vol. 33(4), pp. 322-340 https://doi.org/10.1504/IJTM.2006.009247

Kollmann, T., Lomberg, C. and Peschl, A. (2016), "Web 1.0, Web 2.0, and Web 3.0: The Development of E-Business", *Encyclopedia of E-Commerce Development, Implementation, and Management*, IGI Global, pp. 1203-1210 https://doi.org/10.4018/978-1-4666-9787-4.ch081

Krohn, W. (2001), "Knowledge Societies", Smelser, N.J. and Baltes, P.B. (ed.s), *International Encyclopedia of the Social & Behavioral Sciences*, Elsevier, Pergamon, pp. 8139-8143, https://doi.org/10.1016/B0-08-043076-7/03190-9

Kwilinski, A. (2018), "Mechanism of formation of industrial enterprise development strategy in the information economy", *Virtual Economics*, Vol. 1(1), pp. 7-25. https://doi.org/10.34021/ve.2018.01.01(1)

Leuprecht, C., Skillicorn, D.B. and Tait, V.E. (2016), "Beyond the Castle Model of cyber-risk and cyber-security", *Government Information Quarterly*, Vol. 33(2), pp. 250-257, https://doi.org/10.1016/j.giq.2016.01.012

Li, Q. and Wu, Y. (2020), "Intangible capital, ICT and sector growth in China", *Telecommunications Policy*, Vol. 44(1), 101854. https://doi.org/10.1016/j.telpol.2019.101854

Line, M.B., Tøndel, I.A. and Jaatun, M.G. (2016), "Current practices and challenges in industrial control organizations regarding information security incident management – Does size matter? Information security incident management in large and small industrial control organizations", *International Journal of Critical Infrastructure Protection*, Vol. 12, pp. 12-26, https://doi.org/10.1016/j.ijcip.2015.12.003

Liu, C., Wang, N. and Liang, H. (2020), "Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment", *International Journal of Information Management*, Vol. 54, https://doi.org/10.1016/j.ijinfomgt.2020.102152

Naicker, V. and Mafaiti, M. (2019), "The establishment of collaboration in managing information security through multisourcing", *Computers & Security*, Vol. 80, pp. 224-237, https://doi.org/10.1016/j.cose.2018.10.005

OSCE Cyber/ICT security, https://www.osce.org/secretariat/cyber-ict-security (accessed 20 August 2020).

OSCE Participating States, available at: https://www.osce.org/participating-states (accessed 20 August 2020).

OSCE Transnational Threats Department Cyber/ICT Security, available at: https://www.osce.org/files/f/documents/c/c/256071.pdf (accessed 20 August 2020).

Paananen, H., Lapke, M. and Siponen, M. (2020), "State of the art in information security policy development", *Computers & Security*, Vol. 88, https://doi.org/10.1016/j.cose.2019.101608

Pereira, T., Barreto, L. and Amaral, A. (2017), "Network and information security challenges within Industry 4.0 paradigm", *Procedia Manufacturing*, Vol. 13, pp. 1253-1260, https://doi.org/10.1016/j.promfg.2017.09.047

Premachandra, I.M., Chen, Y. and Watson, J. (2011), "DEA as a tool for predicting corporate failure and success: A case of bankruptcy assessment", *The International Journal of Management Science Omega*, Vol. 39, pp. 620-626. . https://doi.org/10.1016/j.omega.2011.01.002

Regulation (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed 20 August 2020).

Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council Text with EEA relevance, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012R1025 (accessed 20 August 2020).

Saen, R.F. (2010), "A new model for selecting third-party reverse logistics providers in the presence of multiple dual-role factors", *International Journal of Advanced Manufacturing Technology*, Vol. 46, pp. 405-410. https://doi.org/10.1007/s00170-009-2092-x

Safa, N.S., Maple, C., Watson, T. and Von Solms, R. (2018), "Motivation and opportunity based model to reduce information security insider threats in organisations", *Journal of Information Security and Applications*, Vol. 40, pp. 247-257, https://doi.org/10.1016/j.jisa.2017.11.001

Samonas, S., Dhillon, G. and Almusharraf, A. (2020), "Stakeholder perceptions of information security policy: Analyzing personal constructs", *International Journal of Information Management*, Vol. 50, pp. 144-154, https://doi.org/10.1016/j.ijinfomgt.2019.04.011

Sauerwein, C., Pekaric, I., Felderer, M. and Breu, R. (2019), "An analysis and classification of public information security data sources used in research and practice", *Computers & Security*, Vol. 82, pp. 140-155, https://doi.org/10.1016/j.cose.2018.12.011

Schmitz, C. and Pape, S. (2020), "LiSRA: Lightweight Security Risk Assessment for decision support in information security", *Computers & Security*, Vol. 90, https://doi.org/10.1016/j.cose.2019.101656

Segev, E. (2010), "Google and the Digital Divide: The Bias of Online Knowledge", Chandos Information Professional Series, Chandos Publishing, pp. 163-178, https://doi.org/10.1533/9781780631783

Shameli-Sendi, A. (2020), "An efficient security data-driven approach for implementing risk assessment", *Journal of Information Security and Applications*, Vol. 54, https://doi.org/10.1016/j.jisa.2020.102593

Singh, J. (2014), "Review of e-Commerce Security Challenges", *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 2(2), pp. 2850-2858.

Skopik, F., Settanni, G. and Fiedler, R. (2016), "A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing", *Computers & Security*, Vol. 60, pp. 154-176, https://doi.org/10.1016/j.cose.2016.04.003

Solak, S. and Zhuo, Y. (2020), "Optimal policies for information sharing in information system security", *European Journal of Operational Research*, Vol. 284, pp. 934-950, https://doi.org/10.1016/j.ejor.2019.12.016

Song, M., Wu, J. and Wang Y. (2011), "An extended aggregated ratio analysis in DEA", *Journal of Systems Science and* Systems *Engineering*, Vol. 20(2), pp. 249-256, https://doi.org/10.1007/s11518-011-5162-1

Sönmez, F.Ö. (2019). "A Conceptual Model for a Metric Based Framework for the Monitoring of Information Security Tasks' Efficiency", *Procedia Computer Science*, Vol. 160, pp. 181–188, https://doi.org/10.1016/j.procs.2019.09.459

Soomro, Z.A., Shah, M.H. and Ahmed, J. (2016), "Information security management needs more holistic approach: A literature review", *International Journal of Information Management*, Vol. 36(2), pp. 215-225, https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Szczepaniuk, E.K., Szczepaniuk, H., Rokicki, T. and Klepacki, B. (2020), „Information security assessment in public administration", *Computers & Security*, Vol. 90, https://doi.org/10.1016/j.cose.2019.101709

Technical Department of ENISA Section Risk Management ENISA: Risk Management - Principles and Inventories for Risk Management / Risk Assessment methods and tools, June 2006

Tewari, A. and Gupta, B.B. (2020), "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework", *Future Generation Computer Systems*, Vol. 108, pp. 909-920, https://doi.org/10.1016/j.future.2018.04.027

Tøndel, I.A., Line, M.B. and Jaatun, M.G. (2014), "Information security incident management: Current practice as reported in the literature", *Computers & Security*, Vol. 45, pp. 42-57, https://doi.org/10.1016/j.cose.2014.05.003

UNCTAD: Digital Economy Report 2019 (2019), "Value creation and capture: implications for developing countries", available at: https://unctad.org/en/PublicationsLibrary/der2019_en.pdf (accessed 20 August 2020).

Veiga, A. da, Astakhova, L.V., Botha, A. and Herselman, M. (2020), "Defining organisational information security culture—Perspectives from academia and industry", *Computers & Security*, Vo. 92, https://doi.org/10.1016/j.cose.2020.101713

Zu, T., Kang, R., Wen, M., and Yang, Y. (2018), An optimal model using data envelopment analysis for uncertainty metrics in reliability, *Soft Computing*, Vol. 22, pp. 5561–5568, https://doi.org/10.1007/s00500-018-3329-0

ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2021 Volume 9 Number 1 (September)
http://doi.org/10.9770/jesi.2021.9.1(8)

Agnes KEMENDI is PhD student at Doctoral School of Safety and Security Science, Óbuda University, Budapest, Hungary. Research interest: enterprise safety and security, information security with quality management and continuous improvement mindset.
ORCID ID: orcid.org/0000-0002-6452-8563

Pál MICHELBERGER is PhD in Military Technology, Professor at Institute of Mechanical Engineering and Security Sciences, Donát Bánki Faculty of Mechanical and Safety Engineering, Óbuda University, Budapest, Hungary. Research interests: IT projects, information security, introduction of standardised management systems, development of business processes.
ORCID ID: orcid.org/0000-0001-5752-0224

Agata MESJASZ-LECH is a Doctor habitat of management, Associate Professor on the Faculty of Management, Czestochowa University of Technology, Poland. Research interests: reverse logistics, inventory management, statistical analysis of logistics system effectiveness, sustainable entrepreneurship, application of statistical and econometric methods in the management process.
ORCID ID: orcid.org/0000-0001-9577-2772