2021
Vol.24 No.2

POLISH JOURNAL OF MANAGEMENT STUDIES
Kobis P., Karyy O.

IMPACT OF THE HUMAN FACTOR ON THE SECURITY OF INFORMATION RESOURCES OF ENTERPRISES DURING THE COVID-19 PANDEMIC

Kobis P., Karyy O.*

Abstract: This article aims to determine the impact of the human factor on the security of information resources of enterprises during the Covid-19 pandemic. The theoretical section of the article describes the phenomenon of the human factor in the security of intangible resources, and isolates the most important mistakes noted in the literature made by employees, clients, and business partners, affecting the level of security of the information system of business entities. The empirical section of the article contains an analysis of selected, current research by recognised business intelligence companies around the world, providing for the impact of the human factor on information security, along with comparing them to data from before the Covid-19 pandemic. The presented research was conducted both among the IT staff as well as persons who on a daily basis manage information resources in enterprises. The data was acquired with the use of electronic questionnaires and through an analysis of data coming from particular security software produced or distributed by the authors of reports. The research results contain an applicable, critical analysis. It has been proven that the current Covid-19 pandemic affects the security of information resources, and that remote work practiced in modern enterprises carries an increased risk of errors in information management. The purpose of the article is to present how changing the way of working during the pandemic affects information security, and to show the problems which modern enterprises are facing.

Key words: human factor, information security, enterprises, covid-19, remote work

DOI: 10.17512/pjms.2021.24.2.13

Article history:
Received August 21, 2021; *Revised* September 09, 2021*; Accepted* September 19, 2021

Introduction

The security of information resources is currently one of the main factors guaranteeing the proper functioning of business entities. This is due to the fact that the potential of a modern enterprise, which guarantees its competitiveness in the economic market (Haseeb et al., 2019; Gavurova et al., 2020, Bacik et al., 2019; Kemendi et al., 2021; Wysokińska-Senkus, Górna, 2021), is accumulated in its information resources, including patents, developed methods of producing products, databases of products and services, proprietary marketing methods, etc. Each economic entity also processes information related to personal data, which is under

*__Paweł Kobis,__ BEng, PhD, Czestochowa University of Technology, Faculty of Management
Oleh Karyy, Prof., Lviv Polytechnic National University, Department of Management of Organizations, Ukraine
✉ corresponding author: pawel.kobis@pcz.pl
✉ oleh.i.karyi@lpnu.ua

specific legal protection depending on the country. Any incidents of information security breach may result in taking over the intangible resources by third parties (e.g. competitors), their destruction, or making them public. As a consequence, an economic entity is exposed to, e.g.:
-loss of key information that distinguishes it from other enterprises on the economic market;
-loss of credibility and reputation among clients (e.g. publishing a list of their logins and passwords);
-loss of reputation and credibility among business partners;
-legal and financial sanctions (leakage of protected personal data).
Most of present information resources are stored and processed digitally using computer technology. It is a great facilitation in the processes of storing, processing, and analysing information. Contemporary IT tools using ICT networks allow large amounts of information to be processed in a relatively short time. They enable remote work, regardless of the location of the information carrier and computer software (cloud computing model). They facilitate virtual, international teams working together despite geographic distances. They make it possible to send virtually unlimited amounts of information at any distance in a relatively short time. This creates countless possibilities for development and creation of various work concepts. It also carries a number of risks. Information available via the Internet is exposed to attempts to illegally obtain it by third parties or attempts to deliberately destroy and block access (encryption-ransomware). Some of these incidents result from insufficient protection of information resources by enterprises, and some from non-observance of certain rules of their processing (human factor – Tamasevicius et al., 2020; Tóth et al., 2020; Plėta et al., 2020; Fakunle, Ajani, 2021). This article focuses on the (intentional and unintentional) mistakes made by employees during information management, which in turn lead to risks for the intangible resources of economic entities. Currently, during the COVID-19 pandemic, there is an increase in information loss incidents (Muangmee, et al., 2021). This may be due to many factors, and one of the most important of them is the increase in the amount of remote work in enterprises. The aim of the article is to present how this change of work organisation influenced the number of detected information security breach incidents. Problems with which modern economic entities have to face in the light of the forced change in the work organisation were shown.

Literature Review

Information security management is one of the fields in the comprehensive information management process. There are a few definitions of the concept of information management which, despite the passage of time and changes in the methods and technologies of information management, remain valid in the light of the management process itself. For example, C. W. Choo (2002) believes that "information management is a series of processes that support learning the organisation of: identifying information needs, obtaining information, organising

and storing information, developing information products, distributing information, and using it". D. A. Marchand (2000) believes that "information management handles the ways in which the enterprise is represented through information, the quality and integrity of information, and the use of information to create economic value for the enterprise".

The term “information management” has also been defined at the government level of many countries. For example, US government guidelines define this term as "planning, budgeting, processing, and controlling information throughout its life cycle; the life cycle is defined as stages through which information passes, which are typically characterised as creating or collecting, processing, spreading, using, storing, and disposing the information" (Zygała, 2007, p. 45).

However, the COVID-19 pandemic has forced companies to radically transform the way in which people process information and operate in their workplace. In order to survive on the market, business entities were forced to organise remote work. Work patterns have changed with the use of new digital systems to communicate and exchange information between the workplace (usually home) and the place where it is stored (company servers or cloud computing). The pandemic has made IT play a key role in many, if not all, (behavioural, temporal, social, organisational) aspects of work (Carroll & Conboy, 2020, p. 102186). Many enterprises that have so far avoided working remotely have been forced to introduce necessary "ad hoc" procedures due to the situation (Herath & Herath, 2020, p. 277–278). As a result, the solutions implemented under time pressure were and are not fully deliberate. They were intended to be temporary, but reality has shown that these solutions have to become a long-term alternative to "normal work.” While the organisation of remote work can be improved over a longer period (depending on the needs), the security of digital information resources must be ensured from the moment of implementing new forms of work.

Information security can be considered on:

-The technical level, and

-The behavioural level.

The technical level regards all hardware and software security, both on the side of employee and server where the information is stored. It also concerns the security of the medium itself through which information is sent (local networks, Internet network). They will not be described in this article.

The behavioural level, classified in the subject literature as a human factor, regards the behaviour of employees who manage information resources, and refers to their level of education, experience, knowledge, personal characteristics, current psychophysical state, intuition, instinct, etc (Hughes-Lartey et al., 2021; Safa and Maple, 2016(Kovačević i in., 2020); Ivanová et al., 2021; Shevyakova et al., 2021). It includes all human-made errors leading to an increased risk of a security breach incident (Evans et al., 2019; Kobis, 2021, p. 166). Actions leading to mistakes can be divided into deliberate and nondeliberate. In the case of deliberate actions, the issue is deliberate acting to the detriment of the enterprise for various reasons: the

desire to take revenge on the employer due to, for example, unsatisfactory remuneration, willingness to sell information to competitors, economic espionage or convenience, laziness manifested by the use of low-quality passwords, or failure to properly secure the workplace. However, nondeliberate actions result from a lack of knowledge about information security, lack of experience, or one's current psychophysical state: fatigue, illness, etc.

The human factor is perceived as a set of human characteristics and behaviours influencing the way a given system works or the behaviour of the environment. As a "component" of many systems functioning within business entities, a human is a key element that influences their operation. The human factor determines, for example, the functioning of IT systems implementing the processes of storing, searching, and processing information. The concept of the human factor is defined by Y. Wang (2008, p. 75), who writes that "Human factors are the roles and effects of human activity in the system, which introduce additional strengths, weaknesses, and uncertainties." It also determines the taxonomy of human factors, in which it specifies factors included in the three categories listed in the definition (Table 1).

Table 1. Taxonomy of human factors

Category	**Factors**
Strengths	Natural intelligence, autonomic behaviour, complex decision-making process, highly qualified actions, intelligent senses, perception power, complex human coordination, adaptability
Weaknesses	Low efficiency, slow reactions, proclivity to mistakes, fatigue, concentration loss
Uncertainties	Efficiency, accuracy, reaction time, persistence, reliability, approach, performance, motivation to try uncertain actions

Source: (Wang, 2008, p. 75)

Such an interpretation of the human factor concept as the one proposed by Wang is also used while considering security in the broad sense of the word (Kobis, 2021, p. 165).

Why is the human factor so important in the period of work reorganisation during the Covid-19 pandemic? It seems correct to assume the hypothesis that every economic entity aware of the risk, taking care of its own information base, will take steps to ensure the maximum technical security of its intangible resources. However, it does not have a large impact on the individual behaviour of its employees in relation to the processed information outside the company premises. While on the premises of the economic entity, we are dealing with a properly secured local computer network, potential monitoring of workstations, and direct control of the supervisor over the employee; in the employee's home conditions, we are dealing with their private computer network, and limited or no direct control. By giving an

employee the possibility to remotely access the company resources, we can only assume that their method of managing information will not contribute to its potential damage or loss (Ogbanufe, 2021; Vnoučková, 2020, p. 18–21). We can assume that the right level of employee training, knowledge, and experience will prevent them, for example, from accidentally sharing a computer with people from their immediate environment. Naturally, there can be many scenarios that increase the risk of information loss in the case of working at home, but all of them come down to the right or wrong behaviour of the person, as an "element" of the information security system.

How, therefore, can human factors in regard to information security be countered during the reorganisation of work caused by the Covid-19 pandemic? A certain number of vulnerabilities of the information system can be eliminated by means of technical security measures (imposing strong passwords, logging in with the use of biometric devices, using strong software security, and encrypting connections with VPN). However, these are widely-known solutions, and it should be assumed that enterprises that care about their resources will use them. However, they will not fully protect the economic entity from deliberate or nondeliberate human behaviour in the discussed range of information security (Babbs, 2020; Meshkat i in., 2020). It can be assumed that the key activities on the part of enterprises should be:

-creating suitable working conditions for employees - both social and in terms of technical equipment;

-recurrent training focused on security of remote work.

The first of these actions minimises the risk of deliberate moves of the employee. Creating a favourable working environment, both in terms of social and working conditions, should limit the willingness to act to the detriment of the employer (Kemper, 2019). Building a proper bond between an employee and their workplace may reduce, for example, their will to spy on behalf of third parties (competition). This is a broad topic which also takes into account other sciences, such as psychology and sociology, and goes beyond the science of management itself. Nonetheless, according to the author, it is very important from the point of view of information protection and crucial in the processes of creating its security.

The issue of training on the security of information resources is equally important. Certainly, a number of enterprises have been practicing this type of competence improvement among their employees for many years. However, actions should be taken to organise training courses focused primarily on the aspect of remote work. It is necessary to specify and pay attention to those elements which, while working at home, most often contribute to making mistakes leading to an increased risk of a specific incident. Trainings have a multi-levelled dimension for the organisation:

-they increase knowledge of software operation;

-they increase information security through the correct operation of the software;

-they increase employee efficiency by using applications which are full of potential;

-they increase the sense of confidence among employees;

-they facilitate decision making.

All of the above-mentioned points have a direct impact on the quality of information and knowledge management in an economic organisation. The only question is: how often should employees be trained? There is no clear answer here. It seems that the interested parties themselves should jointly decide on it, reporting their observations to their immediate superiors. Perhaps it depends on the pace of development of new technical and technological solutions, about which employees should be informed and trained (Bilan et al., 2020). It may depend on the emergence of new risks, requiring the employee to behave in a certain way and take possible action.

The implementation of the training, and setting its needs and goals, is a universal process. It can be based on the generally-known scheme of the training process in an economic organisation presented by R. W. Griffin (2004, p. 458) (Fig. 1).

The first point in the process is identifying training needs. This requires the use of proper tools for probing the needs of the target group. It can be an ordinary meeting, a conversation (e.g. via instant messaging), or it can also be a more official tool in the form of a questionnaire (e.g. electronic). A properly formulated questionnaire can also provide information on the level of training needs and training goals. The next steps in the process enable the development of a training program, the evaluation of the training after its completion, and the launch of activities aimed at refining the training program for other groups of learners.

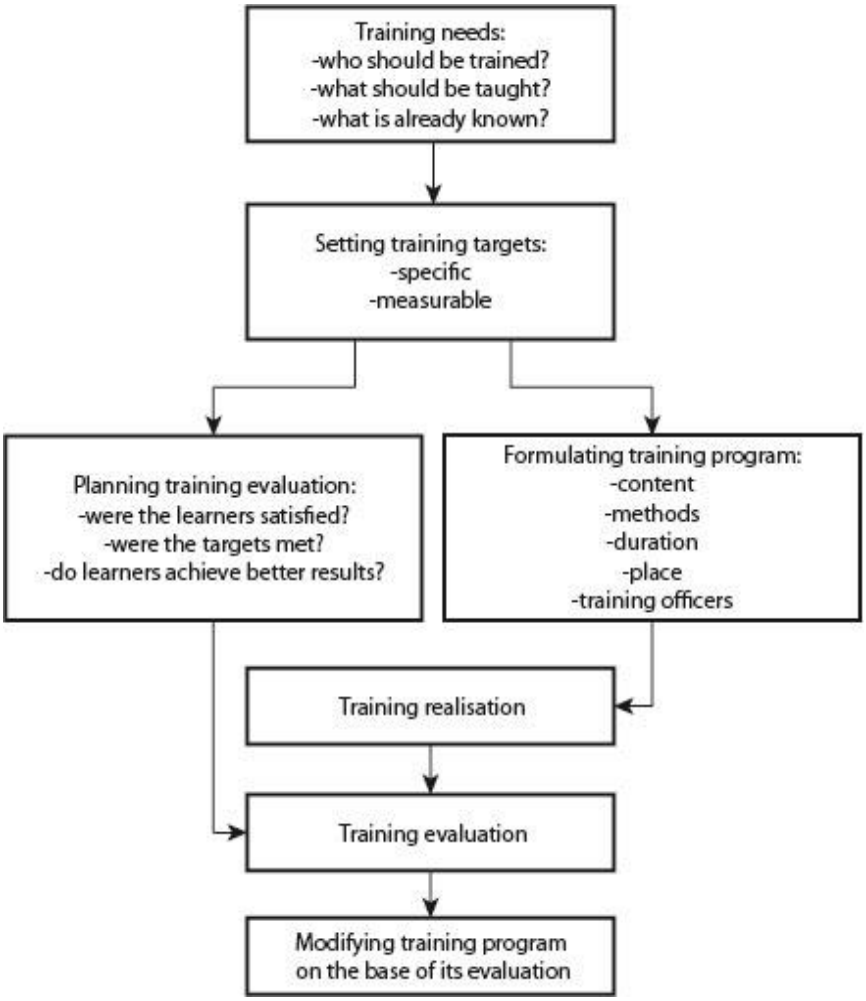

Figure 1: The training process in an economic organization
(Griffin, 2004, p. 458)

The knowledge and skills acquired during training are valuable and contribute to the effective management of resources of the entity. However, they alone are not enough. Skilled and willing employees who want to use their skills and abilities to build a market advantage of an economic entity, people who will motivate colleagues to achieve the set goals, are necessary: here, we return back to the first point, i.e. creating suitable working conditions for employees.

Methodology and Results

The presented research comes from multiple sources and has been acquired with the use of various research methods. Part of the research has been acquired using the

method of observation with regard to threats recorded by security software. In this way it was possible to acquire reliable results that reflect the actual state of occurring incidents. The research acquired from the report by VMWare was conducted by an independent research organisation Opinion Matters in December 2020. The research participants included 3542 CIO (Chief Information Officer), CTO (Chief Technology Officer) and CISO (Chief Information Security Officer) in companies f multiple trades, including the financial sector, healthcare, state and local government bodies, retail trade, production and engineering, food and beverages, municipal services, professional services, media and entertainment. The research constitutes part of a global research project run in 14 countries, including Australia, Canada, Saudi Arabia, Middle East, Great Britain, France, Germany, Spain, the Netherlands, Scandinavia, Italy, Japan, Singapore, and the United States. The research whose results have been presented in the report by Proofpoint, was conducted in the group of over 3500 employed adults in the United States, Australia, France, Germany, Japan, Spain, and Great Britain. The research, whose results presents the report by IBM, was conducted by Ponemon Institute in the period August 2019 – April 2020 in the group of 524 organisations that experienced security breaches. To make the conclusions of the research refer to a wide range of enterprises, organisations of various sizes were considered in the report, which came from 17 countries and regions, representing 17 different industries.

According to the study by IBM (The Hacker News, 2021), a human error is responsible for 95% of all cyber security breaches. Thus, a human is responsible for as many as 19 out of 20 intrusions into the information systems of economic entities (Aloha, 2021). According to a report published by Proofpoint, Inc. (2020 User Risk Report: Exploring Vulnerability and Behavior in a People-Centric Threat Landscape, 2020), as many as 26% of employees worldwide believe that public Wi-Fi networks are secure, over 50% do not protect home Wi-Fi networks with a password, 32% do not know what a virtual private network (VPN) is, and 90% of working adults admit that they use devices provided by an employer for personal activities. On the other hand, only 42% of respondents use a biometric lock (e.g. fingerprint) on a personal device (smartphone), 24% use a four-digit PIN code and 10% have no lock at all on their device. According to the same survey, as many as 50% of respondents admitted that they shared a corporate computer device with family or friends. According to the study by the National Center for Cyber Security (National Cyber Security Center, 2019), the "123456" password remains the most popular password in the world, and 45% of respondents use their email password again on other services.

All of the above studies were published in 2019 and 2020. Therefore, they cover both the period before the pandemic and the beginning of remote work. The presented results are highly concerning, given the general trend of working remotely during the pandemic. In the report entitled "Global Security Insights Report 2021: Extended enterprise under threat" (vmware, 2021), it was revealed that as many as 78% of global cybersecurity specialists stated that the number of attacks increased

because of employees working remotely, and 79% stated that the attacks had become more sophisticated. The greatest increase in the number of attacks based on working from home was recorded in France (96%), then Australia (89%), and the United Kingdom (86%). A lower percentage was recorded in the USA and Scandinavia (63%) (vmware, 2021, p. 18). It is suspected that this number may be higher, as the limited control over employees using the home network and personal devices does not fully reflect the actual scale of the phenomenon: a number of attacks are not detected (vmware, 2021, p. 4).

The transition of a large number of enterprises to remote work has exposed the weaknesses of the most important "element" of an information security system: the human. Lack of direct control over an employee and work in a private network environment increased the number of observed attacks on information resources of economic entities. The attackers were well aware of the fact that an employee performing the duties outside the company premises, and simultaneously communicating with its information resources, is a relatively easy target (Georgiadou et al., 2021(Ergen i in., 2021)). A particular increase has been recorded in the area of ransomware attacks (Richardson, 2021, pp. 5-8). Attacks of this type take advantage of the inattention or ignorance of the employee by sending specially-crafted e-mails that look like a real message (Burke, 2021, s. 12–14). By clicking on the "attachment" to the message (e.g. described as an invoice for payment), the user unknowingly launches the damaging encryption program. After the computer is infected, the recipient receives information about the ransom, the settlement of which will allow them to obtain the decryption key. Figure 2 presents the average ransom amounts obtained from entrepreneurs in individual quarters of 2020 as a consequence of ransomware attacks. The values are given in US dollars, although the ransom itself is most often made using cryptocurrencies. Ransomware attacks were most often recorded in countries such as Germany, France, the United States, the United Kingdom, Scandinavian countries, and Japan (vmware, 2021, p. 19). The increase in ransom amounts tie in with the outbreak of the COVID-19 pandemic. This correlation is also confirmed by Europol (2021), emphasising that the most common targets are organisations such as hospitals, governments, and universities.

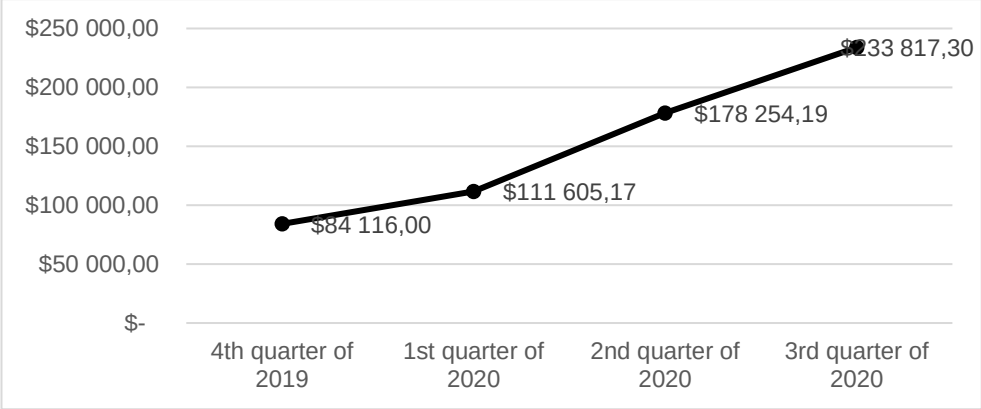

Figure 2: Average quarterly ransom payments for data decryption after ransomware attacks
(Sophos, 2021, p. 8)

The average ransom demand increased in the following quarters and almost tripled in one year. Criminal organisations analyse the costs of downtime of individual economic entities and "test" the ability of companies to obtain the ransom amount on this basis.
Remote work during COVID-19 requires connection with the information resources of the servers of economic organisations. Encrypted connections and proper data transfer protocols should be used for this purpose. It is necessary to create specific accounts for users of a given system, regardless of the connection method. It is important that these accounts have unique names and sufficiently strong passwords. Leaving "default" user names in server systems exposes economic entities to attacks from the global network. Figure 3 presents the top 5 usernames for all failed login attempts. This indicates that if the names of the default system accounts are not changed, there is a high probability of losing information resources. It should be emphasised here that the names mentioned in Figure 3 also appear on devices of end users: personal computers, laptops, and portable devices. It is important that users follow the rules for creating unique names themselves.

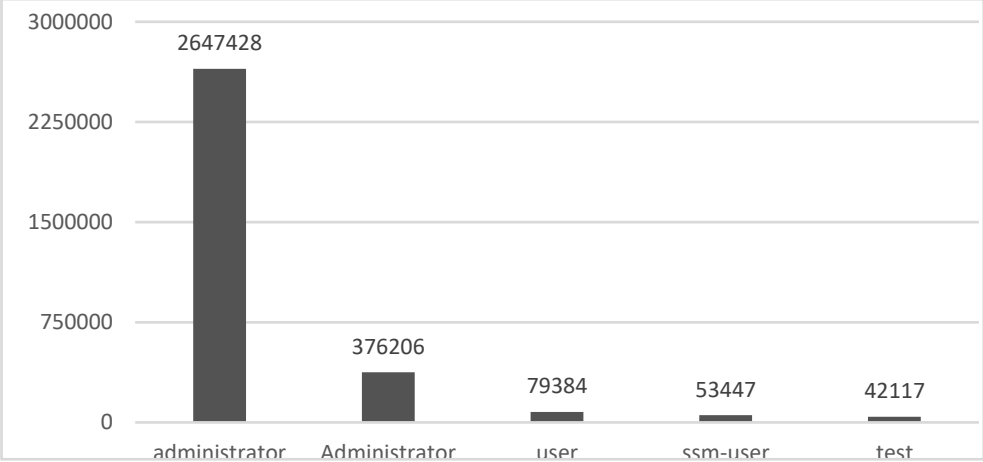

Figure 3: The 5 most common usernames for all failed login attempts
(Sophos, 2021, p. 15)

Figure 4 shows a graph comparing the current study from the report entitled "Global Security Insights Report 2021: Extended enterprise under threat" with an identical study published in 2020. Thus, a comparison of data from 2019 and 2020 was obtained, presenting the opinions of respondents on the most sensitive points/elements amenable to generating intrusions in the security infrastructure of an economic entity. The introduction of remote work in 2020 as a result of the COVID-19 pandemic had a significant impact on the results.

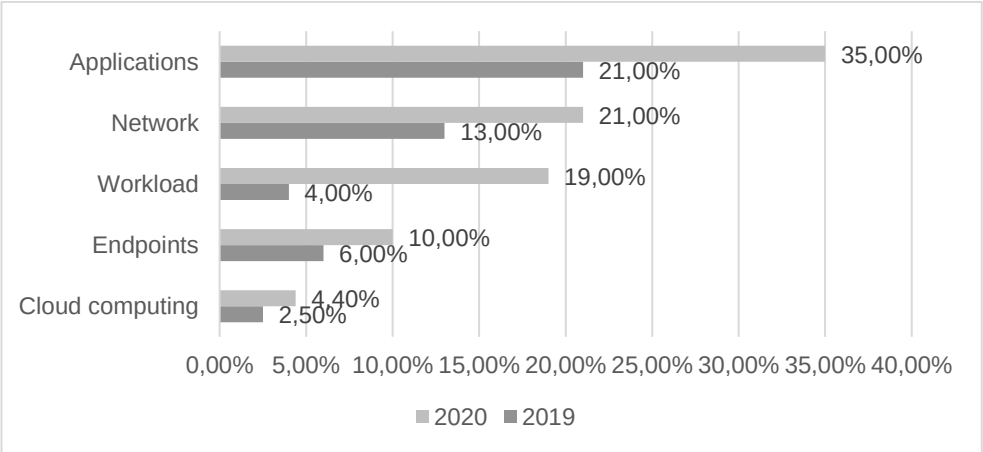

Figure 4: The most vulnerable points/elements amenable to generating intrusions in the security infrastructure
(vmware, 2021, p. 26)

Among the five areas mentioned in Figure 4, all of them obtained a higher result than in the previous year. As a result, the change in the organisation of work significantly contributed to the increase of the IT system susceptibility to potential dangers. The largest percentage increase was observed on the workload side. It can be concluded that remote work is more burdensome for employees: it requires greater concentration and autonomy with limited support from people from the company. A large increase in "applications" can also be observed. This is likely related to the lack of systematicity in system and software updates at home, vulnerability detection by cybercriminals during remote work, and connecting to the server or cloud computing. The following values concern:
-network - here, the important thing is for the user to use encrypted transmission (VPN), SSL, and TLS protocols, and not unsecured networks (public hotspots);
-endpoints - proper protection of personal computers, not sharing the computer with unauthorised people (family, friends);
-cloud computing - proper determination of logins and passwords to access cloud computing resources, not sharing them with third parties.
The presented examples of increased activity of cybercriminals during the pandemic present only selected aspects of the existing problem. There are many more (Khan et al., 2020; Lallie et al., 2021). There is a need to constantly monitor the current risks and develop effective plans to counter them. In the field of the human factor, the most effective seems to be the implementation of the process of raising continuous awareness of users through their training and increasing qualifications.

Discussion

The presented research results are a part of the phenomena covering the issues of security of information resources. The author is aware that there are many levels and areas in which the change of the mode and organisation of work stem from the need to pay attention to aspects that did not take place in traditional work. There are also a number of other risks not listed in this article; it would be impossible to address them all within the framework of one study. This study is aimed at drawing attention to the human factor when it comes to providing three selected examples of foreign research.
The research is in line with the extensive research pertaining to the human factor in information security. While considering the number of the attacks that aim at acquiring ransom (Fig. 2) and analysing other research related to information security one can observe certain correlations. For instance, in the report published by the British company Tessian (2021, p. 5), one can read that as many as 1 in 4 of the surveyed respondents in the course of work clicked on a phishing email, which is a primary source of malicious software encrypting information. Additionally, according to the same research as many as 57% of employees are more distracted while working from home, which undoubtedly contributes to surge of threats. The situation is not improved by the fact that as many as 50% of employees make more

mistakes when they are stressed, and 43% is more prone to errors being tired. The research included in the report by Tessian also shows that 93% of the survey participants have experienced tiredness and stress at work, and 1 out of 10 persons feels tired every single day of the week. Thus, it can be concluded that the curve shown in Figure 2 is a resultant of all the causes of errors.

Then, while analysing the presented in Figure 3 names that are most frequently used in all the unsuccessful attempts of logging in, one can conclude that the basic form of security is to establish unique names, which will constitute a primary barrier for persons who want to gain illegal access to information resources. This is particularly important in the cloud computing model, in which logging data allows for full access to information resources. In a sense, this is confirmed by the research presented in Figure 4, where applications and the network are the most vulnerable points/elements susceptible to generating break-ins. In the case of applications and the network one can also consider information security from the perspective of BYOD (Bring Your Own Device) trend, which has intensified during the Covid -19 pandemic and remote work. This has been confirmed by the research „2021 BYOD Security Report" published by Cybersecurity Insiders (2021, p. 3), where one can learn that 47% of organisations have observed a significant increase in BYOD use caused by transition to remote work at the time of COVID 19 pandemic. Additionally, 29% of the investigated organisations are unable to control the devices used by their employees.

By forcing economic entities to change the form of work organisation, the COVID-19 pandemic made entrepreneurs aware of how dynamic our world is, and how quickly it is necessary to adapt to the new realities. It could be stated that the pandemic opened a "new chapter" in the activities of economic entities: it made people aware of the need to be ready for constant changes, also in the future, after the pandemic ceases. Even in the period of stabilisation, enterprises must constantly improve their resource management facilities, including information management, in order to adapt to the changing reality in a relatively short time, using the latest solutions available on the market. They should implement plans and solutions enabling continuous training of their employees, so that human resources are provided with skills and competences that enable the best possible implementation of the tasks set by the company.

The changes faced by modern enterprises had to be introduced practically "overnight." Some economic entities, who had no experience in remote work, were forced to quickly introduce selected solutions. The result of such activities was the weakening of IT infrastructures in terms of their security, with particular emphasis on the human factor. It can be assumed with high probability that, at the time of introducing new solutions, many enterprises did not anticipate the fact that these solutions would become part of the daily operation of the organisation for the next several months. However, currently, as we are not able to predict the date of return to the original structure of work organisation, all measures should be taken to

minimise the risk of threats to information: a resource which is the main element of competitive advantage in the economic market in the modern world.

Summary

This article raises current issues of the security of enterprise information resources during the reorganisation of work during the COVID-19 pandemic. Selected issues are described, along with current research that directly refers to the human factor as one of the main reasons for generating threats in the information environment.

The research has been conducted by renowned IT firms that provide solutions for customers all over the world and information agencies with a research potential that allows to gather information on all the continents. Therefore, in the opinion of the author the selection of foreign research for this paper was purposeful and appropriate. This is conditioned by the particular time period, which the research refers to. Moreover, the dynamics of changes in the information security area driven by COVID-19 is so large that the potential of possibly best reflection of the actual state on the global scale lies only with the largest research organisations. Certainly, it is scientists who should analyse this research, and the author believes this has been done in the paper.

The author is aware that the research area discussed in the study is very broad and covers a number of issues that have not been discussed here due to the volume of the article. The article is aimed at contributing to the discussion on information security, with particular emphasis on the human factor in information management security. The issues raised in the study may constitute the basis for further considerations in the area of security on the change of the form of work performance, and the related change in the form of information processing, which was compelled by the existing COVID-19 pandemic.

The presented in the paper aspects pertaining to the impact of the human factor on information security should inspire economic entities to develop secure systems of non-material resources management. The presented results also outline the areas which require particular attention in terms of security. The change of the paradigm of rendering work from on-site to remote, which has been driven by the existing pandemic, has reorganised functioning of enterprises to such an extent that information security needs to be perceived from a new perspective.

The presented research pertains to threats and security of information management on a global scale. Therefore, this should constitute a basis for conducting this type of research on the micro-region scale, as this constitutes a rich source of inspiration in the scope of the research area.

References

Ahola, M., (2021). The Role of Human Error in Successful Cyber Security Breaches. Usecure.

Babbs, A., (2020). How to leverage data security in a post-Covid world. *Computer Fraud & Security*, 2020(10), 8–11.

Bacik, R., Fedorko, R., Abbas, E. W., Rigelsky, M., Ivankova, V. and Obsatnikova, K., (2019). The impact of selected quality management attributes on the profitability of TOP hotels in the Visegrad group countries. *Polish Journal of Management Studies*, 19(1), 46–58.

Bilan, Y., Hussain, H. I., Haseeb, M. and Kot, S., (2020). Sustainability and Economic Performance: Role of Organizational Learning and Innovation. *Engineering Economics*, 31(1), 93–103.

Burke, S., (2021). How to prepare for the onslaught of phishing email attacks. *Computer Fraud & Security*, 2021(5), 12–14.

Carroll, N., Conboy, K., (2020). Normalising the "new normal": Changing tech-driven work practices under pandemic time pressure. *International Journal of Information Management*, 55, 102186.

Choo, C. W., (2002). Information Management for the Intelligent Organization: The Art of Scanning the Environment. Information Today, Inc., Medford.

Cybersecurity Insiders. (2021). BYOD Security Report, Available at: https://www.cybersecurity-insiders.com/portfolio/2021-byod-security-report-bitglass/ Access on: 27.09.2021.

Ergen, A., Ünal, A. N. and Saygili, M. S., (2021). Is It Possible to Change the Cyber Security Behaviours of Employees? Barriers and Promoters. *Academic Journal of Interdisciplinary Studies*, 10(4).

Europol. (2021). Covid-19: Ransomware. Available at: https://www.europol.europa.eu/covid-19/covid-19-ransomware. Access on: 22.06.2021.

Evans, M., He, Y., Maglaras, L., Yevseyeva, I. and Janicke, H., (2019). Evaluating information security core human error causes (IS-CHEC) technique in public sector and comparison with the private sector. *International Journal of Medical Informatics*, 127, 109–119.

Fakunle, S. O., Ajani, B. K., (2021). Peculiarities of ICT adoption in Nigeria. *Insights into Regional Development*, 3(4), 51-61.

Gavurova, B., Belas, J., Bilan, Y. and Horak, J., (2020). Study of legislative and administrative obstacles to SMEs business in the Czech Republic and Slovakia, *Oeconomia Copernicana*, 11(4), 689–719.

Georgiadou, A., Mouzakitis, S. and Askounis, D., (2021). Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal*.

Griffin, R. W., (2004). *Podstawy zarządzania organizacjami (II zmienione).* Wydawnictwo Naukowe PWN. Warszawa.

Haseeb, M., Hussain, H. I., Kot, S., Androniceanu, A. and Jermsittiparsert, K., (2019). Role of Social and Technological Challenges in Achieving a Sustainable Competitive Advantage and Sustainable Business Performance. *Sustainability*, 11(14), 3811.

Herath, T., Herath, H. S. B., (2020). Coping with the New Normal Imposed by the COVID-19 Pandemic: Lessons for Technology Management and Governance. *Information Systems Management*, 37(4), 277-283.

Hughes-Lartey, K., Li, M., Botchey, F. E. and Qin, Z., (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon*, 7(3), e06522.

Ivanová, E., Žárská, V. and Masárová, J., (2021). Digitalization and human capital development. *Entrepreneurship and Sustainability Issues*, 9(2), 402-415.

Kemper, G., (2019). Improving employees' cyber security awareness. *Computer Fraud & Security*, 2019(8), 11–14.

Khan, N. A., Brohi, S. N. and Zaman, N., (2020). *Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic*. TechRxiv. Preprint.

Kemendi, A., Michelberger, P. and Mesjasz-Lech, A., (2021). ICT security in businesses – efficiency analysis. *Entrepreneurship and Sustainability Issues*, 9(1), 123-149.

Kobis, P., (2021). *Zarządzanie bezpieczeństwem informacji w systemach informacyjnych małych i średnich przedsiębiorstw z uwzględnieniem czynnika ludzkiego.* Towarzystwo Naukowe Organizacji i Kierownictwa. Dom Organizatora. Toruń.

Kovačević, A., Putnik, N. and Tošković, O., (2020). Factors Related to Cyber Security Behavior. *IEEE Access*, 8, 125140–125148.

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C. and Bellekens, X., (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, 105, 102248.

Marchand, D., (2000). *Competing with Information: A Manager's Guide to Creating Business Value with Information Content* (D. A. Marchand, Red.; 1 edition). Wiley.

Meshkat, L., Miller, R. L., Hillsgrove, C. and King, J., (2020). Behavior Modeling for Cybersecurity. *2020 Annual Reliability and Maintainability Symposium (RAMS)*, 1–7.

Muangmee, C., Kot, S., Meekaewkunchorn, N., Kassakorn, N., Khalid, B., (2021). Factors determining the behavioral intention of using food delivery apps during covid-19 pandemics. *Journal of Theoretical and Applied Electronic Commerce Research*, 16(5), 1297-1310

National Cyber Security Centre., (2019). Most hacked passwords revealed as UK cyber survey exposes gaps in online security. Available at: https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security. Access on: 17.06.2021.

Ogbanufe, O., (2021). Enhancing End-User Roles in Information Security: Exploring the Setting, Situation, and Identity. *Computers & Security*, 108, 102340.

Plėta, T., Tvaronavičienė, M. and Della Casa, S., (2020). Cyber effect and security management aspects in critical energy infrastructures. *Insights into Regional Development*, 2(2), 538-548.

Proofpoint, Inc., (2020). 2020 User Risk Report. Exploring Vulnerability and Behaviour in a People-Centric Threat Landscape.

Richardson, R., (2021). Ransomware: The Landscape Is Shifting - A Concise Report. *International Management Review*, 17(1), 5-8.

Safa, N. S., Maple, C., (2016). Human errors in the information security realm – and how to fix them. *Computer Fraud & Security*, 2016(9), 17–20.

Shevyakova, A. Munsh, E., Arystan, M. and Petrenko, Y., (2021). Competence development for Industry 4.0: Qualification requirements and solutions: *Insights into Regional Development*, 3(1), 124-135.

Sophos., (2021). Sophos 2021 Threat Report: Navigating cybersecurity in an uncertain world.

Tamasevicius, V., Diskiene, D. and Stankeviciene, A., (2020). Human Resource Management Practice in Lithuania: Evidences and Challenges, *Montenegrin Journal of Economics*, 16(1), 207-226.

Tessian., (2021), Psychology of Human Error. Understand the mistakes that compromise your company's cybersecurity.

The Hacker News., (2021). Why Human Error is #1 Cyber Security Threat to Businesses in 2021. The Hacker News.

Tóth, A., Juhász, T. and Kálmán, B., (2020). The Role of Innovation and Human Factor in the Development of East Central Europe. *Montenegrin Journal of Economics*, 16(1), 251-274,

VMWare., (2021). Global Security Insights Report. Extended enterprise under threat 2021. vmware.

Vnoučková, L., (2020). Impact of COVID-19 on human resource management. *Revista Latinoamericana de Investigación Social*, 3(1). 18-21.

Wang, Y., (2008). On Cognitive Properties of Human Factors and Error Models in Engineering and Socialization. *International Journal of Cognitive Informatics and Natural Intelligence*, 2(4), 70-84.

Zygała, R., (2007). *Podstawy zarządzania informacją w przedsiębiorstwie*. Wydawnictwo Akademii Ekonomicznej im. Oskara Langego we Wrocławiu. Wrocław.

Wysokińska-Senkus, A., Górna, J., (2021). Towards sustainable development: risk managemet for organizational security. *Entrepreneurship and Sustainability Issues*, 8(3), 527-544.

WPŁYW CZYNNIKA LUDZKIEGO NA BEZPIECZEŃSTWO ZASOBÓW INFORMACYJNYCH PRZEDSIĘBIORSTW PODCZAS PANDEMII COVID-19

Streszczenie: Celem artykułu jest określenie wpływu czynnika ludzkiego na bezpieczeństwo zasobów informacyjnych przedsiębiorstw podczas pandemii Covid-19. W części teoretycznej artykułu opisano zjawisko czynnika ludzkiego w bezpieczeństwie zasobów niematerialnych oraz wyodrębniono najważniejsze błędy odnotowane w literaturze przez pracowników, klientów i partnerów biznesowych, wpływające na poziom bezpieczeństwa systemu informatycznego podmioty gospodarcze. Część empiryczna artykułu zawiera analizę wybranych, aktualnych badań uznanych wywiadowni gospodarczych na całym świecie, dotyczących wpływu czynnika ludzkiego na bezpieczeństwo informacji, wraz z porównaniem ich z danymi sprzed pandemii Covid-19. Prezentowane badanie zostało przeprowadzone zarówno wśród pracowników IT, jak i osób na co dzień zarządzających zasobami informacyjnymi w przedsiębiorstwach. Dane pozyskano za pomocą ankiet elektronicznych oraz poprzez analizę danych pochodzących z określonego oprogramowania zabezpieczającego produkowanego lub dystrybuowanego przez autorów raportów. Wyniki

badań zawierają stosowną, krytyczną analizę. Udowodniono, że pandemia Covid-19 wpływa na bezpieczeństwo zasobów informacyjnych, a praca zdalna praktykowana w nowoczesnych przedsiębiorstwach niesie ze sobą zwiększone ryzyko błędów w zarządzaniu informacją. Celem artykułu jest przedstawienie, jak zmienia się sposób pracy w czasie pandemii wpływa na bezpieczeństwo informacji, a także pokazuje problemy, z jakimi borykają się współczesne przedsiębiorstwa.

Słowa kluczowe: czynnik ludzki, bezpieczeństwo informacji, przedsiębiorstwa, covid-19, praca zdalna

COVID-19 大流行期间人为因素对企业信息资源安全的影响

摘要：本文旨在确定 Covid-19 大流行期间人为因素对企业信息资源安全的影响。文章的理论部分描述了无形资源安全中人为因素的现象，并隔离了员工、客户和业务合作伙伴在文献中指出的最重要的错误，这些错误影响了无形资源信息系统的安全水平。商业实体。本文的实证部分包含对全球知名商业智能公司当前选定的研究的分析，提供人为因素对信息安全的影响，并将其与 Covid-19 大流行之前的数据进行比较。所呈现的研究是在 IT 人员以及日常管理企业信息资源的人员中进行的。这些数据是通过使用电子问卷并通过分析来自报告作者制作或分发的特定安全软件的数据而获得的。研究结果包含适用的批判性分析。事实证明，当前的 Covid-19 大流行会影响信息资源的安全，现代企业中的远程工作会增加信息管理出错的风险。这篇文章的目的是展示如何改变工作方式 大流行期间影响信息安全，并展示现代企业面临的问题

关键词：人为因素，信息安全，企业，covid-19，远程工作