Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 181 (2021) 173–181

Procedia Computer Science

www.elsevier.com/locate/procedia

CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies 2020

Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions

Paulo Nunes[1], Mário Antunes[2,3*], Carina Silva[1,4]

[1]*Lisbon School of Health Technology, Polytechnic Institute of Lisbon, Portugal*
[2] *Polytechnic of Leiria, School of Technology and Management and CIIC, Leiria, Portugal*
[3] *Center for Research in Advanced Computing Systems, INESC-TEC, University of Porto, Portugal*
[4] *Centro de Estatística e Aplicações – Universidade de Lisboa, Portugal*
6490@alunos.estesl.ipl.pt, mario.antunes@ipleiria.pt, carina.silva@estesl.ipl.pt

Abstract

The growing digitization of healthcare institutions and its increasing dependence on Internet infrastructure has boosted the concerns related to data privacy and confidentiality. These institutions have been challenged with specific issues, namely the sensitivity of data, the specificity of networked equipment, the heterogeneity of healthcare professionals (nurses, doctors, administrative staff and other) and the IT skills they have.

In this paper we present the results obtained with a study made with healthcare professionals on evaluating their awareness level with the information security, namely by assessing their attitudes and behaviours in cybersecurity.

The methodology consisted in translating, adjusting and applying two previously validated and already published Likert-type response scales, in a healthcare institution in Portugal, namely "Centro Hospitalar Barreiro Montijo" (CHBM). The scales used were cybersecurity risky behaviour (RScB) and cybersecurity and cybercrime in business attitudes (ATC-IB).

Although there were no significant statistical differences between the sociodemographic factors and the scores obtained on both scales, the results showed a relationship between acquired behaviours and the attitudes of involvement with work and organizational commitment, establishing a bridge for the quantification in awareness.

* Corresponding author. Tel.: +0-000-000-0000 ; fax: +0-000-000-0000 .
E-mail address: mario.antunes@ipleiria.pt

1877-0509
10.1016/j.procs.2021.01.118

Keywords: Cybersecurity; Cyber-awareness; Behaviours, Attitudes, Cyber-hygiene, Health Information Systems.

1. Introduction

Information Technology (IT) has evolved rapidly in recent decades. Digital transformation of health institutions has leveraged new opportunities for quality development, but at the same time challenged healthcare institutions to deal with electronic patient records, records of diseases, family history data and other patients' sensitive data.

Cybersecurity awareness among health professionals is worth studying as they have to process sensitive data and, in most of the cases, don't have technical IT skills to do it accurately and applying the best practices in applications security. In fact, healthcare professionals have to be fully committed with their primordial mission, that is to treat patients. IT skills and information security best practices are not in their major concerns.

The development of new social models of relationship between patient and healthcare professional, based on trust, brings to front line new behaviors and attitudes regarding the understanding of the reality of individual and collective health. That is, medical data and information gives confidence to the health professionals and, at the same time, the patient is increasingly informed and aware of his medical condition.

This new way of looking at health brings growing concerns about information security and the application of new digital tools in health for professionals and citizens, as they will, in this new paradigm, control their own health data and may question the medical authority. The increasing information produced can be easily shared and delivered online to the general public, which includes health professionals.

Until 2016, cybersecurity was something on hold in the healthcare organizations [1], apart from the little investment in security measures, understandable in part by the nature of the services provided [2,3,4]. However, recently we have faced several cyberattacks against hospitals, as well as loss of reputation and sensitive information leakage, namely the WannaCry ransomware attack that took place on May 2017, which managed to infect more than 200.000 systems in 150 countries [5].

Despite the growing on cybersecurity awareness, there are few empirical studies to assess and measure individual user differences in information security within healthcare institutions that determine the existence of an unintentional internal threat [6]. In the context of Information Security, it is understood that *attitudes* are the psychological side of *behavior*, its perceptions, expectations and knowledge. Together, they may influence the assessment of something made by someone. Overall, evaluation can lead to behavior, thought or feelings. Through thoughts and feelings, we can realize behaviors, and through behaviors we can deduce attitudes, establishing a relationship between impulsiveness and information security [6,7,8].

It is important to understand that the risks associated with cybersecurity can be managed and mitigated, but not eliminated. The scale and complexity associated with cybersecurity is of major extent, leading organizations to constantly adapt to maintain the resilience of systems against continuous and dynamic threats. Risk analysis in cybersecurity should therefore be a continuous and iterative cycle advocated by key stakeholders, led by a team of skilled information security professionals and evangelized by all staff with good cybersecurity practices [9].

Healthcare professionals are trained and qualified to perform healthcare, often subject to high levels of stress due to overload of work and responsibilities. On a daily routine they work as a team, cooperate within the organizational hierarchy and there is a natural tendency to trust those around them, as their common focus is health care. For instance, sharing (easy guess) password and having one desktop computer for a team are usual practices in the hospitals.

Although aware of good practices in cybersecurity, the hospitals administrations have relegated them to background, making professionals' behaviors and attitudes of the greatest vulnerability in terms of information security. From another perspective, and given the stressful nature of their professions, health care professionals may be more vulnerable to social engineering [4].

This paper aims to target research into health cybersecurity awareness and cyber hygiene needs in a hospital environment. The research intends to identify key risky cybersecurity attitudes and behaviors in healthcare institutions

and in their health practitioners. The study that was carried on used two distinct scales (attitudes and behaviors) in order to measure a kind of "human vulnerability risk index" among the healthcare professionals. The methodology used was based on two internationally validated and published metric assessment questionnaires that was translated to Portuguese language and adapted to be applied in healthcare institutions, to measure the cybersecurity risky behaviors of health professionals and their attitudes towards cybersecurity. The paper is organized as follow. In Section 2 we summarize the literature review around the main scales used to measure the cybersecurity risk and attitudes. Section 3 depicts the methodology adopted in the research. In Section 4 we describe the results obtained and present a comprehensive results analysis. Finally, in Section 5 we present the major conclusions and a set of future works that can be further developed.

2. Literature review

Security breaches are common in organizations and are widely assigned to human error and misusage. There is a need to increase awareness of information security within organizations and their employees, as well as to promote their ability to engage in unsafe cybersecurity behavior. Factors such as gender and age can affect different behavior in cybersecurity [6]. Scales have thus been defined to measure the risky attitudes and behaviors regarding information security in an organization. The most relevant, including those used in this research, as described below.

The Human Aspects of Information Security Questionnaire (HAIS-Q), developed by Parsons et al [10], uses a scale composed of 63 items, divided into three separated sub-areas that measure knowledge, attitudes and behaviors. This questionnaire intends to evaluate and understand the levels of information security awareness in an organization.

Serge Egelman and Eyal Peer develop the Security Behavior Intentions Scale (SeBIS). It comprises 16 items and includes four sub-scales addressing attitudes toward password design and applicability, digital device protection, proactive engagement and recognition, and finally software update [8].

Ögütçü et al developed a metric to correlate cybersecurity behaviors with different levels of conscientiousness. The metric was obtained by four distinct scales: Risky Behavior Scale (RBS), Conservative Behavior Scale (CBS), Exposure to Offence Scale (EOS) and Risk Perception Scale (RPS) [13].

The motivation for the study developed by Lee Hadlington was the lack of studies or measures covering the influence of human factors on accidental or opportunistic insider attacks within the organizations [11]. Initially Hadlington dealt with the characterization and exploitation of the key human factors that can contribute to an individual may become a threat, developing a set of key frameworks designed to mitigate such threats. Further research was on the development of an exploratory study about the relationship between risky behavior in cybersecurity, attitudes towards cybersecurity in a business environment, Internet dependence and impulsiveness. In this study Hadlington presented the following scales: Abbreviated impulsiveness scale (ABIS), Online cognition scale (OCS), Risky cybersecurity behaviors scale (RScB) and Attitudes towards cybersecurity and cybercrime in business (ATC-IB) [11].

Aivazpour *et al.* [12] replicated Hadlington's work and concluded that his research, together with Egelman's research [8], could provide a good starting point for the study of impulsiveness in risky cybersecurity behaviors. The need to develop RScB and ATC-IB scales, mentioned in Aivazpour's conclusions, pushed Hadlington towards an improvement by initiating a study to explore whether company size, age or attitudes influence employees' relationships with risky cybersecurity behaviors and general awareness of cybercrime.

In this paper we have translated RScB and ATC-IB scales to Portuguese and have further adapted them to be applied in healthcare institutions, as these scales were originally defined in English language and for business companies, which have different aims and goals. In Section 3 we detail the methodology adopted to assess the scales in our case studies.

3. Methodology

Our research was based on the use of two Likert type scales, namely RScB and ATC-IB. The research is observational, quantitative, cross-sectional and descriptive, related to attitudes and behaviors in cybersecurity, in a healthcare institution environment. The metrics obtained by the two scales are compared with the socio-demographic

factors and the professional group, namely age groups, professional classes and gender. The participation was made by filling a questionnaire and it was available to all healthcare practitioners with age between 18 and 69 years old.

RScB scale is partly based on the SeBIS scale developed by Egelman *et al*. [8]. It assesses behaviors that may induce poor cybersecurity practices and that may reflect human vulnerability for businesses and, in particular, healthcare institutions. The RScB scale has a score ranging from 0 to 120 points, with higher values being indicators of riskier behaviors generally associated with low levels of cybersecurity awareness [6]. This scale is composed by twenty Likert items of seven levels, scored from 0 to 6 points (0 = Never to 6 = Daily), where participants are asked to rate their cybersecurity behaviors retrospectively over the past six months. The scale presents items with inverse scores on questions 11 and 18.

The ATC-IB is also a Likert type scale that varies between 25 and 100 points, with higher scores being synonymous of positive engagement in cybersecurity while a strong security awareness and lower score indicates weaker engagement and limited awareness in cybersecurity. The ATC-IB is made up of twenty-five Likert items of four response levels scored from 1 to 4 points (1 = Totally Agree; 2 = Agree; 3= Disagree and 4 = Totally Disagree). This scale contains items with inverse scores namely items 2,14,15, 19, 20 and 21.

The adopted methodology aims to evaluate the following research hypotheses: i) to verify if there are significant differences in mean RScB values between age groups, professional classes and gender; ii) to verify if there are significant differences between the mean values of the ATC-IB scale between the age groups, professional classes and gender; iii) to check if there is a correlation between RScB and ATC-IB scale values considering the different ages; and iv) to determine if there are differences by items of the RScB scale and the ATC-IB scale considering the different age groups, professional classes and gender;

Fig. 1 depicts the methodology applied for translation and validation of questionnaires, which follows Beaton's five steps methodology [14]. Firstly, a translation of both scales from English language to Portuguese was made. Then, a summary of translated versions and a retranslation was made for both scales, as some discrepancies have to be fixed before sent the questionnaire to the experts' panel evaluation, in step four. Finally, a pre-testing was made in step 5.

Fig. 1 – Translation and validation methodology according to Beaton [14]

Table 1 - English version of the questionnaires RScB and ATC-IB, both adapted from the original version available in [6].

1. Sharing passwords with friends and colleagues.
2. Using or creating passwords that are not very complicated (e.g. family name and date of birth).
3. Using the same password for multiple websites.
4. Using online storage systems to exchange and keep personal or sensitive information.
5. Entering payment information on websites that have no clear security information/certification
6. Using free-to-access public Wi-Fi
7. Relying on a trusted friend or colleague to advise you on aspects of online security.
8. Downloading free anti-virus software from an unknown source.
9. Disabling the anti-virus on my work computer so that I can download information from websites.
10. Bringing in my own USB to work in order to transfer data on to it.
11. Checking that software for your smartphone/tablet/laptop/PC is up to date.
12. Downloading digital media (music, films, games) from unlicensed sources
13. Sharing my current location on social media.
14. Accepting friend requests on social media because you recognise the photo.
15. Clicking on links contained in unsolicited emails from an unknown source.
16. Sending personal information to strangers over the Internet.
17. Clicking on links contained in an email from a trusted friend or work colleague.
18. Checking for updates to any anti-virus software you have installed.
19. Downloading data and material from websites on my work computer without checking its authenticity.

1. I think that management have the responsibility to ensure a company is protected from cybercrime
2. I am aware of my role in keeping the company protected from potential cybercriminals.
3. I believe everyone in the company has a role to play in protecting against threats from cybercriminals.
4. It is hard to know how I can help protect the organisation from cybercrime.
5. I don't have the right skills to be able to protect the organisation from cybercrime.
6. I do not feel that IT security is a priority within my organisation.
7. Computer systems provide all the protection a company needs.
8. I think that reporting cybercrime is a waste of time.
9. The Police lack the capacity to deal with cybercrime effectively.
10. I believe that cybercriminals are more advanced than the people who are supposed to be protecting us.
11. I think that information provided by the Government and Police on cybercrime is not relevant to business.
12. I feel that the Police are far too busy to deal with cybercrime.
13. I worry that if I report a cyberattack to the Police it might damage the reputation of the company.
14. I think more could be done to communicate the risks from cybercrime to individuals in the organisation.
15. I am aware of the company's IT use policy and attempt to follow it.
16. I would not know how to report a cyberattack if one happened.
17. I don't think that reporting a cyberattack on the company is my responsibility.
18. I don't pay attention to company material about the threats from cybercrime.

20. Storing company information on my personal electronic device (e.g. smartphone/tablet/laptop)

19. I am confident that I would be able to spot the signs of a cyberattack.
20. I think the biggest threat for IT systems comes from people within the company.
21. I feel that any individual within the company are at risk of manipulation from confidence tricksters.
22. I think that cybercrime only target a company when there is a substantial financial gain.
23. I believe only large companies are targeted by hackers and cybercriminals.
24. I feel that only companies that take payments using online systems are at risk of being victims of cybercrime.
25. I don't think I know who is responsible for protecting the company from cybercrime.

After the five stages illustrated in Fig. 1, the questionnaires were made available digitally, to be filled on an online survey platform (`https://www.esurveycreator.com/`), by the practitioners of "Centro Hospitalar Barreiro Montijo (CHBM),

Table 1 lists both RScB and ATC-IB questionnaires in English version, with the adjustments made in some items, regarding the original version [6]. The corresponding Portuguese version of the questionnaires are available on demand, by contacting the authors.

In order to avoid multiple participation by the same participant, the navigation session ID of the participants was blocked by setting a digital platform's own cookie. The following professional groups participated: operational assistants, Technical/Technical Assistant/ Administrative Staff, nurses, physicians, senior technician, Senior Diagnostic and Therapeutic Technician (SDTT).

Traditional descriptive methods were used to describe demographic characteristics, namely mean and standard deviation for continuous variables and percentages for categorical variables. Cronbach's alpha was used to analyze the internal consistency of the two scales. A 0.7 reliability is considered adequate for a survey instrument [15], although some authors consider 0.6 and higher adequate [16]. Items negatively worded were reverse-scored for further analysis. Shapiro-Wilk test was used to test for normality adjustment of the data, ANOVA analysis or the alternative non-parametric Kruskal-Wallis test were conducted whenever normality assumption was verified to compare more than two independent groups. Mann-Whitney test was used to compare two independent groups and Spearman's coefficient was used to analyze correlation between RScB and ATB-IB scales. Boxplots were used to compare distributions between groups and Bland-Altman plot was used to analyzes the agreement between the two scales. We have considered a 5% significant level and multiple testing adjustments were made using Bonferroni approach.

For the statistical data analysis, we have used the following applications: IBM SPSS (Statistical Package for the Social Sciences, version 22) and Microsoft Office Excel for Office 365.

4. Results analysis

This Section describes the analysis of the results obtained by filling out the RScB and ATC-IB questionnaires by CHBM employees. The analysis was made to the corresponding scales already previously described.

According to 2018 CHBM report, the estimated population if of 1726 professionals from where 65 responded to the questionnaires, which corresponds to a participation rate of 3.8%. After applying inclusion and exclusion criteria it was obtained a sample of 56 respondents. The age of the participants ranged between 27 and 61 years with mean (SD) 44.3 (9.2). It was observed that 40 participants are female (71%) and 16 participants are male (29%). The professionals who did respond the questionnaires were distributed as follows: Operational Assistants 8.9% (n=5); Technical/Technical Assistant/ Administrative Staff 3.6% (n=2); Nurses 33.9% (n=19); Physician 17.9% (n=10); Senior Technician 3.6% (n=2); Senior Diagnostic and Therapeutic Technician (SDTT) 32.1% (n=18).

4.1. RScB scale

The RScB scale assumes score values between 0 to 120 and higher values are indicative of riskier behavior in cybersecurity. The values obtained by the participants ranged between 0 and 64 with a mean (SD) of 31.6(14.2). It was achieved a Cronbach's alfa of 0.745, where the authors of the questionnaire [6] obtained 0.823.

A one-way ANOVA analysis was conducted to compare the mean scores of the scale between professional classes and between age groups ($\leqslant$37; 38-43; 44-53 and $\geqslant$53), and it was not found significant differences (F=1.189, p =

.323; F=0.675, p = .571). To compare man and woman median scores of the scale a Mann-Whitney test was used, and no significant differences was found (U=285.5, p = .531).

An individual item analysis was conducted to compare between age classes, between professional groups and between gender. A Kruskal-Wallis test was used to compare the medians of the items between age groups and in Fig. 2 it is represented the boxplots of the items where it was found significant differences between age groups.

Fig. 3 depicted the boxplots of the items where it was found significant differences between professional classes. Technical Assistants and Senior Technicians were not considered in this analysis since the simple sizes are too small. When comparing items by gender it was found significant differences in the item 12, "Download digital contents (music, movies, games) from unreliable sources" (Mann-Whiney test: U = 140.5, p =.001).

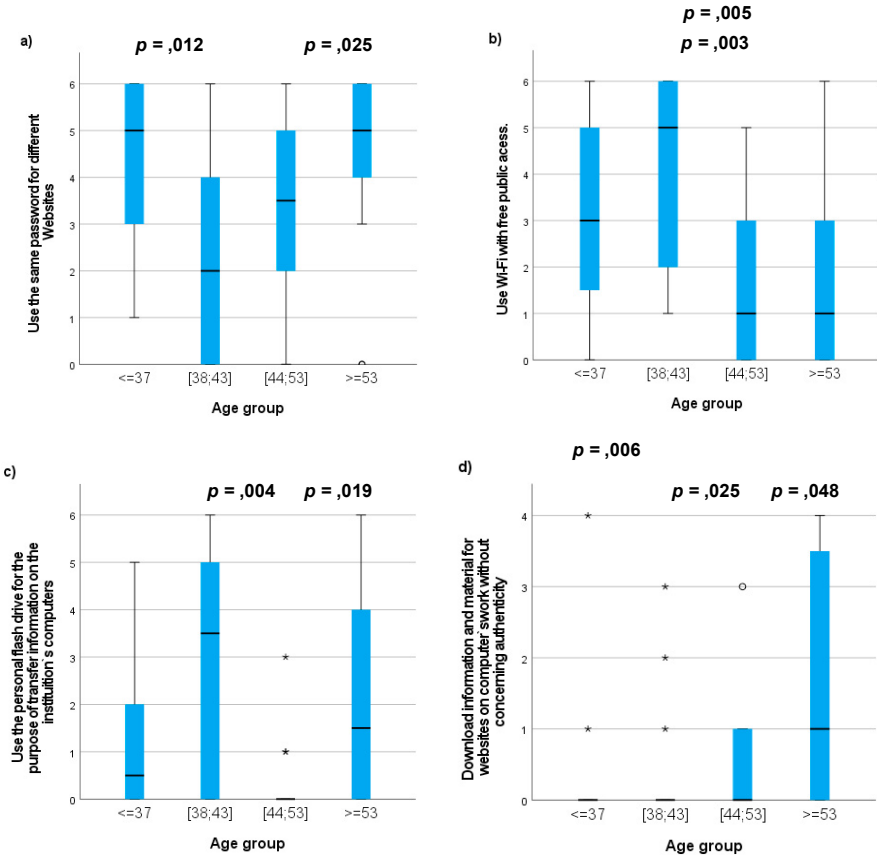

Fig. 2 - Boxplots of the items where it was found significant differences between age groups. $p$values on boxplots were adjusted for multiple comparisons. Kruskal-Wallis statistical value and corresponding $p$value: a) KW = 7.98, p = .046; b) KW = 12.0, p = .007; c) KW = 9.994, p = .019; d) KW = 8.424, p = .038.

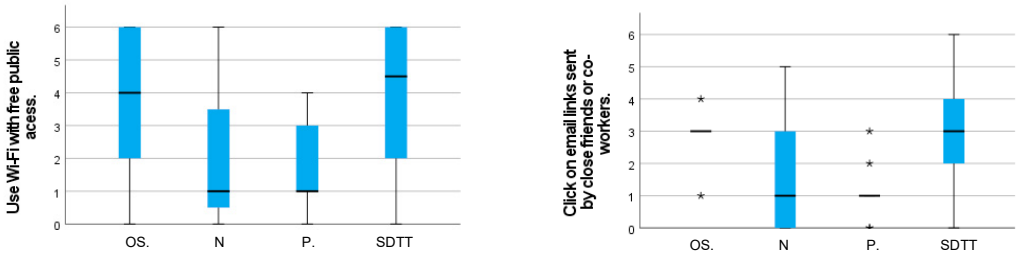

Fig. 3 - Boxplots of the items where it was found significant differences between professional classes. *p*values on the boxplots were adjusted for multiple comparisons. OA: Operational Assistants; N: Nurses; P: Physicians; SDTT: Senior Diagnostic and Therapeutic Technician. Kruskal-Wallis statistical value and corresponding *p*value: a) KW = 7.99, p = .046; b) KW = 8.79, p = .032.

4.2. ATC-IB scale

The ATC-IB scale has scored values between 25 to 100 and lower values indicate a riskier behavior in cybersecurity. The values obtained in this sample ranged between 48 and 82 with a mean (SD) of 66.4 (6.3). It was achieved a Cronbach's alfa of 0.723, where the authors of the questionnaire [6] obtained 0.744.

A one-way ANOVA analysis was conducted to compare the mean scores of the scale between professional classes and between age classes ($\leqslant$37; 38-43; 44-53 and $\geqslant$53), and it was not found significant differences (F=0.418, p = .741; F=1.071, p = .370). To compare man and woman median scores of the scale, a Mann-Whitney test was used, and no significant differences was found (U=310, p = .856).

An individual item analysis was conducted to compare between age classes, between professional groups and between gender. Considering age groups, it was not found any significative differences. Considering professional classes it was found significative differences in the item 7, "Information systems offer all the protection that an institution needs" (KW=8.126, p = .046) and in the item 12, "The Authority is too busy to be concerned about cybercrime" (KW=10.513, p = .015). A Mann-Whitney test was used to compare the medians of the items between gender. In Fig. 4 it is represented the boxplots of the items where it was found significant differences.

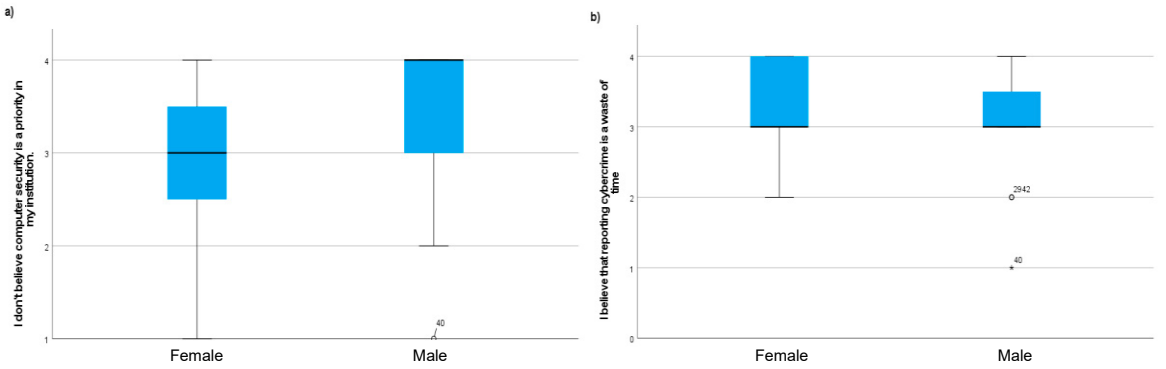

Fig. 4 - Boxplots of the items where it was found significant differences between gender. a) MW = 214, p = .039; b) MW = 222, p = .046.

4.3. Comparison of RScB and ATC-IB scales

Fig. 5 depicts the Bland-Altman plot of the two scales under evaluation for this research: RScB and ATC-IB. It was considered the z scores of both scales. The results obtained allowed us to analyze the agreement between them and, it can be observed that are several values out of the limits of agreement, meaning that both scales have a low level of agreement. It was also verified that there is a statistically significant moderate correlation between RScB and ATC-IB (r = -0.414, p = .002).

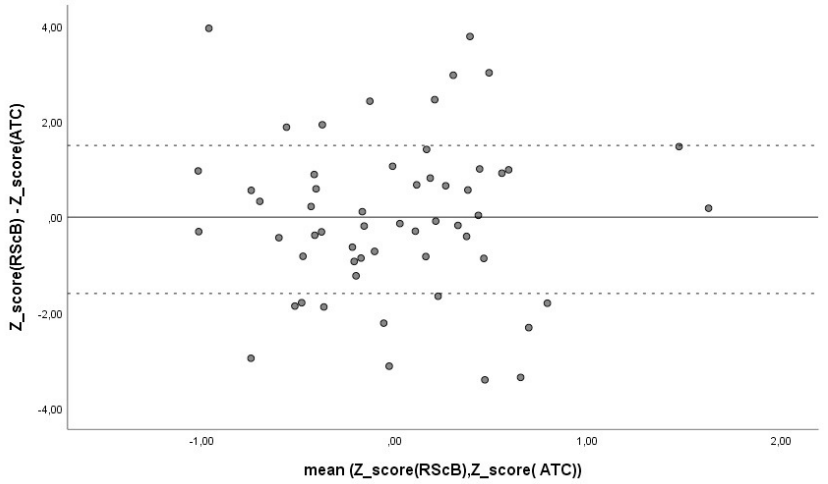

Fig. 5 - Bland-Altman plot of the z scores of the RScB and ATC-IB scales. The solid line represents the mean of the differences of both scales and dotted lines the corresponding 95% confidence interval.

5. Conclusions and future work

This paper presents the evaluation of the healthcare practitioners' awareness level regarding information security, namely by assessing their attitudes and behaviors in cybersecurity through two questionnaires. This study has confirmed the correlation between risky behavior in cyber-security and attitudes towards cyber-security in the business environment, as described in the literature, establishing the bridge for the quantification of information security culture promoted by the Knowledge–Attitude–Behavior (KAB) model [10].

The major conclusions of the application of these questionnaires to this population group is two-fold: it revealed the value added by this pioneering application in Portuguese healthcare institutions; it allowed to make a portrait of the behaviors and attitudes in terms of cyber-security in the institution that was evaluated.

The cybersecurity ability and skills of health professionals need to be quantified, as technologically evolved systems need people with knowledge to avoid security breaches according to established security standards. However, given the small sample size, further research is needed to confirm the convergence of the translated version with the objective of its future use to obtain a more comprehensive trend in behaviors and attitudes towards cybersecurity.

Acknowledgements

We'd like to thank Professor Lee Hadlington, of the University of Montfort, Leicester, author of the RScB and ATC-IB scales, for his permission to translate and apply them to the Portuguese language, which was kindly granted.

We'd also like to thank to "Centro Hospitalar Barreiro Montijo", for the availability to apply the questionnaires.

This work is partially financed by national funds through FCT Fundação para a Ciência e a Tecnologia under the project UIDB/00006/2020.

References

[1] James Scott. "What the health sector needs to know about cryptocurrency technologies, blockchain and cryptojacking attacks"; Available from: Institute for Critical Infrastructure Technology; May 2018; https://irishtechnews.ie/what-the-health-sector-needs-to-know-about-cryptocurrency-technologies-blockchain-and-cryptojacking-attacks/

[2] Stanciu, Victoria, and Andrei Tinca. "Exploring cybercrime–realities and challenges." Accounting and Management Information Systems 16.4 (2017): 610-632.

[3] Tandon, Aditya, and Anand Nayyar. "A Comprehensive Survey on Ransomware Attack: A Growing Havoc Cyberthreat." Data Management, Analytics and Innovation. Springer, Singapore, 2019. 403-420.
[4] Sittig, Dean F., and Hardeep Singh. "A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks." Applied clinical informatics 7.02 (2016): 624-632.
[5] Tara Seals; " One Year After WannaCry: A Fundamentally Changed Threat Landscape"; Available at https://threatpost.com/one-year-after-wannacry-a-fundamentally-changed-threat-landscape/132047/
[6] Hadlington L. "Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours". Heliyon . 2017;3(7):e00346.
[7] Henry Gleitman, James Gross, Daniel Reisberg; "Psychology"; 8th ed; ISBN 978-0-393-11726-4; Editor: Sheri L. Snavely; 2011
[8] Egelman S, Peer E. "Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS)". Proc ACM CHI'15 Conf Hum Factors Comput Syst [Internet]. 2015;1:2873–82.
[9] Kruse, Clemens Scott, et al. "Cybersecurity in healthcare: A systematic review of modern threats and trends." Technology and Health Care 25.1 (2017): 1-10.
[10] Parsons K, Calic D, Pattinson M, Butavicius M, McCormac A, Zwaans T.; "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies."; Comput Secur 2017;66:40–51.
[11] Hadlington L. "The Human Factor in Cybersecurity". In: Psychological and Behavioral Examinations in Cybersecurity [Internet]. 2018. p. 46–63.
[12] Aivazpour Z, Rao VSC. "Impulsivity and Risky Cybersecurity Behaviors : A Replication"; Proc Am Conf Inf Syst. 2018;(2017):1–9.
[13] Öğütçü, Gizem, Özlem Müge Testik, and Oumout Chouseinoglou. "Analysis of personal information security behavior and awareness." Computers & Security 56 (2016): 83-93.
[14] Beaton DE, Bombardier C, Guillemin F, Ferraz MB. "Guidelines for the process of cross-cultural adaptation of self-report measures."; Spine (Phila Pa 1976); 2000 Dec 15;25(24):3186–91.
[15] Bland, M. and Altman, G. "Statistics notes: Cronbach's alpha", British Medical Journal, Vol. 314, 1997, p. 572.
[16] Field, A. "Discovering Statistics Using SPSS for Windows", SAGE Publications, London. 2000.