Measuring cyber security awareness within groups of medical professionals in Poland

Luiza Fabisiak
West Pomeranian University of Technology in Szczecin, Poland
lfabisiak@zut.edu.pl

Tomasz Hyla
West Pomeranian University of Technology in Szczecin, Poland
thyla@zut.edu.pl

Abstract

The goal of this study is to measure the cyber security awareness of medical professionals in Poland, i.e. to verify whether healthcare specialists have knowledge and understanding of basic cyber security threats. This survey was based on the cyber security recommendations from the European Union Agency for Network and Information Security and the U.S. Department of Health and Human Services. The survey consisted of 23 single and multiple-choice questions divided into four parts. The results categorized the respondents and measured the level of cyber security awareness. Among the 620 persons invited to participate in the survey, 300 (48.39%) responded and answered all of the questions. The results show a an unsatisfactory level of knowledge regarding information security in Poland. The main conclusion drawn from the survey is that the quality of cyber security training among medical professionals should be improved and frequency of the trainings should be increased.

1. Introduction

Electronic medical documentation is becoming increasingly popular. It has many advantages compared to paper-based documentation. Several information systems are used during the healthcare process, starting from a system for managing patient documentation (e.g. electronic health records (EHRs)) and organisational issues (e.g. patient admission) at healthcare sites, and ending at financial systems. All security systems depend on security measures. In addition, the proper management of a system, e.g. applying security updates, system configurations, and user training, has a heavy impact on system security. The users play a vital role in the security of eHealth systems. Improper user behaviours such as writing passwords on sticky notes, using the same USB drives in many different computers (e.g. at the hospital and at home), and downloading unsecured attachments from emails, create entry points for hackers who want to penetrate an eHealth system.

Cyberattacks on eHealth systems can have many different consequences impacting the basic security properties of medical records, i.e. availability, confidentiality, and integrity [1, 2]. For example, when patient data become unavailable (e.g. from numerous ransomware attacks on hospitals that delete or encrypt their medical data), the hospital can no longer provide healthcare services. In addition, patient-sensitive data might be disclosed, which has many negative consequences for patients and is a serious legal problem for healthcare sites. Finally, an undetected and unauthorised modification of medical records might lead to an incorrect treatment.

1.1. Motivation and contribution

The goal of this study was to verify whether healthcare specialists (e.g. physicians, nurses, and laboratory assistants) in Poland have sufficient knowledge regarding basic cybersecurity threats, particularly whether they are trained to fulfil all security requirements required by the General Data Protection Regulations (GDPR) [3], recommendations of the Health Care Information Systems Center [4], and Polish acts regulating patient rights and hospital operations. As the main contribution, results from a survey can be used to improve the application of cyber security training in Poland.

2. Background

2.1. e-Health systems

Electronic health record (EHR) systems are being developed in many different countries around the

URI: https://hdl.handle.net/10125/64215
978-0-9981331-3-3

world. The basic concept of EHR is that it is a virtual container for health-related documentations of a subject undergoing care (for a precise definition, see ISO 13606 [5]). Nation-wide EHR systems provide a single point of access to patient medical data. Apart from an EHR, several eHealth systems are usually deployed to facilitate the healthcare process, e.g. for telemedicine, drug detection, adverse interactions, decision-support systems, prescriptions, or sick leave certificate management.

The adoption rates of EHR systems vary around the world. In 2015, Chang and Rupta [6] reviewed the EHR adoption rate in Canada. They found that, depending on the region, between 40% and 75% of physicians are using an EHR system. In the European Union, some countries have a very high EHR adoption. However, we still see EU countries with a low EHR implementation. The problems with EHR adoption were fully discussed in [7]. The concerns of potential patients regarding the privacy and security of medical records in the United States were studied by Patel et al. [8], who found that most adults are confident in the privacy and security of their medical records. However, many have declared concerns regarding information sharing between different providers. A minority of consumers withhold information from their providers owing to privacy and security concerns.

In Poland, electronic medical documentation is commonly used in hospitals; however, such systems are usually local and are not interconnected. In 2018, the pilot implementation of nation-wide e-prescription systems commenced testing, which will continue until 2020 with the aim of transitioning to only e-prescriptions. It is worth mentioning that many physicians electronically issue prescriptions, which are stored in a local system, and the patients receive a printed version. Poland's EHR system, called the Electronic Platform for Collection, Analysis, and Provision of Digital Resources on Medical Events, should be operational in 2020.

2.2. Healthcare data security

In 2019, Jalali et al. [9] published the bibliometric analysis of the literature concerning cyber security in healthcare for the last 20 years. They analysed 472 English-language journal articles. More than half of the papers were related to the technological and management issues. The analysis' result shows that human and organizational aspects as well as physical security in healthcare might be understudied.

Medical data have a sensitive nature and should be protected using appropriate security measures. Many studies regarding security and privacy aspects in the field of eHealth have been published [10-12]. However, owing to the complex nature of eHealth systems, it is difficult to achieve a desirable security level in practice.

The most cited papers about technological aspects of cyber security concern security and privacy issues connected with: wireless body area networks [13], the framework for m-Health security [14], and the security architecture designed for providing authentication and authorization services in web-based distributed systems [15]. Moreover, aspects such as security of IoT devices [16] or new cryptographic schemes, e.g. [17], designed for healthcare systems are a common subject.

Cyber security in hospitals was studied from an organisational perspective by Jalali et al. [18] in 2018. One of their main findings is that reducing the end point complexity increases the security, mainly because the complex IT environment in a hospital is vulnerable for exploitation by cybercriminals. Their analysis shows that efforts to homogenise resource availability across hospitals reduce the probability of a cyberattack. In Europe, Landolt et al. [19] evaluated the current status of information security in Swiss hospitals. The results showed very low scores, particularly for basic security issues. Cyber security problems in healthcare in the US were summarised in 2017 by Health Care Industry Cybersecurity Task Force [20].

Luna et al. [21] analysed 19 articles and Kruse et al. [22] 31 articles concerning cyber threats in healthcare. The results of that studies show that healthcare industry lags behind in security and that current security systems in healthcare are insufficient in relation to capabilities of cyber criminals.

The European Union Agency for Network and Information Security (ENISA) published a study [23] in which they recognised security expertise and awareness as two of the most important cyber security challenges in eHealth. This is an important issue because minimising human errors, which can be a cause of successful cyberattacks, is crucial [24, 25]. The human factor in certain countries, e.g. Austria, is considered the most important cause of security failures [23].

The user plays an important role in cyber security. Because the training of an IT staff alone is insufficient, many cyber security threats are caused by human error or a lack of awareness [26]. Even in well-secured eHealth systems, user credentials can be compromised using social engineering techniques. Risk awareness is an important factor in a user's decision-making process when faced with cyber threats. User compliance regarding cyber security rules depends on the knowledge and understanding of

the rules [27]. Bellekens at el. [28] verified through a survey the user risk awareness with regard to connected eHealth wearables. The results indicate a low understanding of the threats related to connected wearables, and that a vast majority of users underestimate the risk encountered when using such devices. In addition, the participants were unaware of the consequences of certain threats.

2.3. Social engineering attacks

In recent years, hospitals have been the targets of many different types of cyber security attacks. One of the most common attacks is a ransomware attack, in which hackers try to encrypt a hospital database and obtain a ransom in exchange for a decryption key [29]. Sittig and Singh [30] proposed an eight-dimensional socio-technical approach for preventing or mitigating ransomware attacks. With this approach, they recommend health organisations to train users on ransomware prevention strategies, including how to identify malicious emails and avoid clicking on potentially weaponised attachments, and to train users not to use USB flash drives from untrusted sources. A similar recommendation comes from the U.S. Department of Health and Human Services [31], as summarised by Pope [32]. In addition to the above recommendations, it has been emphasised that users should never install or download software on their computers unless it comes from a verified source, and should understand what types of electronic information they are permitted to access.

Apart from ransomware threats, if a hacker obtains unauthorised access to patient medical data owing to an omission by a healthcare professional, the professional may suffer legal consequences. In addition, if a healthcare professional incorrectly verifies the authenticity of a false file with medical data created by an impostor, it may have a seriously negative effect on a patient's treatment, resulting in serious legal consequences for the healthcare professional.

3. Methods

The survey was created to test cyber security awareness in Poland. The survey, set up as a cross-sectional study, was conducted in the second half of 2017. This survey was based on the cyber security recommendations from the European Union Agency for Network and Information Security [23] and the U.S. Department of Health and Human Services [24]. Questions were chosen in such a way that they tested issues raised in these recommendations. As an additional requirement, the respondents must be able to answer all questions in less than 10 min, making it easier to obtain more responses from overworked medical professionals. The assumed time limit reduced the number of questions applied.

The survey consisted of 23 single and multiple-choice questions divided into four parts: the respondent's particulars (Information Part), electronic systems usage at a healthcare site (Part I), cyber security knowledge and skills (Part II), and basic cyberattack scenarios (Part III). The survey was anonymous and an electronic version was mainly used. The survey was sent to the contact addresses of healthcare sites along with a cover letter from the department at our university, which described the purpose of the survey. We received individual responses. A few hospitals contacted us to verify the origin of the survey as they thought it might be a part of cyberattack, which was a reaction that we expected.

The research was aimed at measuring the level of cyber security awareness of healthcare professionals in Polish hospitals. The results were collected to conduct a statistical analysis of the gathered data. A result was used, where the answers to unambiguous questions were rated on a point scale of zero or 1 (answer correct). For the multiple-choice questions, each correct answer was given 1 point. The result categorised the respondents and measured the level of cyber security awareness among the surveyed personnel. In addition, the SPSS program was used to analyse the collected factors. The program showed which independent results should be obtained for each question, as well as the results within the groups of respondents. Normalisation eliminated all components with a value of below 1.0, where a significance of $p<.05$ was assumed. No additional criteria for determining the optimal number of factors were examined because doing so was not the purpose of this particular study. Each respondent's influence on the level of cyber security awareness in their hospital was determined using the F-Snedecora test, and *p*- and *t*-tests. The differences among the questions examined were calculated based on the R^2 determination coefficient and the standard deviation (SD). The survey took into account the results, which allowed the resulting classifications of the examined groups (e.g. doctors, physiotherapists, and nurses) to be shown in terms of percentage. In addition, the confidence interval was measured for the groups of surveyed respondents, in which the average number of points from the questionnaire was obtained. The findings made it possible to analyse the main objective defined (proposed) in this document.

4. Results

Of the 620 people invited to participate in the survey, 300 (48.4%) responded and answered all of the questions. The remaining respondents, namely 320 (51.6%), resigned during the completion of the questionnaire. We suspect that that the relatively high resignation ratio comes from the fact that many of the respondents only opened the survey, looked at it, and decided to not fill it out. The questionnaire was also considered finished when the participants declared that they do not use electronic documentation in the workplace. The categories 'Invite', 'Dismissed', and 'Completed' in Table 1 indicate whether a page of the survey was visited. Questions from the initial information section were fully filled in, and for the last question, 'Do you use electronic health-related documentation in your work?' a negative answer ended the survey. According to this research approach, a group of 300 (48.39%) respondents was achieved. Only the 300 completed datasets were used for further analysis.

Table 1. Analysis of returned questionnaires

Characteristic	n (%)
Invite	
Doctors	420 (67.7)
Nurses and midwives	20 (3.2)
Physiotherapists	80 (12.9)
Laboratory assistants	20 (3.2)
Medical administrators	80 (12.9)
Dismissed	
Doctors	220 (68.8)
Nurses and midwives	5 (1.6)
Physiotherapists	29 (9.1)
Laboratory assistants	10 (3.1)
Medical administrators	56 (17.5)
Completed	
Doctors	200 (66.7)
Nurses and midwives	15 (5)
Physiotherapists	51 (17)
Laboratory assistants	10 (3.3)
Medical administrators	24 (8)

Out of the 620 respondents who completed the questionnaire, approximately 36,1% have worked for less than 5 years in the health care industry. The study investigated knowledge about cybersecurity of the whole medical group without division into professions.

Table 2. Ratio of correct answers in relation to the corresponding knowledge

	PART 1 Electronic system usage at a healthcare site	PART 2 Cyber security knowledge and skills	PART 3 Basic cyberattack scenarios
Doctors	45.2%	50%	37.5%
Nurses and midwives	45.3%	45.3%	33.3%
Physiotherapists	35.5%	48.2%	31.1%
Medical laboratory workers	43%	39%	44%
Medical administrators	42.5%	36.3%	34.5%

To determine the general knowledge regarding cyber security awareness in the hospitals in Poland, each answer within the group of respondents was calculated as independently to question in the survey. The percentages shown in Table 3 indicate the number of respondents with knowledge regarding cyber security in the medical field. Each correct response within the group of respondents was divided into three parts: electronic systems use at the healthcare site (Part I), cyber security knowledge and skills (Part II), and basic cyberattack scenarios (Part III). Based on the 300 (48.4%) respondents working in hospitals in Poland who completed the questionnaire, a factor analysis of the 23 questions contained in the questionnaire was conducted, as presented in the tables, and five questions were excluded (the first questions were concerning the information of the respondents themselves, and not their knowledge regarding cyber security).

The respondents who completed the questionnaire achieved total scores ranging from 33% to 50% out of a maximum score of 100%. These results for the three parts of the questionnaire are shown in Table 2, in which each individual result of the professional group (doctors, nurses and midwives, physiotherapists, medical laboratory workers, and medical administrators) was calculated as a percentage of the number of correct answers to the questions in the survey. These percentages are presented in Figure 1 as correct answers to questions from the questionnaire. In addition, the results in Figure 1 show the ratio of knowledge of the individual groups in relation to the individual parts contained in the survey.

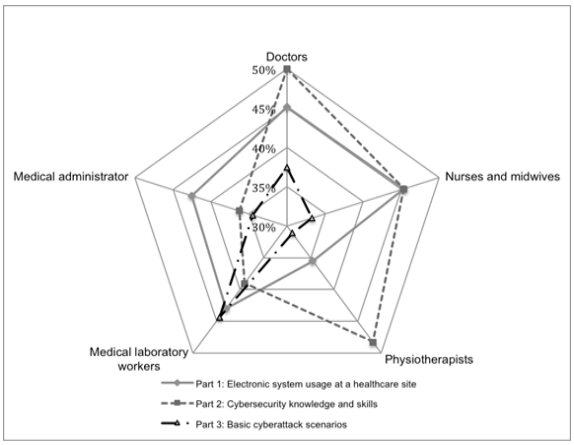

Figure 1. Evaluation of correct answers of healthcare professionals to questions on the survey

In the present study, the results of the correct answers were measured from the respondents based on the confidence intervals. This study included the maximum number of points from the completed questionnaire, which was 20 points. In the survey, the respondents answered 23 questions, five of which were excluded (the first questions concerned information on the respondents themselves, and not their knowledge regarding cyber security). The confidence interval included a correct answer rate of 95%, namely, the probability that the result of a correct answer outside this area would be less than $p< 0.05$. A 95% confidence interval for the standard normal distribution is thus the interval (11.74, 15.09) because 95% of the answers where applied. The confidence interval included 95% of the correct answers of the respondents. It should be noted that the maximum score from one questionnaire was 20 points out of 18 questions, pointing out that the two questions were multiple choice.

One of the most important data obtained from the survey is presented in Table 2. It needs to be underlined that Table 3 shows the ratio of all responses, each of the surveyed groups of respondents, and their correct answers to the questions. The average score shown in the table indicates the group of doctors who filled in 44.2% of the correct answers to the questionnaires. The worst answered the questions to medical administrators who responded to 37.8% of questions correctly. The results in Table 3 show the percentage of correct answers that can be classified into knowledge regarding the respondents' answers.

Table 3. Results of correct answers of respondents to questions measured in terms of percentage

		Doctors	Nurses and midwives	Physiotherapists	Medical laboratory workers	Medical administrators
PART 1 **Electronic system usage at a healthcare site:**						
1	Did you have cyber security training at work?	75%	66.7%	58.8%	80%	83.3%
3	Do you think that the electronic circulation of documents at your healthcare site is adequately protected?	55%	66.7%	17.7%	50%	25%
4	Do you use a mobile device (smartphone or tablet) to read electronic medical records?	55%	33.3%	21.6%	80%	0%
5	Can you copy medical records to a non-secured portable storage?	55%	66.7%	21.6%	100%	79.2%
6	The program for creating and processing electronic medical records does not allow granting physicians the rights to:	34.5%	20%	11.8%	0%	8.3%
7	When making an incorrect entry in the electronic medical records system, the entry…: (3 correct answers)	35%	66.7%	19.6%	0%	41.7%
		52,5%	33.3%	47.1	0%	25%
		5%	0%	1.9%	50%	16,7%
8	Does the electronic medical record system allow you to: (multiple choice, 2 correct answers)	70%	66.7%	100%	100%	100%
		70%	66.7%	68.6%	50%	41.7%
PART 2						

Cyber security knowledge and skills:						
1	Do you know the legal consequences related to the public disclosure of a patient's medical data?	95%	100%	90.2%	50%	100%
2	Can you securely send a patient's medical records by email?	50%	46.7%	39.2%	30%	41.7%
3	Are you aware of the existence of simple online tools that allow you to impersonate any email address?	50%	46.7%	25.5%	0%	0%
4	Can you electronically sign documents?	40%	0%	10%	0%	0%
5	Do you issue medical certificates in the form of digitally signed documents?	30%	66.7%	39.2%	50%	20.8%
6	What conditions must exist to consider e-documents secure?	65%	66.7%	78.4%	80%	50%
7	Does a pdf file containing the scan of a printed and signed document have more legal value than a pdf document without an electronic signature (in Poland)?	12.5%	0%	29.4%	0%	0%
8	Is the software on your computer continuously updated? (2 correct answers)	90%	26.7%	49%	80%	95.8%
		2.5%	33.3%	13.7%	20%	4.2%
PART 3 **Basic cyberattack scenarios:**						
1	If you find a pen drive in a cafe, will you connect it to your computer at work? ...: (2 correct answers)	75%	33.3%	29.4%	60%	16.7%
		20%	33.3%	29.4%	0%	83.3%
2	You received an email in your work inbox with information from the system administrator asking you to click on a link, log in, and confirm your password to conduct administrative tasks in the system. What will you do? ...: (3 correct answers)	20%	0%	29.41%	0%	20.8%
		15%	33.3%	29.4%	50%	20.8%
		40%	33.3%	0%	50%	41.7%
3	You received medical documentation (in the form of a.pdf file) as an email attachment regarding a patient from another specialist. Can you trust that the documentation received is authentic? How can you check it? (multiple choice, 2 correct answers)	42.5%	33.3%	49%	50%	0%
		50%	66.7%	50.9%	100%	58.3%

Table 4. Results of statistical analysis of the results obtained from the questionnaire (rotated component matrix)

		Mean	SD	SE	Pr>F	t	F	p	Correlation	R2
PART 1 **Electronic system usage at a healthcare site**										
1	Did you have cyber security training at work?	43.60	60.12	.151	6.37	0.008	40.59	.008	.965	.931
2	Do electronic systems at your healthcare site facilitate your work?	12.00	9.434	.485	1.12	0.346	1.25	.346	.542	.294
3	Do you think that the electronic circulation of documents at your healthcare site is adequately protected?	28.00	45.89	.238	3.83	0.031	14.64	.031	.911	.830
4	Do you use a mobile device (smartphone or tablet) to read electronic medical records?	8.00	12.57	.179	5.97	0.017	40.07	.017	.945	.894
5	Can you copy medical records to a non-secured portable storage?	8.00	9.08	.329	2.49	0,09	6.22	.088	.821	.675

6	The program used for creating and processing electronic medical records does not allow to grant physicians rights to…:	28.00	34.48	.221	10.27	0,15	28.96	.038	.513	0.838
7	When making an incorrect entry in the electronic medical records system, the entry…:	8.00	7.11	.473	1.208	0.34	1.58	.335	.556	.322
8	Does the electronic medical records system allow you to…: (4 answers)	48.00	54.61	.299	4.97	0.32	45.53	.322	.619	.607
PART 2 **Cyber security knowledge and skills**										
1	Do you know the legal consequences related to the public disclosure of patient's medical data?	56.00	76.42	.339	2.387	.097	5.69	.097	.809	.655
2	Can you securely send patient medical records by email?	28.00	40.74	.058	17.15	.000	294.08	.000	.995	.990
3	Are you aware of the existence of simple online tools that allow you to impersonate any email address?	24.00	42.83	.156	6.186	.009	38.26	.009	.963	.927
4	Can you electronically sign documents?	20.00	34.64	.090	10.94	.002	119.75	.002	.988	.976
5	Do you issue medical certificates in the form of digitally signed documents?	20.00	23.18	.107	9.21	.003	84.73	.003	.983	.966
6	What conditions must exist to consider e-documents secure?	40.00	51.98	.148	6.71	.008	46.33	.008	.965	.932
7	Does a.pdf file containing the scan of a printed and signed document have more legal value than a.pdf document without an electronic signature (in Poland)?	32.00	33.98	.124	7.89	.004	62.39	.004	.977	.954
8	Is the software on your computer continuously updated?	26.00	38.4	.431	1.79	.375	5.61	.375	.549	.380
PART 3 **Basic cyberattack scenarios:**										
1	If you find a pen drive in a cafe, will you connect it to your computer at work?	12.00	11.83	.426	1.69	.399	4.61	.399	.536	.397
2	You received an email in your work inbox with information from the system administrator asking you to click a link, log in, and confirm your password to deal with administrative tasks in the system. What will you do?	15.00	20.52	2.303	8.27	.137	120.97	.022	.941	.889
3	You receive medical documentation (in the form of a.pdf file) as an email attachment regarding a patient from another specialist. Can you trust that the documentation received is authentic? How can you check it?	29.00	33.38	.20	8.13	.008	73.93	.008	.968	.937

The next step in the research was a factor analysis; the 300 (48,39%) respondents who completed the questionnaire in hospitals in Poland are presented in Table 4. Each group was assigned several questions (Parts I and II), and a cyberattack scenario (Part III) was also applied. When the set of questions was divided into smaller parts, they pointed to stimulating factors. It should be noted that the table presents factors with the highest test variable and determination coefficient for each of the questions asked in the particular professional groups.

The zero hypothesis that the level of knowledge on cyber security with regard to medical care is high within all occupational groups might be rejected ($p< 0.05$) in accordance to the variability of the test (F-Snedecor). In the statistics on the probability distributions (F-Snedecor), if the values are less than $p<.05$, then the zero hypothesis is rejected, namely, there are significant differences. Table 4 shows that there was a significant difference in the distribution of Part I for questions 1, 3, 4, and 6. In Part II, we did not reject the hypothesis in only questions 1 and 8. In Part III, a significant difference in distribution occurred in questions 2 and 3, where we rejected the null hypothesis. Additionally, the determination coefficient, R^2, which is a measure of the quality of a model fit [0,1], was calculated. Table 4 shows a matching factor model, where the result is closer to 1, and is a good fit. It should be noted that there is a poor fit in questions 2 and 7 of Part I. In Parts II and III, the factor model is a good fit with a value of close to 1.

5. Discussion

In the course of the analysis, a comprehensive, effective, and fast method for verification cyber security awareness in institutions in Poland was introduced and successfully applied to 630 respondents. Less than half (48.39%) of all respondents answered all of the questions, however. Moreover, the analysis showed how important information security is and how to make medical professionals aware of the existence of cyberattacks. In addition, it should be emphasised that, in the case of basic security measures, respondents have a high level of knowledge, although this difference does not

reach a statistical significance when procedures related to securing medical records are consistently applied.

The results show that average percentage of correct answers is within the range of 36–50% depending on the group, which is significantly less than expected from a group of trained respondents. Additionally, Part III contained multiple-choice questions that were simple use cases reflecting the starting point of different cyberattacks. The average score was around 10% worse in Part III than in Part II. This shows that, even when the respondents have knowledge, using such knowledge in real world scenarios is much more difficult. There is also a significant difference in the results between the different groups of medical professionals. The medical administration staff group achieved the lowest average score, the reason for which probably results from the different ways the groups have been trained in the area of cyber security.

The overall results are rather unsatisfying, and they show that there is much to be done in terms of security training and that there is high potential risk of cyberattacks exploiting medical professionals instead of technical security measures. There have been few studies focusing on measuring how secure an eHealth system is in reality. The results of our survey are similar to those of the security levels found in Swiss hospitals [21]. Such results were measured from another perspective, i.e. by verifying how hospitals comply with the ISO/IEC 27002 standard; however, the results also indicate that the audited hospitals have a low level of security. Another recently published work by Jalali and Kaiser [19], who studied cyber security in hospitals using a series of interviews, shows that one of the reasons is the end point complexity of the systems applied. This might be the case in Poland where numerous different applications are used, making it more difficult to create training programs for medical professionals that will cover all possible scenarios.

An analysis of the results in the context of the digitisation process in the healthcare field in Poland leads to the following conclusions:

1. A lack of standardised applications and the distributed nature of medical records, with only a few central government applications, make it difficult to design short comprehensive cyber security training for all workers.

2. Many healthcare sites use out-dated software with implemented security measures that are currently not recommended, or use software that was designed for local application without proper security measures, and thus the users must be better trained.

3. Many medical professionals (particularly older ones) have a problem with using a computer. This is a common problem in Poland. This situation, in which they are largely computer illiterate, has made it more difficult to teach people about cyber security.

Cyber security training should be improved and applied more frequently; moreover, cyber security should be taught at the university level. Apart from standard recommendations that IT systems should be simple, easy to use, and configured in the way to minimise the possibility of user errors, healthcare organisation can improve cybersecurity awareness by improving the trainings by:

- including simple hands-on laboratories;
- including real time demonstrations of past cyberattacks carried out by cybersecurity professionals;
- including role playing activities that demonstrate persuasion techniques used by cyber criminals;
- establishing periodic (e.g., once a years) mandatory refreshing e-learning courses.

The cyber security awareness campaigns in general must take into consideration the factors that influence human behaviour [33]. Among others, trainings' solutions should be aligned with risks and designed to change people behaviour by providing simple consistent rules of behaviour that are easy to follow [34]. The Bada et al. [34] provide a good analysis of these factors and analyse a few general cyber security awareness campaigns. Moreover, the use of the various teaching methods allows people to better understand a given topic [35].

In comparison to the general public awareness campaigns, the healthcare professionals are subject to a greater number of risks. The consequences of unauthorized disclosure of medical documentation are serious. In European Union, GDPR strictly describes responsibilities of persons processing medical data. In Poland, unauthorised disclosure of medical data might result in a penalty, deprivation of liberty, imprisonment for up to 2 years or suspension of the professional licence. Additionally, the patient will be able to claim compensation before a court.

Another result of the present study shows, above all, the lack of appropriate tools for a fast and inexpensive assessment regarding cyber security awareness in a large number of hospitals. These results indicate that one can quickly and safely check the awareness of individuals regarding the risks associated with cyberattacks. The main difficulty is to find a large number of respondents. Such surveys are perceived by many persons from management as a part of a cyberattack itself (which is the correct

attitude toward surveys in which the source is unknown). Therefore, some type of official authorisation of the survey is required, which slows down the process.

Frequent audits of user cyber security awareness will become increasingly important because large numbers of hospitals need to address information security issues in their healthcare systems. The security of information processing in hospitals, such prevention the manipulation (deliberate or intentional) of data, is critical to a patient's health. In addition, patient health data are protected by law, and all data must be stored, transferred, and processed in a secure manner ensuring confidentiality and integrity.

6. Conclusion

This paper presented the results from a survey measuring cyber security awareness. The results show a rather low level of knowledge regarding information security. This might be caused by the fact that many aspects of cyber security are difficult to learn during a few days of training. In addition, several cyber security threats are abstract for people without in-depth computer knowledge. Hence, they sometimes have difficulties in understanding the consequences of the threats, and therefore underestimate how much negatively they can influence the healthcare process. Effective teaching of new skills can lead to the prevention of risky behaviours in the selected environment, as lack of motivation is sometimes a real lack of skills [36].

This study indicates an urgent need to take action and improve the security of information in hospitals by raising the awareness of healthcare professionals regarding cyber threats. This should be done mainly by improving the quality of cyber security training among medical professionals and increasing their frequency.

Future work will include building an IT system allowing surveys to be conducted, which will give respondents a guarantee that the results remain anonymous (in the present survey we did not collect any data on the responders, which was guaranteed based on our declaration). We suspect that such a system might result in a higher ratio of respondents who complete the survey. In addition, we are planning to create a larger pool of questions that can be used interchangeably, and thus we will become more confident that the medical professionals do not obtain answers from their colleagues. The main reason for developing such a system is that, without a proper tool to measure cyber security awareness, it will be difficult to monitor how such awareness changes.

7. References

[1] M. Nieles, K. Dempsey, V.Y. Pillitteri, "An Introduction to Information Security", NIST Special Publication 800-12 Revision 1, June 2017.

[2] D.B. Parker, "Toward a New Framework for Information Security?", Computer Security Handbook (eds S. Bosworth, M. E. Kabay and E. Whyne), 2015.

[3] European Parliament and Council of the European Union, Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), L119, 4 May 2016;1–88, http://data.europa.eu/eli/reg/2016/679/oj;

[4] Polish Health Care Information Systems Center, "Recommendations of the Health Care Information Systems Center in the field of security and technological solutions used during processing of medical records in electronic form" (in Polish), Warsaw, 2017, https://www.csioz.gov.pl/fileadmin/user_upload/rekomendacje_csioz_bezpieczenstwo_wrzesien2017_59cd1e951e9ba.pdf.

[5] ISO, ISO 13606-1:2008 Health informatics - Electronic health record communication - Part 1: Reference model. ISO/TC 215; Health informatics: Stage 90.92, 2012.

[6] F. Chang, N. Gupta, "Progress in electronic medical record adoption in Canada", Can Fam Physician, vol. 61(12), 2015, pp. 1076-84.

[7] D. F Sittig, H. Singh, "A Socio-Technical Approach to Preventing, Mitigating and Recovering from Ransomware Attack." Appl Clin Inform, vol. 7(2), 2016, pp. 624–632.

[8] J. King, V. Patel, E.W. Jamoom, M.F., Furukawa, "Clinical Benefits of Electronic Health Record Use: National Findings", 2014, Health Serv Res, vol. 49, pp. 392-404.

[9] M. S Jalali, S, Razak, W. Gordon, E. Perakslis, S. Madnick, "Health Care and Cybersecurity: Bibliometric Analysis of the Literature", J Med Internet Res, 2019, vol. 21(2):e12644.

[10] J.J. Rodrigues, I. de la Torre, G. Fernández, M. López-Coronado, "Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems", J Med Internet Res, vol. 15(8):e186, 2013.

[11] M.A. de Carvalho Junior, C.L. Feijó Ortolani, I. Torres Pisa, "Health Information System (HIS) security standards and guidelines history and content analysis". J. Health Inform, 2016, vol. 8(3), pp. 95-102.

[12] F. Rezaeibagha, Y. Mu, F. Susilo, K.T. Win, “Multi-authority security framework for scalable EHR systems”, International Journal of Medical Engineering and Informatics, 2016, vol. 8(4), pp. 390–408.

[13] M. Li, W. Lou, K. Ren, "Data security and privacy in wireless body area networks," in IEEE Wireless Communications, vol. 17(1), 2010, pp. 51-58.

[14] R. Lu, X. Lin, X. Shen, "SPOC: A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency," IEEE Transactions on Parallel and Distributed Systems, 2013, vol. 24(3), pp. 614-624.

[15] D. Gritzalis, C. Lambrinoudakis, “A security architecture for interconnecting health information systems”, 2004, International Journal of Medical Informatics, vol. 73(3), pp. 305-309.

[16] A. Strielkina, D. Uzun, V. Kharchenko, "Modelling of healthcare IoT using the queueing theory," 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Bucharest, 2017, pp. 849-852.

[17] C. C. Tan, H. Wang, S. Zhongm Q. Li, "IBE-Lite: A Lightweight Identity-Based Cryptography for Body Sensor Networks," IEEE Transactions on Information Technology in Biomedicine, 2009, vol. 13(6), pp. 926-932.

[18] M. S. Jalali, J. P. Kaiser, “Cybersecurity in Hospitals: A Systematic, Organizational Perspective”, Journal of Medical Internet Research, 2018, vol. 20(5): e10059.

[19] S. Landolt, J. Hirschel, T. Schlienger, W. Businger, A.M Zbinden, “Assessing and Comparing Information Security in Swiss Hospitals”, Interactive Journal of Medical Research, 2012, vol. 1(2):e11.

[20] Health Care Industry Cybersecurity Task Force: Report on improving cybersecurity in the health care industry, 2017, https://www.phe.gov/Preparedness/ planning/CyberTF/Documents/report2017.pdf

[21] R. Luna, E. Rhine, M. Mythra, R. Sulivan, C.S. Kruse, “Cyber threats to health information systems: A systematic review.”, Technol Health Care, 2016, vol. 24(1), pp. 1-9.

[22] C. S. Kruse, B. Frederick, T. Jacobson, D. K. Monticone, “Cybersecurity in healthcare: A systematic review of modern threats and trends, Technology and Health Care”, 2017, vol. 25(1), pp. 1-10.

[23] D. Liveri, A. Sarri, C. Skouloudi, “Security and Resilience in eHealth Infrastructures and Services”, ENISA Report, ISBN 978-92-9204-137-3, December 2015.

[24] J. Rajamäki, R. Pirinen, “Towards the cyber security paradigm of ehealth: Resilience and design aspects”, AIP Conference Proceedings, 2017, vol. 1836(1), pp. 20-29.

[25] J. Winnefeld, C. Kirchhoff, D. Upton, “Cybersecurity’s Human Factor: Lessons from the Pentagon”, Harvard Business Review, September 2015, https://hbr.org/2015/09/ cybersecuritys-human-factor-lessons-from-the-pentagon.

[26] J. Rajamäki, J. Nevmerzhitskaya, C. Virág, “Cybersecurity education and training in hospitals: Proactive resilience educational framework (Prosilience EF)", IEEE Global Engineering Education Conference (EDUCON), Tenerife, 2018, pp. 2042-2046.

[27] M. Evangelopoulou, C.W. Johnson, “Attack Visualisation for Cyber-Security Situation Awareness”, 9th IET International Conference on System Safety and Cyber Security 2014 Oct. 15-16, Manchester, UK, pp. 1-6.

[28] X. Bellekens, A. Hamilton, P. Seeam, K. Nieradzinska, Q. Franssen and A. Seeam, "Pervasive eHealth services a security and privacy risk awareness survey," 2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA), London, 2016, pp. 1-4.

[29] M. Duggan, “The legal corner (TLC): Ransomware attacks against health care IT”, Journal of Informatics Nursing, 2017, vol. 2(4), pp. 30-31.

[30] F.D. Sittig. H. Singh, “A Socio-Technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attack”, Appl Clin Inform., 2016, vol. 7(2), pp. 624–632.

[31] U.S. Department of Health and Human Services, Fact sheet: ransomware and HIPAA, 2018, https://www.hhs.gov /sites/default/files/RansomwareFactSheet.pdf.

[32] J. Pope, “Ransomware: Minimizing the Risks”, Innov Clin Neurosci, 2016, vol. 13(11-12), pp. 37–40.

[33] P. Dolan, M. Hallsworth, D. Halpern, D. King, I. Vlaev, “MINDSPACE Influencing behaviour through public policy”, Institute for Government, Cabinet Office, 2010. http://www.instituteforgovernment.org.uk/sites/ default/files/publications/MINDSPACE.pdf

[34] M. Bada, A.M. Sasse, J. R.C. Nurse, “Cyber Security Awareness Campaigns: Why do they fail to change behaviour?”, International Conference on Cyber Security for Sustainable Society, 2015, http://arxiv.org/abs/1901.0267

[35] J. Abawajy, “User preference of cyber security awareness delivery methods”, Behaviour & Information Technology, vol. 33(3), 2014, pp. 237-248.

[36] I. Winkler, “7 elements of a successful security awareness program”, 2017, https://www.csoonline.com /article/2133408/network-security-the-7-elements-of-a-successful-security-awareness-program.html [online: 29.08.2019].