Awareness Level of Information Security Managers in Small Enterprises in Poland

Paweł Kobis and Grzegorz Chmielarz
Faculty of Management, Czestochowa University of Technology, Poland

pawel.kobis@pcz.pl
grzegorz.chmielarz@pcz.pl

Abstract: The security of information assets largely depends on the real level of knowledge of those managing the information system. Particularly important is the knowledge acquired on an ongoing basis through reading and analysing: new reports published by specialised intelligence services worldwide, thematic portals, industry and scientific publications. Today's rapid pace of development of information, communication systems means that knowledge of digital information security acquired a year or more ago becomes partly outdated. Although there are specific, unchangeable canons of behaviour, proceedings in the processes of information protection - they are only a foundation for building an effective system of protecting intangible resources. Special attention should be paid to the fact that information protection is not an individual activity - it is a process running parallel to all processes operating in enterprises. The global pandemic situation has had an irreversible impact on the perception of information asset security. The situation in which most business entities were forced to work remotely necessitated a new approach to information security among its managers. The relatively stable environment of business entities until the pandemic suddenly forced the use of new techniques and technologies enabling work from private, home networks. Have such conditions changed the attitudes of security managers to the need for continuous education, to expand their knowledge in this area? Did those responsible for the security of intangible assets gain more experience with information security during the pandemic? The aim of this article is to present research on the knowledge and awareness of information security managers conducted before the pandemic in 2018 and 2019 among small businesses in Poland on the real perceptions of those responsible for information security and to compare them with the same research conducted in 2022 after the pandemic.

Keywords: Information security, Small businesses, Security management, Information security awareness

1. Theoretical introduction

The human factor is currently the catalyst for most of the risks recorded in modern companies (Hughes-Lartey et al, 2021; Lin et al, 2022; Metalidou et al, 2014). There is a need to implement a number of measures to secure information assets in the area of human information management. For example, cyber-security experts advocate the need to train personnel in cyber-awareness and to become acquainted with new ways of social engineering functioning (Tayouri, 2015; Washo, 2021). Five main recommendations for reducing the risk of information security breaches can be found in the literature (Sedgwick, 2019):

- The need for pre-implementation testing of new technological solutions implemented in companies in order to avoid unwanted actions on the part of users (employees). The design of the system should take into account both the ergonomics of work and minimise the generation of accidental errors on the part of employees.
- The need to organise regular awareness training on IT security.
- Implementation of "cyber hygiene" principles in companies.
- Establishing rules of cooperation between employees and those responsible for information security. Building a support and assistance system for employees.
- Building a system to encourage reporting of information security breaches. Eliminating situations where security breaches are covered up by employees.

In order for the recommendations listed above to be implemented, they must be understood by managerial personnel of enterprises. Those responsible for information system security should be familiar with the realities of modern threats, and be able to transfer them to the operation of a particular enterprise. It is very important to understand the principles of risk management and the impact of the human factor on these risks (Shaikh & Siponen, 2023; Noga & Brzeziński, 2022). It is essential to classify the possible information security risks in the area of organisational functioning and to be able to determine their relevance to individual departments/workstations (Kobis, 2021, pp. 267-268).

2. Research Methodology

The research presented was carried out twice, in the same way, on the same number of: 287 enterprises with a time interval of 3 years. In the second survey, the majority of enterprises overlapped with those in the first survey, and a small number were new. This was due to the fact that, between the first and second surveys, some enterprises had ceased their activities or developed from small enterprises into micro-enterprises. The research techniques adopted for the survey were the F2F (Face to Face) face-to-face questionnaire interview with the use of a computer (CAPI - Computer Aided Personal Interview), which in some cases was replaced by an interview conducted via instant messaging allowing direct, natural audio-visual contact with the respondent while adhering to the applicable rules for conducting the survey, and the CAWI (Computer-Assisted Web Interview) technique. Thus, the so-called Mixed-Mode was used. The same questionnaire was used in both techniques. The first research took place in 2018-2019, the second in 2022. The inspiration to repeat the same research was the turbulent pandemic period for companies, which, by changing the form of work provision (remote working) in many cases, significantly affected the perception of information security among business entities. Thus, it is the authors' intention to compare the findings obtained before and after the pandemic period. The people surveyed were those in entities who had the greatest knowledge of information security and who were directly involved in the processes of establishing and updating security policies in the organisation. Thus, these included such individuals as heads of IT departments, employees of IT departments, individuals specifically (full-time or part-time) involved in the security of digital information assets, presidents, directors, owners and co-owners.

The presented research results represent a slice (fragment) of the authors' research conducted in the area of the SME sector and concerning the security of information resources.

3. Research Results and Discussion

The starting point in estimating the knowledge regarding the impact of the human factor on information security among those responsible for protecting information assets is to determine its importance in the minds of respondents (Kobis, 2021, p. 268).

Table 1 presents the results of a survey showing the view of the level of effectiveness of IT security safeguards in the information system of an enterprise. These safeguards can be broadly divided into technical and behavioural safeguards. The former refer to all physical and software safeguards that hinder or, in selected cases, eliminate the possibility of an attack on information resources. Behavioural safeguards are a set of measures aimed at training and making employees aware of the principles of proper information security management, so that it does not fall into the wrong hands. It should be noted here that currently available research indicates that the human factor is mostly responsible for the loss or destruction of information in modern organisations. During the first survey in 2018-2019, as many as 57.8 per cent of the respondents said that professional software and hardware security was able to eliminate most incidents of information loss and leakage. Only 25.1 per cent of them held the opposite view. This means that only in one in four enterprises, those caring for information security were aware of the real impact of non-technical factors in reducing the risk of unwanted incidents. The situation changed slightly in 2022, with a predominance of respondents on the side of ineffectiveness of physical security (49.1%) over those in favour of it (41.5%). The percentage of those who could not decide on the question also decreased.

The pandemic period forced many entities to work remotely (Benitez et al., 2023). Thus, employees performed their duties from their homes, private networks, and public networks, often on their own, unprotected computing devices. Many of the respondents, responsible for information security in their own enterprises, realised that it was largely up to the employee to keep information resources secure or not. In remote working, many of the safeguards previously in place on the enterprise's internal network did not directly translate into security on the employee's private network. It is mainly up to the employee to ensure that the information is secure.

Table 1: Respondents' Answers to the Question: Is Professional IT Security a Guarantee of Information Security in the Enterprise?

	2018/2019 research		2022 research	
	Number	Percentage	Number	Percentage
Yes, physical and software safeguards are able to eliminate most incidents of information loss and leakage	166	57,8%	119	41,5%
No, physical and software safeguards do not guarantee the elimination of most threats of information loss and leakage	72	25,1%	141	49,1%
No opinion	49	17,1%	27	9,4%

Source: Own elaboration

Unfortunately, the current figure of 41.5 % is still not encouraging. Many entities believe that technical security is the most important. This mindset may contribute to a significant increase in malware incidents. It justifies the belief among cybercriminals that a more effective form of attack on information assets is through the human factor. This is a very dangerous phenomenon, given the multitude of types of solutions currently in place. In extreme cases, without proper safeguards, malware can operate in a company for months or years. An example of this is spyware, which can continuously collect certain information and transmit it without the owner's knowledge to others. Apart from using part of the hardware resources, the programme does not reveal its presence and is therefore 'invisible' to the user. In the case of modern computers with significant memory resources and high computing power, the load of a spyware programme can be completely unnoticeable in day-to-day operation.

Extending the discussion, the attitudes of enterprises in terms of combating potential risks, it is worth identifying, according to the respondents, the sources of security incidents. Table 2 shows the areas in which enterprises engage their financial and human resources to minimise potential risks.

Table 2: Sources of Possible Threats to the Information System, Together with the Percentage Level of Enterprise Involvement in Terms of Their Potential Combating

	2018/2019 research		2022 research	
	Number	Percentage	Number	Percentage
IT risks (software and hardware)	160	55,7%	104	36,3%
Threats related to the "human factor", social engineering activities	92	32,1%	166	57,8%
Direct physical threats (burglary, theft of equipment, documents)	35	12,2%	17	5,9%

Source: Own elaboration

In the first round of the survey (2018-2019), again, as in the previous survey, the most important area according to respondents is IT (software and hardware) threats. As many as 55.7 per cent of the organisations overall engaged their resources in combating such dangers. Only 32.1% perceived threats from behavioural activities. In the 2022 survey, there was a polarisation of indications after the pandemic. Only 36.3% of the respondents viewed the source of possible threats on the software and hardware side, compared to 57.8% of the respondents. As with the previous question, the reason for the change in view of these aspects can be found in the change in the form of work provision from stationary to remote. It was in the responsibility of the employee that security for information resources was sought.

The least involvement of enterprises (in both the first and second surveys) can be seen on the level of direct, physical threats (burglary, equipment theft). Attempts to illegally obtain information tend to be of a remote nature - via a computer network or human factors: employee bribery, business intelligence, etc. Cases of physical intrusions for the sole purpose of obtaining information are relatively rare. The loss of intangible resources in this way tends to be related to actions aimed at stealing the equipment and tangible assets on which (disks, internal memories) the information was stored.

Table 3 shows the share of companies that allow or prohibit access from computing devices to social networking sites and online chat rooms. Both before and after the pandemic period, this ratio is similar and has not changed much.

Table 3: Percentage Share of Companies Whose Information Security Policy Does or Does not Allow Access from Company Computer Devices to Social Networking Sites, Online Chat Rooms, etc.

	2018/2019 research		2022 research	
	Number	Percentage	Number	Percentage
Yes	222	77,4%	213	74,2%
No	65	22,6%	74	25,8%

Source: Own elaboration

Applications used to communicate over the internet pose risks that can be divided into:

- unauthorised and uncontrolled transmission of information in the form of text or files by company employees;
- accidental or intentional posting of company-related material on social networks; and
- fake news and hyperlinks sent by cyber criminals;
- other activities organised by cyber criminals using social engineering.

It is also important to note whether instant messaging is used for work-related purposes or whether it is only used for private conversations.

Transmission of text or files via instant messaging typically occurs in three cases:

1. Text and file transfer between employees - a quicker and easier path than using official tools (e.g. document exchange system).
2. Transmission of text and files to third parties by dishonest/bribed employees.
3. Text transfer to friends, family.

In the first case, the danger is limited to the transmission of an unencrypted signal (this is the default setting of most communicators) and thus easily accessible to eavesdropping by third parties. In the second case, we are talking about the easy, uncontrolled, difficult-to-monitor transmission of files with virtually no quantitative limits. In the third case, with potentially the least harm, we are talking about the possible disclosure of confidential information during a conversation and eavesdropping by third parties (Curry, 2013).

Posting company-related material on social networks usually involves publishing photos of the workplace and possible information about the nature of the work being done. This information can be used for potential social engineering activities by cybercriminals. In addition, posted photos may reveal information that was accidentally photographed, which may be potentially relevant to criminal activities.

Significant threats from instant messaging and social networking sites include fake posts, spreading information containing hyperlinks to infected sites and malware. The appearance and content of messages crafted by cybercriminals usually inspire a high level of trust among users, which increases the potential risk of the threat. The most common threats are XSS (Cross-Site Scripting), SNS (Social Networking Service) and so-called phishing to extract relevant information from users through social engineering activities (Gruber et al., 2012, p. 356).

A group of socio-technical activities also includes 'impersonation' on social networks and instant messaging sites by persons known or potentially known to a specific employee. When contacting a specific employee, for example, the cybercriminal introduces himself as, for example, "a colleague from another department of the organisation" and tricks the employee into providing certain information under the pretext of performing his duties.

As in the case of instant messaging and social networking, it is important from the point of view of information security to implement general rules for the use of the global network. The multitude of communication solutions and technologies that allow to carry out conversations or send information of virtually any size without the use of any additional programs (e.g. https://wetransfer.com/) should result in the implementation of a set of rules for the use of network resources. At present, any website (store, information portal, theme portal, auction system, etc.) can be a source of threat to the intangible resources of a business organisation.

Establishing internal regulations that normalize the rules of network use, also providing for certain sanctions for employees, can become one of the more effective tools for reducing the risk of information security breaches. According to the survey, as many as 66.9% (in 2018-2019) and 64.8% (in 2022) of enterprises have no regulations in this regard (Table 4). This is not an optimistic result and indicates the need for quick action before business entities. This is an important aspect, as the literature shows a steady increase in reported attacks through crafted and infected websites.

Table 4: Percentage of companies With or Without an Internal set of Rules for Using Internet Resources in Their Information Security Policy

	2018/2019 research		**2022 research**	
	Number	**Percentage**	**Number**	**Percentage**
Yes	95	33,1%	101	35,2%
No	192	66,9%	186	64,8%

Source: Own elaboration

Another threat to the security of information resources that has the hallmarks of a human factor is the use and manner in which employees use portable data storage (Pabian et al., 2020). Modern technology makes it possible to store hundreds of GB of data in a volume of 1-2 cm^3. This means that practically imperceptibly any employee with access to information resources can copy them and carry them unnoticed outside the enterprise area. Moreover, the currently popular "flash drives" are for many people the primary storage place for documents and software files used in daily work. This is due to the convenience, speed of access and versatility of such a solution. These solutions, due to their practical advantages, can also be used for private purposes. In practice, situations arise in which users store both "company" and personal materials on portable data stores in parallel. All these situations can lead to such risks as:

- using portable data storage devices to steal information;
- storing, for example, the only copy of a particular document on a memory stick (the employee edits the files directly on the USB drive);
- possibility of disclosing information to third parties, e.g. while viewing private information on the same medium;
- losing the data carrier and, consequently, the possibility of unauthorised persons intercepting the information;
- the possibility of infecting a workplace computer workstation by first connecting the USB storage medium to other (e.g. private) computer devices.

In order to prevent the aforementioned risks, it is recommended to block or review any portable data storage in business organizations. Various software solutions are used for this purpose, allowing to maintain control over these resources in any programmed way. Table 5 shows the results describing the position of the surveyed economic entities on the aforementioned issue. Only 23.3% of enterprises had developed control mechanisms in 2018-2019. Three years later, this percentage has increased very little (25.8%). This is a low result exposing the vulnerability of enterprises' information systems to relatively simple ways of losing information., Interestingly, for three years, 4.8% of enterprises have introduced regulations forbidding the bringing and carrying away of data stores, and only 2.5% have implemented their enforcement. This also shows too little interest on the part of those responsible for information security in this topic.

Table 5. Respondents' Answers to the Question: Is There any Form of Control In Enterprises Over the Bringing and Taking of Portable Data Storage by Employees (SD card, PenDrive, USB drive, CD, DVD, BR)?

	2018/2019 research		2022 research	
	Number	Percentage	Number	Percentage
No	138	48,1%	117	40,8%
There are regulations prohibiting such practices, but direct control is not used	82	28,6%	96	33,4%
Yes	67	23,3%	74	25,8%

Source: Own elaboration

An analogous problem in terms of minimising the risk of information loss is the use of private computing devices by employees on the company's network. The currently popular BYOD phenomenon generates a number of problems in ensuring the security of intangible resources (Barlette et al., 2021; Zahadat et al., 2015). The most important of these is the blurring of the line between the use of a computer for professional and private purposes. From the point of view of information protection (problems analogous to the studies included in Table 5), this type of practice should be prohibited. However, many enterprises calculate the gains and losses of practicing this trend and allow the use of their own laptops, tablets and smartphones in daily work. In the 3-year period under review, the usage rate increased very significantly: from 59.9% all the way up to 91.6%. This is a result of the shift to remote working, where many employees performed their duties on private computer equipment. The very short period of assimilation into remote work meant that many businesses were not prepared for this. As a result, expressing consents to the use of private equipment was a natural consequence. The results are shown in Table 6.

Table 6. Respondents' Answers to the Question: Are Employees Allowed to use Private Computing Devices (Laptop, Tablet, Smartphone) in the Enterprise Network?

	2018/2019 research		2022 research	
	Number	Percentage	Number	Percentage
Yes	172	59,9%	263	91,6%
No	115	40,1%	24	8,4%

Source: Own elaboration

Enterprises that allow the use of private devices in the workplace should implement appropriate systems to monitor the behaviour of these computers on the enterprise's local network. This can significantly minimize the risk of information threats, and in selected cases eliminate them. The basic idea should be to establish a policy that provides for the use of private computers as data processing devices under certain conditions imposed by a properly configured system. At the same time, the possibility of storing any information or data in the memory of these devices should be prohibited. Thus, they should only provide an interface to work on information resources located on the enterprise's server or in the cloud computing (Irsheid et al., 2022). The actual position of economic entities on this issue is shown in Table 7.

Table 7: Measures to Monitor Employees' Private Computing Devices on the Company's Local Network

	2018/2019 research		2022 research	
	n=172		n=263	
	Number	Percentage	Number	Percentage
No need to monitor and authorise employee equipment	135	78,5%	83	31,6%
Devices are authorized in the network, but no one monitors the transmission of information	26	15,1%	166	63,1%
Each device is authorized and monitored against transmitted information	11	6,4%	14	5,3%

Source: Own elaboration

From the research results presented in Table 7, it can be observed that with the transition of economic entities to remote work, the need to authorize employees' devices on the enterprise's local network has increased significantly (Y. Sun et al., 2023). At the same time, it can be seen that the phenomenon of monitoring these devices has not changed (in fact, it has decreased somewhat). This is directly related to the question in Table 6 - in connection with the use of private devices by employees, they should be authorized on the network. However, there are no tools for monitoring private computers. Moreover, in many countries this would be a violation of the law.

A very important aspect in the protection of information is the organisation of work in places where customers and business partners are served. Currently, we can consider these issues on two levels:

- Protection of personal data (compliance with GDPR);
- Protection of business-critical information from accidental disclosure.

Both levels require adequate preparation on both theoretical (general set of rules, regulations) and practical (preparation of premises) grounds. These measures minimize the risk of information threats, reducing the human factor in such situations as the possibility of eavesdropping on employees' business conversations, the possibility of accidentally seeing documents placed on a desk or computer screen, and more direct ones, such as attempted theft. Table 8 shows the solutions to the aforementioned problem operating in enterprises.

The survey shows that 38.7% (2018-2019) and 36.2% (2022) of enterprises receive their customers in a dedicated room. This is a good result compared to other described measures to minimize the risk of information security breaches involving the human factor. Probably also caused by the fact that the requirements of the so-called "clean desk" and "clean monitor screen" appear in the GDPR regulation, which provides for high, financial criminal penalties for violations of personal data protection. However, as many as 49.9% (2018-2019) and 54.7% (2022) of enterprises still do not have practices to counter information security breaches.

Table 8: Places to Serve Customers and Business Partners In Enterprises

	2018/2019 research		2022 research	
	Number	Percentage	Number	Percentage
They are received in specially prepared rooms	111	38,7%	104	36,2%
They are received in one of the rooms in which employees carry out their daily work	117	40,8%	121	42,2%
Customers/business partners can move freely between rooms/departments of the enterprise	26	9,1%	36	12,5%
Due to the nature of the business operations, we do not personally receive customers and business partners at the premises of the company	33	11,5%	26	9,1%

Source: Own elaboration

Another aspect is the allocation of those information resources to employees that are necessary for them to perform their duties. Defining the rules for the use of software and hardware solutions makes it possible to significantly reduce the occurrence of potential risks and provides a set of basic guidelines related to information management in the company. However, additional attention should be paid to the extent and scope of access to information by those who manage it to any degree. The establishment of a resource entitlement policy is, in addition to the aforementioned principles, an elementary measure to prevent the loss or destruction of information. Assigning each employee a well-defined information area ensures that even in the case of deliberate, damaging actions by an employee, only selected intangible resources are at risk. Table 9 shows the results demonstrating the approach of economic entities in terms of entitlements.

It can be seen that during the pandemic period in which employees performed their duties through remote connections, the percentage of enterprises taking care of the proper allocation of resources for each employee increased (from 73.9% to 88.9%). In the case of small enterprises, one should additionally take into account the fact that in many of them there are no separate departments with specific responsibilities, and all "matters" concerning the entity's operation in the area of digital information are handled by one employee or the owner himself, for example. He then automatically has access to all intangible resources and there is no basis for applying any authority and these entities are included in the group represented by the results of 26.1% (2018-2019) and 11.1% (2022).

Table 9: Employees' Rights to Access Company Information Resources

	2018/2019 research		2022 research	
	Number	Percentage	Number	Percentage
Each employee has access to a specific information resource	212	73,9%	255	88,9%
Every employee has access to all information resources	75	26,1%	32	11,1%

Source: Own elaboration

The last issue discussed for the protection of information resources involving the human factor, perceived in the literature on the subject as one of the more effective, but at the same time controversial from the point of view of ethics, is monitoring. In light of modern technological developments, monitoring can cover virtually any aspect of human activity in the process of information processing. In general, regardless of the area in which it operates, it performs three basic security activities:

- preventive - by functioning in the consciousness of employees, it can minimize the number of mistakes made and reduce potential attempts to steal or destroy information;
- in the case of monitoring e-mails, telephone conversations, it can prevent potential intrusions into the network using social engineering activities;
- in a critical situation, after a threat has occurred, it allows to reconstruct to a certain extent the actions that led to the loss or destruction of information, and thus develop effective defence mechanisms for the future.

In the research conducted, an attempt was made to answer the questions: how many enterprises use monitoring techniques, and what areas they cover. The question was multiple-choice, so that respondents could mark any number of techniques used. The results are shown in Table 10. Direct interviews with respondents also show that each monitoring technique was implemented in accordance with the laws in force in Poland and each employee affected by the monitoring was informed about it. In special situations requiring additional authorizations, the appropriate consent was given by the employee.

In 2018-2019, the most popular technique was visual monitoring implemented through a system of video cameras installed in specific locations (25.1% of enterprises). In 2022, the most popular monitoring technique is already "software monitoring of activities performed on the computer" (up from 14.3% to 32.1%), and "control of e-mail correspondence" (up from 15.7% to 28.2%). As with the previous questions, the predominant focus during remote work is control of equipment or control of data managed by the employee. A direct surveillance system in the form of cameras is no longer relevant for obvious reasons.

Table 10: Monitoring Techniques Used in Companies (multiple choice)

	2018/2019 research		2022 research	
	Number	Percentage	Number	Percentage
Camera system	72	25,1%	69	24,0%
Control of e-mail correspondence	45	15,7%	81	28,2%
Software monitoring of activities performed on the computer	41	14,3%	92	32,1%
Print control	34	11,8%	38	13,2%
Recording of telephone conversations	11	3,8%	10	3,5%
Monitoring techniques are not used in the company	157	54,7%	93	32,4%

Source: Own elaboration

Computer monitoring is the most extensive and advanced technique (J. Sun, 2022). The number of activities that can be monitored is virtually unlimited. Advanced software solutions can nowadays monitor practically every mouse movement and record every key pressed on a computer keyboard. In the case of installed webcams, the system has the ability to record employee behaviour (similar to security systems installed in cars). The scope of monitored activities depends on the economic entity and possible arrangements with employees, whose opinion and possible objection according to the current law are not binding on the employer anyway (Kryczka, 2019; Ostrowski, 2014).

4. Conclusion

All the research results presented dealt with aspects of information security involving the human factor. Man, as the most important element of an information system, is at the same time its weakest link in the face of ensuring an adequate level of security.

The pandemic period, like no other period of information functioning as a strategic enterprise resource, has significantly contributed to the perception of information security from both technical and behavioural perspectives. The massive "migration" of employees from a desktop form of work to a remote form, carried out in record time, posed previously unknown challenges for business entities. One of them was to provide access to information resources from outside the company's premises in the most secure form possible. As the research presented here shows, the importance of the human factor as a catalyst for many potential risks was also realized on this occasion. The migration from a relatively secure information environment such as an enterprise's internal network to private environments, completely unknown by IT departments, meant that it was in the human (employee) that the greatest hopes were placed for the secure use of intangible resources of economic entities. The research presented here documents the fact that corporate information security decision-makers have changed their attitudes over the past 3 years in terms of behavioural perceptions of information security.

The research presented also confirms that turbulent periods (relevant to the operation of businesses) directly affect the perception and performance of certain management functions. One can also venture to say that the period of the contemporary armed conflict in Ukraine will also be significant for the perception of information security. Thus, further research can make a significant contribution to the picture of the contemporary field of information security management.

References

Barlette, Y., Jaouen, A., & Baillette, P. (2021) “Bring Your Own Device (BYOD) as reversed IT adoption: Insights into managers’ coping strategies” *International Journal of Information Management*, No. 56, 102212.

Benitez, J., Castillo, A., Ruiz, L., Luo, X. (Robert), & Prades, P. (2023) “How have firms transformed and executed IT-enabled remote work initiatives during the COVID-19 pandemic? Conceptualization and empirical evidence from Spain” *Information & Management*, No. 60(4), 103789.

Curry, S. J. J. (2013) *Chapter 41—Instant-Messaging Security,* in: W J. R. Vacca (Ed.), *Computer and Information Security Handbook (Second Edition),* Morgan Kaufmann, pp 721-735.

Gruber, J., Jóźwiak, I. J., & Merks, K. (2012) “Zagrożenia dla informacji udostępnianych na portalach społecznościowych” *Zeszyty Naukowe. Organizacja i Zarządzanie / Politechnika Śląska*, No. 63a, pp. 353–362.

Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021) “Human factor, a critical weak point in the information security of an organization’s Internet of things” *Heliyon*, No. 7(3), e06522.

Irsheid, A., Murad, A., AlNajdawi, M., & Qusef, A. (2022) “Information security risk management models for cloud hosted systems: A comparative study” *Procedia Computer Science*, No. 204, pp. 205–217.

Kobis P. (2021), *Information security management in information systems os small and medium-sized enterprises taking into account the human factor*, Towarzystwo Naukowe Organizacji i Kierownictwa. Stowarzyszenie Wyższej Użyteczności „Dom Organizatora”, Toruń, Poland.

Kryczka, S. (2019), “Służbowy komputer pod ścisłym nadzorem pracodawcy” *Rzeczpospolita*, [online] https://www.rp.pl/Kadry/307279990-Sluzbowy-komputer-pod-scislym-nadzorem-pracodawcy.html

Lin, C., Wittmer, J. L. S., & Luo, X. (Robert). (2022) “Cultivating proactive information security behavior and individual creativity: The role of human relations culture and IT use governance” *Information & Management*, No. 59(6), 103650.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014) “The Human Factor of Information Security: Unintentional Damage Perspective” *Procedia - Social and Behavioral Sciences*, No. 147, pp. 424–428.

Noga M, Brzezinski A., *Economics, Education and Youth Entrepreneurship.International Perspectives*, Routledge Taylor & Francis Group, London/New York 2022, pp. 5-29.

Ostrowski, W. (2014) “Granice dopuszczalnej kontroli pracowników” *Infor.Pl*, [online] https://kadry.infor.pl/kadry/indywidualne_prawo_pracy/odpowiedzialnosc_prawa_i_obowiazki/682749,Granice-dopuszczalnej-kontroli-pracownikow.html

Pabian A, Pabian A, Brzeziński A.(2020) “Young People Collecting Natural Souvenirs: A Perspective of Sustainability and Marketing” *Sustainability*, No. *12*(2).

Sedgwick, S. (2019) “The Human Factor of Cyber Security” *CSO from IDG*, [online] https://www.csoonline.com/article/3504813/the-human-factor-of-cyber-security.html

Shaikh, F. A., & Siponen, M. (2023) “Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity” *Computers & Security*, No. 124, 102974.

Sun, J. (2022) “Computer Network Security Technology and Prevention Strategy Analysis” *Procedia Computer Science*, No. 208, pp. 570–576.

Sun, Y., Jiang, W., Yang, Y., Zhu, H., & Jiang, Y. (2023) “Multi-domain authorization and decision-making method of access control in the edge environment” *Computer Networks*, No. 228, 109721.

Tayouri, D. (2015) “The Human Factor in the Social Media Security – Combining Education and Technology to Reduce Social Engineering Risks and Damages”, *Procedia Manufacturing*, No. 3, pp. 1096–1100.

Washo, A. H. (2021) “An interdisciplinary view of social engineering: A call to action for research” *Computers in Human Behavior Reports*, No. 4, 100126.

Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. A. (2015) “BYOD security engineering: A framework and its analysis” *Computers & Security*, No. 55, pp. 81–99.