O P E R A T I O N S  R E S E A R C H  A N D  D E C I S I O N S
No. 1 2021
DOI: 10.37190/ord210104

# HUMAN FACTOR ASPECTS IN INFORMATION SECURITY MANAGEMENT IN THE TRADITIONAL IT AND CLOUD COMPUTING MODELS

PAWEŁ KOBIS*

Faculty of Management, Czestochowa University of Technology,
ul. Armii Krajowej 19 B, 42-200 Częstochowa, Poland

This paper attempts to classify the main areas of threats occurring in enterprises in the information management processes. Particular attention was paid to the effect of the human factor which is present in virtually every area of information security management. The author specifies the threats due to the IT techniques and technologies used and the models of information systems present in business entities. The empirical part of the paper presents and describes the research conducted by the author on information security in business organisations using the traditional IT model and the cloud computing model. The results obtained for both IT models are compared.

**Keywords:** *information security, human factor, traditional IT model, cloud computing*

## 1. Introduction

Nowadays, information is one of the most valuable resources of the enterprise. Its quality, authenticity, topicality and uniqueness largely affect the position of a business entity in the market. It shapes the corporate image and allows for the appropriate response to changing external factors in the business environment and for quick adaptation to current conditions. It is a key element in the diversification of enterprises [23, p. 13].

Information resources in business organisations are defined by two elements such as exchange value, and operational value [7, p. 25]. The exchange value of information depends on its market value and it is measurable. A piece of information can be sold, bought, exchanged for specific resources, and a certain amount of money can be obtained for this information; in general, it has its price. The operational value of information is determined by its potential to generate possible benefits in the future. This does not necessarily have to be financial benefits. Denning [7, p. 25] gives an example of

*Corresponding author, email address: pawel.kobis@pcz.pl
*Received 5 January 2020, accepted 26 February 2021*

information that helps to locate the enemy army or information about treatment options. Both types of information allow obtaining the greatest benefits, i.e., saving human life.

Information protection is currently one of the main activities in modern enterprises. It focuses on the application of technical protection and elimination of the human factor. This paper is devoted to problems related to the impact of human behaviour on information security. With the characterisation of the currently used techniques, technologies, and IT models described in separate subsections, the author attempts to demonstrate the effect of the human factor on each of the mentioned elements of the functioning of modern information management systems.

The paper aims to outline the problem of the human factor in the aspect of information security in enterprises, to indicate major areas of risk, to point at the main factors characterising the deliberate and accidental behaviour of the employee and affecting information security, and to compare them with two current IT models: the traditional model, and cloud computing (CC) model. The human factor in the present paper is understood as a set of all human behaviours, both accidental ones, resulting from the lack of knowledge, experience, competencies, as well as deliberate ones, driven by their benefit. In the subject literature, one can find interesting and up-to-date research in the scope of cloud computing and traditional IT model security. However, it is quite rare that these models are directly compared in the discussed area. This paper is also supposed to trigger the interest of readers regarding this topic and is a sort of an invitation for further analyses and discussions.

## 2. Areas of threats to information security

Nowadays, information is considered an element of effective competitive advantage, both locally and globally. Acquiring valuable information that can be used to extend the knowledge in the business entity is a decisive factor in the implementation of tasks within the ongoing competition on the economic level of enterprises [18]. Therefore, this resource should be protected at every level of management [31, p. 18].

As a desirable intangible resource, information is exposed to various threats [3, p. 51]. They can be classified in different ways, depending on the concept of scientific investigations and the form in which information resources are stored [8, p. 50]. For this paper, the threats can be classified as follows:

1. Threats associated with the use of information technology and techniques.
2. Threats related to the IT model used in the business entity.
3. Threats caused by the human factor, directly related to deliberate and non-deliberate human actions, both in the area of techniques, technologies, and the IT model.

Modern information resources are mostly stored in digital form. A document is a sequence of bits with specific informational content [4, p. 3]. Therefore, new IT techniques and technologies are used to manage, process, and archive information. This results both from the possibilities offered by modern IT solutions such as analysis,

visualization, data archiving, and from the need to control the ever-increasing amount of information [5, p. 45]. In general, the techniques and technologies used in entities can be divided into two categories:

1. Used within the enterprise and local area network (LAN).
2. Used for information transmission in WAN and Internet networks.

The first one contains hardware and software solutions for storage, archiving and processing of information: advanced sector-based applications, ERP systems, CRM, intelligent systems for searching, and analysis of digital resources, etc.

The second concerns the transmission and processing of information outside the headquarters of the business entity. It includes hardware and software for sharing resources for remote work and storage media. It concerns virtual teams or information transfer between the enterprise's branches.

The threats resulting from sharing information on the Internet can be generally classified as follows:

- threats resulting from protecting the LAN network in the place of contact with the global network,
- threats resulting from the lack of encryption of transmitted information,
- threats resulting from the lack of adequate safety in devices receiving information transmitted over the Internet,
- threats resulting from intentional or unintentional human actions, termed human factor (e.g., lack of knowledge of procedures for safe remote work, making remote work equipment available to third parties, intentional actions in favour of competition, negligence).

These threats provide a general overview of the areas in which they may occur. With the development of the IT market, one can observe the emergence of newer and newer methods to take over or permanently damage information resources. New and unknown sub-areas are being formed, in which attention should be paid to the protection of intangible assets [27, p. 154; 28, p. 215]. The general global trend in the domain of information protection is shaped by the continuous "virtual struggle" of employees who develop security solutions with those who want to crack them. However, this rivalry mainly concerns technical protection. The problem of data protection resulting from human factor seems to remain unchanged in its general form [25, p. 8]. Solutions to this problem should be sought in non-technical areas.

## 3. Information security management model and IT infrastructure model in business entities

The perception of information security is also related to the IT model used by a specific business entity. Until the first decade of the 21st century, the main method to manage information in digital form was to create the enterprise's internal IT infrastructure,

which included all devices for storage, archiving and processing of digital resources, and application solutions consisting of the general part (e.g., operating systems, e-mail systems, office software) and the sector-related part (CAD, graphic, financial and accounting software). In the literature, this model is often referred to as the traditional model. Enterprises, especially larger ones, had (and many of them still have) their own IT departments, whose task was to manage their own IT facilities. The traditional model will probably be functioning in a large number of enterprises shortly. This results from the fact that a lot of enterprises own licenses for particular software, process sensitive data which they are afraid to move to the cloud or they are unable to do so due to legal reasons. Moreover, in several cases, investments in local IT infrastructures must return or amortise. It should be also considered that it is not very likely that all organisations will unanimously agree to use cloud solutions will implement them in their enterprises, abandoning the traditional model.

In the second decade of the 21st century, dynamic development of a new model of using IT resources, termed cloud computing, was observed. The model results from a synergy of development of several areas of IT and telecommunications:

- the methods, speed and quality of digital signal transmission,
- availability of broadband networks,
- network programming languages,
- IT equipment,
- methods to store large amounts of data,
- protection of data transmitted in public networks.

Cloud computing is based on the principle of 'borrowing' both server hardware and applications via the Internet. IT firms, both the largest in the world and smaller local providers, develop their colocation systems, IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service) [9, p. 67], and provide virtually any hardware and software solutions to businesses of any size in exchange for subscription fees. Business entities receiving these services do not, therefore, have to create their own full IT facilities, but only equip themselves with computer devices that are receivers (personal computers, laptops) with an operating system, a web browser, and a stable and efficient Internet connection [19, p. 2, 3]. Specific rented services can be scaled, changed, and further equipped at virtually any time and for any time. Upon cessation of business activity, it is sufficient to resign from the subscription [13, p. 215–217].

Depending on the applied model (IaaS, PaaS, SaaS) the scope of responsibility for security of information resources is changing, both on the side of the ordering party as well as a service provider (Fig. 1). Ensuring security (as a phenomenon) is divided between an entrepreneur and a cloud service provider. Enterprises that decide to place and process their information resources in the cloud should perform an analysis of potential scenarios, being an outcome of the undertaken IT infrastructure reorganisation. It should be analysed which data and information can be sent to the cloud and whether a legal

conflict about this type of decision (e.g., sensitive data) does not occur. There is a possibility to utilise the hybrid model, private, partner or dedicated cloud which, by definition, decreases the probability of a risk of losing information resources due to a threat occurrence. Migration of data and information to the cloud is not an antidote for threat occurrence, but it can minimise them to a certain extent, as some authors of papers about security in the cloud believe that few economic entities can afford such security measures as the ones owned by cloud providers (e.g., Amazon, Google or Microsoft).

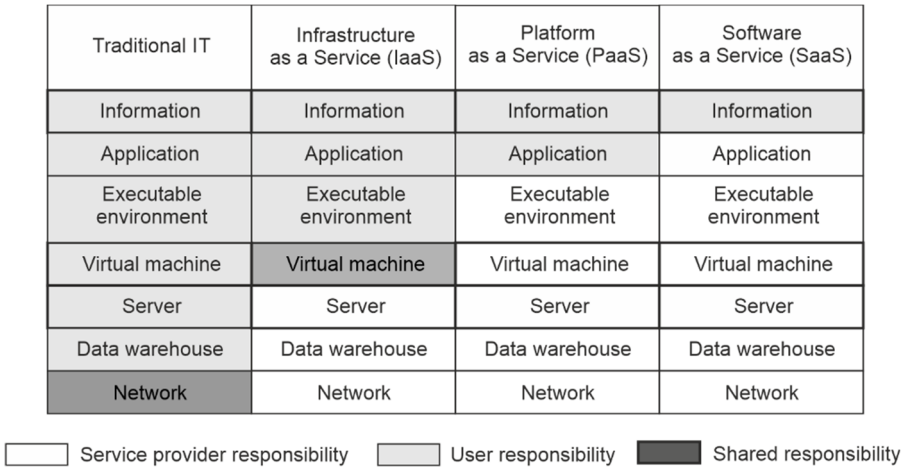


Fig. 1. Scope of responsibility for particular resources in the aspect of information security with a breakdown into IT models. Based on [18, p. 10]

The information security in each of the two IT models discussed so far concern security in terms of appropriate hardware and software protection. However, there is also the security, already mentioned in the previous subsection, related to the human factor. Is it different, depending on the IT model used? In both the first and the second model, people are responsible for security policy and the organisation of information management. It is only the set of tools that allows information processing changes. To partially answer this question, the author researched business entities using the traditional information management model and cloud computing model. The results are presented in the empirical part of the paper.

## 4. The human factor in information security processes in enterprises

The concept of the human factor in the literature on the subject appears in two approaches: a broad approach and a narrow approach. The broad approach covers both human resources and all the possible activities they are involved in within the enterprise. One of the most popular definitions describing the broad approach is developed by

Koźmiński and Jemielniak [15, p. 177]: human factor is *a fairly extensive group of concepts occurring in the theory and practice of management*. These include *concrete individuals and groups of people who fill the organizational structures and perform both duties and tasks arising from their roles in organizations and achieve their own personal goals and aspirations*. Similarly, in 2005, Lent [17, p. w-9] defines the concept of human factor broadly and argues that *human factor determines all the individuals participating in a project and the people around the project environment who are influenced by the project, with all their relations and interactions*.

The narrow approach, more common in English literature, defines the human factor as a set of human characteristics and behaviours that influence the way a given system operates or the behaviour of the environment (e.g., business organisation). It can, therefore, be assumed that this approach is a narrowed type of broad approach. One of the authors defining the narrow approach is Wang [30, p. 75], who emphasises that *Human factors are the roles and effects of human activity within the system, which introduce additional strengths, weaknesses and uncertainties.* The narrow approach provides a kind of foundation for perceiving the human factor as part of information security. Human, being the main component of both the information system and the IT system, by his or her actions that take into account strengths, weaknesses and uncertainties, contributes to the establishment of the level of security of managed resources.

The human factor aspect in information security has been also discussed for many years in popular scientific literature and all sector-related studies on information security. In many studies and reports on information security, it appears as the main cause of threats to information in business entities, based on the principle that the security system is as strong as its weakest link, i.e. human. For example, according to a report by KPMG International (one of the world's largest audit and consulting firms operating in 153 countries worldwide) published in April 2019 [16, p. 5], the human factor is the biggest challenge for companies (63%) in ensuring the expected level of safety. According to the companies surveyed, the reason for this status is the lack of adequately educated staff (61% of responses). In the same survey, respondents answered that they were most afraid of single hacker attacks (84% of indications), and as many as 54% of the companies surveyed were afraid of dissatisfied or bribed employees. The survey was conducted using the CATI method, among people responsible for IT security in companies with a sample of 100 organisations in February 2019 among small (14%), medium-sized (39%) and large (47%) enterprises. The survey was conducted by Norstat Polska.

The human factor is the main reason why so many attacks on information systems in companies are performed successfully [6, 26]. Many developers of viruses and malware use the human factor to infiltrate the company's information system. For example, they use false e-mails that are opened by computer users out of curiosity, recklessness and negligence. The process of opening an e-mail attachment initiates malware installation automatically. Another way is to add malware to one of the popular programs installed by users. In this way, the infected installation package is placed on the website,

waiting for the unaware user to download it and install his or her computer. The user's mistake, in this case, is that they download the software from unverified sources.

The main human mistakes that do not result from bribery on the part of competitors but affect information security include:

- excessive trust in global network contents,
- lack of developed self-control mechanisms when using electronic mail,
- lack of habit of systematic updating of operating systems and application software,
- using low-level security measures (weak passwords, failure to use authorisation levels for the access to data and information),
- using security software in free or insufficient versions to meet current needs (willingness to make savings on security software),
- connecting mobile devices to unsecured networks (hot spots in airports, restaurants, etc.),
- hiding mistakes concerning ensuring information security.

The mistakes made by employees result in an ever-increasing number of incidents affecting the security of corporate information resources. In 2017, Kaspersky Lab published the results of a survey of 5000 companies around the world, which found that [20]:

- 46% of incidents in 2016 were related to accidental breach of the security policy by employees,
- among business entities that fell victim to malware, 53% reported that the reason for the infection was a careless employee and as many as 36% of cases were due to social engineering manipulation of the employees,
- in 40% of the cases of security breaches, employees tried to conceal the incident, thereby exposing the business to even greater losses,
- nearly 50% of the respondents believed that employees in their company may inadvertently disclose corporate information using mobile devices while working.

Elimination of the impact of the human factor on information security is extremely difficult. It can be achieved only through periodic training of employees and understanding the motivation of their actions. One should ensure that employees are aware of the possible risks and tactics of the extraction and acquisition of information by potential competitors [24, p. 180]. The seriousness of this problem is evidenced by the fact that the number of human factor-related problems is not decreasing and has been at a similar level for many years among the factors causing information threats. Most modern hackers and malware developers rely on a statement made by one of the most famous computer hackers, Kevin Mitnick: *I cracked people, not passwords*.

Information processing is currently inseparably linked with the informatics system. Each system requires a particular, different manner of use which, in turn, generates particular behaviours of employees. The results of the research presented in the next chapter are supposed to lead the reader to the area where attempts are made to compare the

influence of the human factor in information security depending on the applied IT model in the enterprise.

## 5. Results of studies on potential incidents and human factors affecting information security

The survey was conducted in the period from January to March 2019 on a sample of 140 business entities belonging in general to the SME sector in Poland. Purposive sampling (arbitrary, non-random) was used to select the study group. The subjective selection of enterprises resulted from the specificity of the survey. This is because 70 enterprises using only the traditional IT model and 70 companies that used cloud computing solutions comprehensively or partially were selected. The survey was conducted using a questionnaire placed on a website (CAWI method: computer-assisted web interview). The questions were addressed to persons responsible for information protection in the enterprises surveyed or are directly responsible for data security. During the survey, they were asked to respond, taking into account the IT model functioning in their business entity. The answers presented in this chapter are part of those referring to the questions asked in the survey. The 2 presented questions include elements from both the area of general information processing in the enterprise, as well as the area purely referring to the human factor. In the survey, they were asked together and in an unchanged form presented in this chapter. All the questions were multiple-choice items. The choice of questions depended on the subject matter of this paper.

In this chapter, the author presents the results of the survey which demonstrate the differences in perceiving information security by enterprises depending on the IT model utilised by them. The author is aware of the fact that the indicated differences may also be implied by other factors (not only the IT model), therefore the present paper constitutes an introduction to further research in this domain. The results obtained do not unequivocally prejudge that the perception of security results exclusively from the application of traditional IT, cloud computing, or the combined model.

In the first question, presented in Fig. 2, the respondents were asked for opinions on the biggest risks of data loss in their enterprise from the point of view of human activity and work. This is related to the activities of employees responsible for creating a secure information management system architecture. This study aimed to identify risks with significant differences between individual IT models. The significant differences were defined as 10% or more. As a result of the received responses, these differences were noted in the following aspects:

1. Remote use of company information resources by employees working outside the enterprise's facilities.

2. Use of private mobile devices in the workplace.

3. The lack of top-down rules for access to information for individual groups of employees.

4. Lack of qualified specialist personnel for managing servers and IT security.

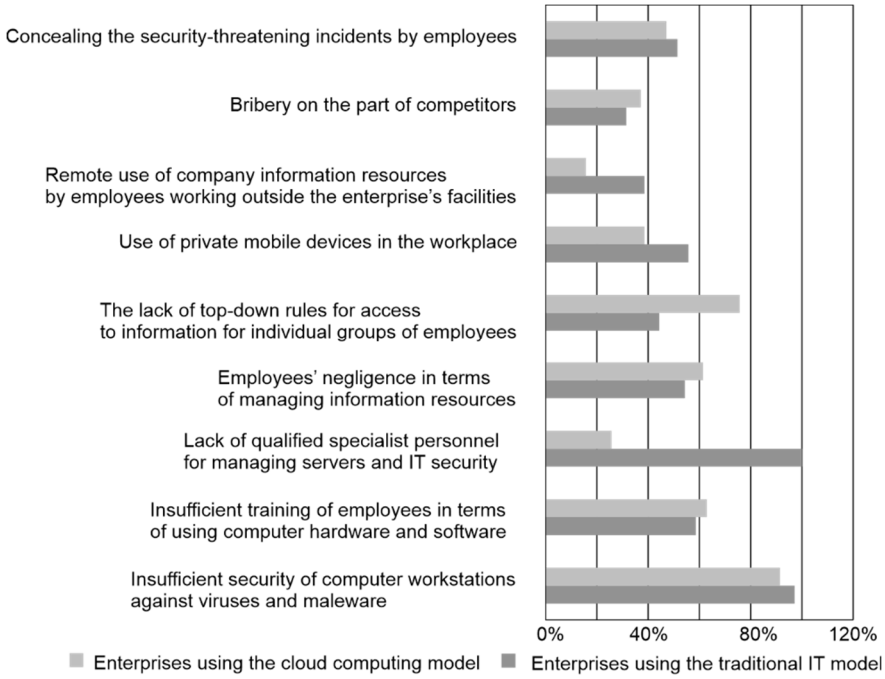


Fig. 2. The actions/negligences that represent the greatest risk of losing information in the enterprise

Differences in the answers should be analysed in two perspectives: technical organisation of information management which is the responsibility of the IT department and the manner of using IT resources by the employees themselves. From the technical perspective, there exists a division of responsibilities between the enterprise and cloud service provider (various depending on the type of cloud). We can say that in a way the IT department of the enterprise is relieved by the cloud provider and therefore particular responsibility for security relies on the cloud provider. In the case of using the cloud by the employees themselves, we can point to the way of using cloud applications and thus a possibility of making mistakes by employees or causing deliberate threats by them.

Differences in the results obtained for the first question can lie in the way in which remote resources are used in individual models. In the case of cloud computing, the remote use of information resources is somehow inherent in the specificity of the model operation [11, p. 17; 12, p. 164]. In a sense, the security of this information is the responsibility of the service provider, offering specific methods of authorisation. Regardless of the location of the employee (inside or outside the enterprise), the use is identical.

A change of location (taking into account similar network protection) should not affect information security. The indication of 16% for the cloud computing model may result from the fact that the respondents took into account unsecured networks, e.g., hot spots, home networks without passwords, etc. In the traditional model, the situation is slightly different. It is the entrepreneur who is responsible for the security of the resources made available to the outside, and he or she must ensure a permanent and secure connection to their servers. The human factor that occurs on the part of the IT staff of a business entity is quite critical in this case. Analysing, in turn, the human factor in the case of employees utilising the service, the fact of general accessibility of the service should be taken into consideration regardless of the localisation (especially in the case of the public cloud). There is a possibility that login data may be illegally taken over by third parties. Quick detection of this type of threat in the case of the cloud is difficult: usually logging into cloud resources is not monitored in enterprises. The situation looks different in the case of traditional IT – administrators identify, for example, IP numbers used to log into the system or time of logging in and can block an intruder anytime.

The difference in indications concerning the use of mobile devices can also be interpreted similarly. However, there is generally a higher percentage of indications here. This is probably since the question concerned private devices which are often out of the employer's control.

The third answer with a large difference in indications between the models concerned the principles of access to information. In this case, companies that use cloud computing expressed greater concerns about maintaining information security. The concerns probably arise from the fact that access to the information processed in the cloud computing takes place only (in most cases) after providing login and password and defining the editing rights. The entrepreneur does not have any control over the resources used, apart from the determination of the above data. The erroneous definition of access rights results in the uncontrolled processing of information by a specific person/employee. In the case of the traditional model, a properly configured IT system operates in a local network from which the activities of a user can be directly monitored. Although access rights must also be defined in this case, the opportunities for control are greater.

The biggest differences occurred in the last of the above-mentioned four risks. They result from the specificity of the operation of individual models. Enterprises that fully utilise the cloud computing model virtually do not need qualified personnel to operate servers, as these are located at the service provider's place. A large indication of 26% for CC may suggest that some of the entities surveyed are still using their servers and are concerned about problems contained in this question. It is worth noting, however, that in the traditional IT model, all enterprises pay attention to the risk emphasised in this part of the question.

The next question concerned the potential threats that respondents are afraid of in terms of loss of information (Table 1).

Table 1. Answers to the question: What potential threats do you consider to be the cause of a possible loss of information? [%]

| No. | Threat | Traditional IT | Cloud computing |
|---|---|---|---|
| 1 | careless and uninformed workers | 100 | 100 |
| 2 | the risk of losing a mobile device | 23 | 26 |
| 3 | social engineering aimed at workers | 30 | 37 |
| 4 | infecting information and data with malware | 100 | 37 |
| 5 | server computer failure | 59 | 27 |
| 6 | personal computer failure | 41 | 23 |
| 7 | failure of the information and data medium | 64 | 26 |
| 8 | hacking activities aimed at stealing information | 59 | 57 |
| 9 | purposive sharing of information by employees | 69 | 59 |
| 10 | no updated software versions (possible software gaps) | 46 | 10 |
| 11 | accidental deletion of a digital record | 24 | 27 |
| 12 | no backup of data and information | 56 | 17 |

The analysis of the answers reveals that the biggest differences in indications between respondents representing different IT models occurred in the following questions:

1. Infecting data and information with malware.
2. Server computer failure.
3. Personal computer failure.
4. Failure of the information and data medium.
5. No updated software versions (possible software gaps).
6. No backup of data and information.

How respondents answered all the above questions (from 1 to 6) is directly related to the principle of functioning of IT models. The answers allow the conclusion that, firstly, a significant percentage of the surveyed enterprises use the cloud computing model allowing for storing all data and information and, secondly, respondents have great confidence in the cloud computing model in terms of the security of their digital resources. The security of resources stored in the cloud does not depend on a hardware failure and lack of backup copies, and infecting data and information is unlikely due to security systems used in cloud computing. However, in the case of malware infections, the response rate of respondents using the cloud computing model was the highest.

The smallest percentage differences in responses concern the problems directly related to the human factor. Uninformed and careless employees may also contribute to the loss of intangible resources both in the traditional IT model and the cloud computing model.

## 6. Discussion

The research presented in the present paper was aimed to demonstrate the differences in the aspect of human factor occurrence as a threat to information resources in the process of information management in enterprises in the two presently functioning IT models: the traditional, and cloud. The results clearly show the differences in perceiving the models in the aspects of the necessity of ensuring the security of information on the side of IT departments. Cloud computing produces significantly less concern concerning software updates, potential data infections, computer hardware failures, and lack of backup copies of information and data. In the typical area of the human factor (regarding direct employees) the answers given by the respondents were similar (a few percentage points in favour of cloud computing): similar results were obtained for potential sociotechnical actions, deliberately taking data and information outside the organisation, lack of proper training for employees and bribing them, for example, by competitors. Similar values of answers may result from the fact that the respondents treat both deliberate as well as accidental actions of people with similar likelihood regardless of IT technologies functioning in enterprises. According to them, human actions are independent of the IT infrastructure and possibly result from the knowledge, experience, and competencies of employees. This is disputable as cloud solutions seem to be more susceptible to, for instance, social engineering techniques – it is enough to steal the login and password to the service or administrator's account [see 1, 2, 29]. This concerns equally the cloud users themselves, as well as technical personnel servicing the cloud.

The selected obtained research results, conducted among Polish enterprises to a certain extent are coherent with the results that can be observed in foreign research on cloud computing. For example, in the survey conducted by Ponemon Institute in 2017 [14] in the question: *Why is security in the cloud still difficult to attain?* as many as 71% of the surveyed replied that *it is more difficult to apply conventional information security in the cloud environment*, and 51% that *it is more difficult to control or limit access of end users*. These answers correlate to a certain extent with the result obtained in the research regarding the answer to the question: *The lack of top-down rules for access to information for individual groups of employees* in Fig. 2.

Similarly, with 50% of indications the respondents of the survey *IT Security Risk Report 2016* conducted by Kaspersky Lab [10] consider improper use of IT resources by employees to be a threat to information resources. The survey pertained to utilising information resources with mobile devices. The research conducted within the confines of the present paper indicated 39% for cloud computing and 56% for traditional IT.

Thus, there exist some similarities between the results obtained in the Polish entities and the results obtained in the foreign ones. However, the author believes that the obtained research results should largely be referred to the Polish conditions of enterprise

functioning. Other available researches indicate that the Polish IT managers find it difficult to assess the differences in the aspect of security breaches between traditional IT and cloud computing – contrary to their foreign counterparts. Sample research results are presented in Fig. 3. This is a summary of the results obtained by Computerworld in Poland and the results of the report *Cloud Security Spotlight Report 2017*.

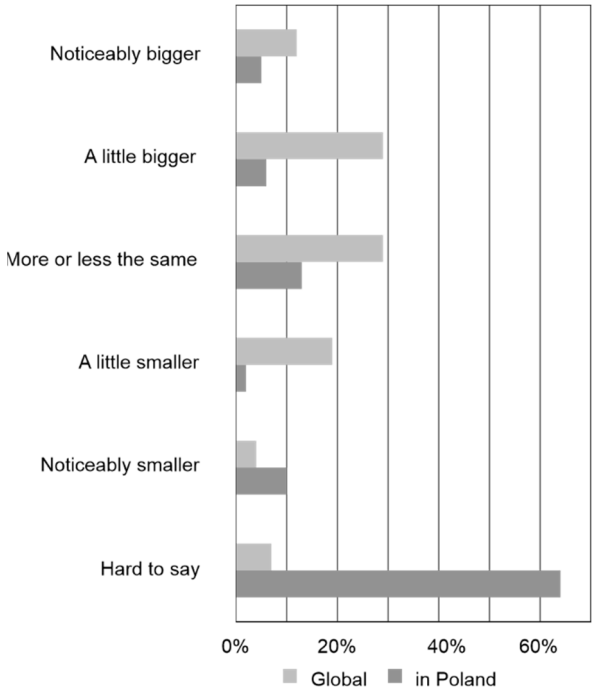


Fig. 3. Number of security breaches in a public cloud compared to traditional IT environments – respondent perspective. Source: [22]

The most significant point resulting from the research is that as many as 64% of the respondents indicated hard to say (vs. 7% of foreign respondents). Where do these disparities come from and do they indicate the lack of proper knowledge and experience? This might result from the commonly observed cautious attitude to cloud computing implementation. Separate research needs to be conducted to provide answers to these questions. Until the time of preparing the present paper, the author did not find any published scientific papers on this issue.

The impact of threats to information in cloud computing caused by the human factor may also result from the lack of proper competencies to this type of implementations in enterprises. According to the survey *Cloud competencies of companies in Poland 2020*, conducted by IDG on commission of Oktawave and 7bulls.com [21], it results that IT

managers most frequently evaluate the general level of cloud competencies of their employees as average (38%), and low (25% of indications). According to the same survey, in turn, only every fifth enterprise in Poland has a team ready to independently implement and run cloud projects.

## 7. Conclusion

In light of the theoretical considerations conducted in the study and the author's research presented here, it is possible to confirm the importance of the human factor in the processes of ensuring the security of information processing. All technical measures, both hardware and software, meet their requirements only if the persons supervising their operation and using computers can respond appropriately to the situation.

The presented research can be treated as an introduction to further analyses, more detailed ones, regarding the impact of the human factor on information resources depending on the IT model. Perhaps, the questions should be more detailed to highlight the respondents' ways of accessing information in each of the studied models. Moreover, it seems necessary to investigate the impact of the human factor on information security on the side of employees, technical departments of enterprises, as well as departments and teams servicing cloud computing. This will allow one to create a certain type of map presenting the threats from the human factor to information resources.

The Polish literature includes only a limited number of research that attempt to determine directly the differences in perceiving the security of traditional model and cloud computing. The author is aware that the presented research does not analyse thoroughly particular types of cloud, but in his opinion, it constitutes a basis for further, more detailed analyses.

### References

[1] ADAPTURE Technology Group, *The Reality of Cloud Security Issues: The Human Factor*, https://adapture.com/the-reality-of-cloud-security-issues-the-human-factor/ (04.12.2020).

[2] AHMED M., KAMBAM H.R., LIU Y., UDDIN M.N., *Impact of human factors in cloud data breach*, [In:] F. Xhafa, S. Patnaik, M. Tavana (Eds.), *Advances in intelligent systems and interactive applications*, IISA 2019, *Advances in Intelligent Systems and Computing*, Vol. 1084, Springer, Cham, 2020, 568–577.

[3] ALAVI R., ISLAM S., JAHANKHANI H., AL-NEMRAT A., *Analyzing human factors for an effective information security management system*, Int. J. Sec. Soft. Eng., 2013, 4 (1), 50–74.

[4] CELLARY W., *Information management instead of document management as a way for transforming public administration*, Elektron. Adm., 2007, 5, 2–7 (in Polish).

[5] CHOMIAK-ORSA I., MROZEK B., *Main perspectives of using big data in social media*, Inf. Ekon., 2017, 3 (45), 44–54 (in Polish).

[6] COLWILL C., *Human factors in information security: The insider threat – who can you trust these days?*, Inf. Sec. Techn. Rep., 2009, 14, 186–196.

[7] DENNING D.E.R., *Informatio075-076n warfare and security*, Wydawnictwa Naukowo-Techniczne, Warszawa 2002 (in Polish).
[8] GALANC T., KOLWZAN W., PIERONEK J., *Informatics systems of decision support and analysis of their security*, Oper. Res. Dec., 2016, 1, 45–53.
[9] IGNATOVA I., BIEHUN A., *Estimating the reliability of the elements of cloud services*, Oper. Res. Dec., 2017, 3, 65–80.
[10] Kaspersky Daily, *Business perception of IT security: In the face of an inevitable compromise*, website: https://usa.kaspersky.com/blog/security_risks_report_perception/, 2017 (01.12.2020).
[11] KIEŁTYKA L., KOBIS P., *Economic aspects of virtualization of IT resources in enterprises*, Przegl. Org., 2013, 4, 13–19 (in Polish).
[12] KOBIS P., *Employee mobility in light of cloud computing model*, *I. Humanistic aspects of knowledge and competencies management*, Przeds. Zarządz., 2016, 17 (7), 159–172.
[13] KOBIS P., *Nature of cloud computing as well as chances and threats associated with the application of cloud computing*, [In:] L. Kiełtyka (Ed.), *Information technologies in organisation functioning*, Stowarzyszenie Wyższej Użyteczności "Dom Organizatora", Toruń 2013, 213–222 (in Polish).
[14] KORZENIOWSKI P., *Human error still poses a significant cloud security risk*, TechTarget, website: https: //searchcloudcomputing.techtarget.com/tip/Human-error-still-poses-a-significant-cloud-security-risk, 2018 (07.12.2020).
[15] KOŹMIŃSKI A.K., JEMIELNIAK D., *Management from the beginning. Academic coursebook*, Wydawnictwa Akademickie i Profesjonalne, Warsaw 2008 (in Polish).
[16] KPMG, Report: *Cybersecurity barometer. In the defence against cyberattacks*, website: https:// assets.kpmg/content/dam/kpmg/pl/pdf/2019/04/pl-Raport-KPMG-Barometr-Cyberbezpieczenstwa -W-obronie-przed-cyberatakami.pdf, 2019 (25.08.2019) (in Polish).
[17] LENT B., *Managing processes of project management: Informatics and communication*, Difin, Warsaw 2005 (in Polish).
[18] ŁAPIŃSKI K., WYŻNIKIEWICZ B., *Report cloud computing: flexibility, efficiency, safety*, ThinkTank, Microsoft, BOOK Cloud Final Pol.pdf, Warsaw 2011 (in Polish).
[19] MALARA M., MALARA Z., *Methodical aspects of knowledge management in a contemporary company*, [In:] N.T. Nguyen, D.H. Hoang, T.-P. Hong, H. Pham, B. Trawiński (Eds.), *Intelligent information and database systems*, *Lecture Notes in Artificial Intelligence 10751*, *Subseries of Lecture Notes in Computer Science*, Springer, Dong Hoi City 2018, 71–81.
[20] MARINESCU D.C., *Cloud computing: Theory and practice*, Morgan Kaufmann Publishers, San Francisco 2017.
[21] PANKOV N., *The human factor: Can employees learn not to make mistakes?*, 2017, website: https: //www.kaspersky.com/blog/human-factor-weakest-link/17430/ (04.05.2019).
[22] PAWLAK M., *Companies in Poland lose out due to lack of cloud competence*, Oktawave, website: https://oktawave.com/pl/blog/firmy-w-polsce-traca-przez-brak-kompetencji-chmurowych, 2020 (06.12.2020) (in Polish).
[23] PIETUSZYŃSKI P., *Security of cloud environments according to IT managers*, Computerworld, website: https://www.computerworld.pl/news/Bezpieczenstwo-srodowisk-3.chmurowych-wedlug-menedzerow -IT,409536.html, 2017, (07.12.2020) (in Polish).
[24] PIPKIN D.L., *Information security: Protecting the global enterprise*, Prentice Hall PTR, Upper Saddle River, New Jersey 2000.
[25] ROZWADOWSKI M., *Economic counterintelligence as a modern method for protection of strategic information for a organization*, Securitologia, 2013, 1, 174–182 (in Polish).
[26] SAFIANU O., TWUM F., HAYFRON-ACQUAH J.B., *Information system security threats and vulnerabilities: Evaluating the human factor in data protection*, Int. J. Comp. Appl., 2016, 5, 8–14.

[27] SAPRONOV K., *The human factor and information security*, 2005, website: https://securelist.com/the-human-factor-and-information-security/36067/ (12.06.2019).
[28] SKOPIK F., SETTANNI G., FIEDLER R., *A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing*, Comp. Sec., 2016, 60, 154–176.
[29] SOOMRO Z.A., SHAH M.H., AHMED J., *Information security management needs more holistic approach: A literature review*, Int. J. Inf. Manage., 2016, 36 (2), 215–225.
[30] TABRIZCHI H., KUCHAKI RAFSANJANI M., *A survey on security challenges in cloud computing: Issues, threats, and solutions*, J. Supercomp., 2020, 76, 9493–9532.
[31] WANG Y., *On cognitive properties of human factors and error models in engineering and socialization*, Int. J. Cogn. Inf. Nat. Int., 2008, 2 (4), 70–84.
[32] ŻEBROWSKI A., *Information protection in enterprises in the conditions of globalisation: Selected problems*, [In:] R. Borowiecki, J. Czekaj (Eds.), *Information resources in limiting economic risk*, Stowarzyszenie Wyższej Użyteczności "Dom Organizatora", Toruń 2011, 13–40 (in Polish).