Success factors for data protection in services and support roles: combining traditional interviews with Delphi method

Pedro Ruivo, NOVA IMS, Universidade Nova Lisboa, Portugal

Vitor Santos, NOVA IMS, Universidade Nova Lisboa, Portugal

Tiago Oliveira, NOVA IMS, Universidade Nova Lisboa, Portugal

Success factors for data protection in services and support roles: combining traditional interviews with Delphi method

Pedro Ruivo, NOVA IMS, Universidade Nova Lisboa, Portugal

Vitor Santos, NOVA IMS, Universidade Nova Lisboa, Portugal

Tiago Oliveira, NOVA IMS, Universidade Nova Lisboa, Portugal

ABSTRACT

The transformation of today's information and communications technology (ICT) firms requires the services and support organizations to think differently about customers data protection. Data protection represents one of the security and privacy areas considered to be the next "blue ocean" in leveraging the creation of business opportunities. Based in contemporary literature, we conducted a two phases' qualitative methodology - the expert's interviews and Delphi method to identify and rank 12 factors on which service and support professionals should follow in their daily tasks to ensure customer data protection: 1) Data classification, 2) Encryption, 3) Password protection, 4) Approved tools, 5) Access controls, 6) How many access data, 7) Testing data, 8) Geographic rules, 9) Data retention, 10) Data minimization, 11) Escalating issues, and 12) Readiness and training. This paper contribute to the growing body of knowledge of data protection filed. We provide directions for future work for practitioners and researchers.

Keywords: *Data protection; data classification; privacy; security; support; services; interviews; Delphi.*

INTRODUCTION

Businesses and organizations are creating and using data at unprecedented rates. With this boom in data comes challenges and problems in data protection. Customers expect their data to be protected and not used in a manner inconsistent. The protection of their data is paramount to customers, and they evaluate information and communications technology (ICTs) firms in part on how well they handle and protect it from being stolen or used improperly. In many industries customers are specifically mandated to evaluate how ICTs firms protects their data. When customers create an account with ICTs firms, or use their services, they expect that a set of specific rules around how ICTs are used to manage their information (Cruz-Cunha & Portela, 2015). Previously, enterprises emphasized perimeter security over things like endpoint protection and data-centric security. If from one side the ever-expanding security and privacy perimeters make it necessary for companies to find data protection processes that secure data from both internal and external threats, placing the focus on sensitive data as it travels within and outside of enterprise networks. On the other side, the ever-changing landscape of data protection is not resulting in knowledge sharing and thoughts. With the sheer quantity of information and resources on data protection available today, it can be difficult to sort through it to find the most trusted and experienced sources that provide accurate insights and educated perspectives on relevant data protection challenges facing modern enterprises. In particular, the literature is lacking on methodological grounded knowledge about how ICT professionals should follow in order to ensure data protection. This is becoming critical as more and more ICT firms are evolving from a purely focus on software and communications to services providers, customer's data protection is critical factors in winning customer trust (Bélanger & Crossler, 2011; Pavlou, 2011; Slyke, Shim, Johnson, & Jiang, 2006; Stantcheva & Stantchev, 2014).

Reputable ICTs firms such as Microsoft, SAP, Portugal Telecom, ONI-Communications and Vodafone among others, have built a strong foundation of privacy and security practices (OECD, 2012). The past decade has brought immense changes in technology, requiring ICTs firms to continually evolve and reaffirm their commitment to trustworthy computing regardless if inshore, nearshore or offshore service and support models (Casado-Lumbreras, Colomo-Palacios, Ogwueleka, & Misra, 2014; Colomo-Palacios, Casado-Lumbreras, Soto-Acosta, Misra, & García-Peñalvo, 2012; Colomo-Palacios, Leeney, Varajão, & Ribeiro, 2011). Hence is a must to continue to meet customer's data protection demands to meet regulations, customer expectations, and consumer perceptions (Hong & Thong, 2013; Pavlou, 2011). Instead of broadly study privacy or security situations handled by professionals this research paper focuses on the data protection field from the outlook of good practice in the management of IT human capital, filling a gap in the literature (Pavlou, 2011). Motivated by these issues, this study seeks to answer to the following research question:

RQ - What are the critical factors and their importance on which ICTs professionals in support and services roles should follow in their daily tasks in order to ensure customer's data protection?

To answer this question we developed and implemented a two phase's research: we commenced with the traditional questionnaires interview methodology with 17 experts in order to identify the factors, and then the Delphi method with 20 experts in order to obtain the ranking and consensus on the factors. The theoretical background is presented in the next section. Then we introduce the combined methodologies. After we present the results and analysis. Then the paper concludes with the main findings, including implications, limitations and future research opportunities.

THEORETICAL BACKGROUND

There are many things that make companies successful. Some are tangible, like products, buildings, and people. Others are intangible, like reputation and trust. These intangible assets are hard to measure, but they are essential to the future of ICT firms (Bansal & Gefen, 2010; Dinev, Xu, Smith, & Hart, 2013; Frye & Dornischa, 2010). Trust should be at the heart of what these firms do. Without it, their customers wouldn't share their information with them, use their services, or buy their products (Culnan & Armstrong, 1999; Liu, Marchewka, Lu, & Yu, 2005). Ensuring the privacy of customer information is a key driver of trust (Bansal & Gefen, 2010). Moreover, protecting privacy is required by law, and it helps ICTs firms avoiding fines and regulatory actions (Cruz-Cunha & Portela, 2015; Milberg, Smith, & Burke, 2000; Okazaki, Li, & Hirose, 2009; Portela & Cruz-Cunha, 2012). Customers' trust is win by making sure that their information is collected, used, and stored with the utmost care and respect.

Accordingly with literature, privacy means respecting the rights of the individual and organizations to control the collection, use, and distribution of their data, as well as providing them with ways to manage their communication preferences (Bélanger & Crossler, 2011; Bélanger, Hiller, & Smith, 2002; Culnan & Armstrong, 1999; Dinev & Hart, 2006). In the past privacy practices were focused on the basics: Notice, Choice, Consent and Personally Identifiable Information. This focus once served the ICT firms well, but the last years has seen tremendous changes: we're online all the time, exchanging information, connecting with friends and colleagues around the world, blurring the lines between personal time and work. Consumers' expectations of privacy have changed, and regulators and service providers struggle to keep up (Bansal & Gefen, 2010; Malhotra, Kim, & Agarwal, 2004; Smith, Dinev, & Xu, 2011). In response, ITC firms are integrating more targeted privacy notice and controls into their products and services, and evaluating risks and threats against a broader set of personal information. Today, privacy is not just about personally identifiable information. Instead, it's about recognizing that all information can carry differing levels of risk depending on a variety of factors, including their connection to other information (Awad & Krishnan, 2006; Hui, Teo, & Lee, 2007; Poindexter, Earp, & Baumer, 2006; Son & Kim, 2008). For example, a piece of anonymous information (like birth year) can quickly become personally identifiable information or even sensitive personally identifiable information when it is found in combination with other information (like full name or real-time location) (Bélanger & Crossler, 2011; Smith, et al., 2011). To manage privacy risks, it's mandatory to know how to classify information, recognize what other data it may be linked to, and understand the potential impact (Bansal & Gefen, 2010; Dinev, et al., 2013; Hong & Thong, 2013; Pavlou, 2011).

Whereas privacy is about respecting individuals' rights to control their personal data, security is actually protecting that data from loss, misuse, unauthorized access, disclosure, alteration, or destruction (Dinev & Hart, 2006; Dinev, et al., 2013; Hong & Thong, 2013; Smith, et al., 2011). Security requirements vary depending on the type of data collected and whether it will be stored locally, remotely, or transferred. Security is essential to privacy. It is not possible to have privacy without security. Hence preventive security measures may include: Access controls, Encryption in transfer and storage, Physical security, Disaster recovery, and Auditing (Acquisti & Grossklags, 2005; Bélanger, et al., 2002; Pietro & Mancini, 2003; Skinner, Han, & Chang, 2006).

Although very few, there are some norms around the protection of customer data: I) ISO 27001 (2013) is widely-recognized international security management certification that specifies privacy and security management best practices. II) Data processing agreements, are contracts ICTs sign with customers. They include specific terms around privacy, security, and handling of customer data. III) The EU commission model clauses (2010) is a contract addendum with extra data protection requirements that it is recommended for commercial deals in the European market. IV) HIPAA (Health Insurance Portability and Accountability Act) (1996) business associate agreements, are contractual obligations that ICTs are required to sign with customers to do business in the US market.

However these norms do not reflect how ICT firms are actually doing in order to ensure data protection. So, this paper aims to systematize the above norms, industry practices and sheer knowledge within ICT professionals to meet the commitment on customer's data protection. We next present the research methodology and explain its implementation in order to identify and rank the critical success factors for data protection in ICTs firms.

METHODOLOGY AND IMPLEMENTATION

Critical success factors can be identified either through a literature review or by exploratory research. The nature of this work is exploratory in nature, following a qualitative approach. Unlike conventional research, we combined the traditional interview and Delphi methodologies in two phases: Phase I) supported on the existing literature in the field of data privacy and security, we used a semi-structured questionnaire for expert interviews to identifying the relevant success factors of data protection in ICT firms (Malhotra, Birks, Palmer, &

Koenig-Lewis, 2007); Phase II) supported on the factors identified on previous phase, we used the Delphi method to obtain the consensus from experts as well as to create a ranking of these factors according to their importance (Okoli & Pawlowski, 2004; Paré, Cameron, Poba-Nzaou, & Templier, 2013).

Given the background and motivation of this research we additionally used the Delphi method mainly due two reasons. Firstly, for this type of exploratory, theory-building research, a Delphi study is an appropriate research design (Akkermans, Bogerd, Yücesan, & Van Wassenhove, 2003). Previous studies have also used this method to address similar research questions. According to Paré, et al., (2013) and Okoli & Pawlowski, (2004), a Delphi study is the appropriate method to address complex issues that requires expert knowledge such our research question in this study. Secondly, it lends itself especially to situations where subjective and complex judgments are of interest, as opposed to precise quantitative results (Daniel & White, 2005). Thus, since the task at hand involves, identifying the relevant success factors, as well as determining their relative importance, the Delphi method fits the purpose and allows us to pinpoint the areas where more attention is required.

Phase I – Expert interviews

The design and implementation of this phase follows the structure and the explanations from Malhotra et al, (2007). Supported on the existing literature in the field of data privacy and security, which is still at the beginning, the first research method was the semi-structured expert interviews. These interviews were conducted with 17 experts (Support, Consultants, Architects, Engineers, product managers, technical sales) in data privacy and security domain within Microsoft, SAP, Portugal Telecom, ONI-Communications, and Vodafone.

The face-to-face interviews were conducted between September 9th and November 15th 2013. Each lasted approximately 30 minutes and was recorded digitally with the verbal permission of the interviewee. A qualitative interview-guide approach was followed, meaning that the topics of each interview were specified in advance and that the responses from the participants were open-ended and not restricted to choices provided by us. The interview-guide had several questions created from the literature and secondary informational sources such as IDC (Amatruda, 2013; Arend, 2013) and OECD (OECD, 2010, 2012). An inductive approach was used and the data analysis method selected was the "content matrix analysis" (Malhotra, et al., 2007; Malhotra, et al., 2004), particularly suitable as the first phase of an exploratory research because it represents a key instrument in the creation of appropriate factors.

The interviews study followed the five steps process as proposed by Malhotra et al, (2007): 1) After all interviews were completed, we transcribed each interview selectively, and irrelevant information was left out. By irrelevant information is meant statements which were not relevant to shed light on the posed research questions. 2) Themes were then identified for each interview, meaning that the transcription was examined for descriptions, patterns, observations and interpretation that could shed light on our research questions. 3) The identified themes for each transcription were then compared across all interviews. 4) Each interview was then further reduced with the aid of the identified themes to a list of statements which 5) afterwards was validated against the raw information (into a matrix of content) to ensure that the statements did not misrepresent the participant and grouped into a list of categories. The results and analysis are presented in next Section.

Phase II – Delphi method

The design and implementation of this phase follows the structure and the explanations from Okoli and Pawlowski (2004). Supported on the factors identified on previous phase, the second research method used was the Delphi method. We designed a web questionnaire where experts were asked to rank those issues based on a 5-Likert scale, where 1 represents "strongly disagree and 5 “strongly agree". A descriptive explanation of each issue was provided. We also include on the questionnaire an informative webpage where experts could read the glossary of main concepts.

The identification of ‘panel experts’ was based on a multiple-step approach suggested by Okoli and Pawlowski (2004). Of the 40 invitations, 25 candidates accepted to participate in the Delphi study. This is considered ideal according to Linstone and Turoff (1975). The panel experts was composed by experts from six countries: Denmark, Germany, Portugal, Spain, United Kingdom and United States of America, and high qualified in Data Protection field, 87% have more than 8 years of experience. The table of the profile of the survey respondents is available from the authors on request.

During the study 5 panel experts dropped out, leaving a panel of 20 experts who participated in the two rounds of the study. The Delphi study took place between March 10th and May 30th 2014. The two rounds were performed during 21 and 15 days respectively, with an interval of 20 days between rounds for data analysis and to prepare the next round. With a homogeneous panel of 20 participants that have completed the study, we believe that the results are relevant and that are not constrained by the number of participants (Okoli & Pawlowski, 2004; Paré, et al., 2013).

The Delphi study followed the three steps process as suggested by Schmidt (1997): 1) Brainstorming - participants were asked to review the list of 12 key issues generated from the interview study. The issues were presented randomly. Participants were encouraged to update issue rationale. 2) Narrowing - we decide to exclude the narrowing phase based on our research goals and the number of items. In the literature, the majority of the studies do not include this step due to the number of items be equal or less to 20 (Schmidt, 1997). In our study 12 issues were analyzed which is meet the criteria used by Schmidt (1997). 3) Ranking - in the first round, the list of 12 factors was sent to the panel in random order to avoid any bias. For the second round, the skills were ordered by mean rank. The panel were asked to indicate their views by rating each factor for relevance. At the end of each round, Kendall’s coefficient of concordance (W) was calculated to assess the degree of consensus among the panelists (Okoli & Pawlowski, 2004; Paré, et al., 2013; Schmidt, 1997). Until achieve a reasonable degree of consensus, one subsequent round was realized. The average values of the variables confirmed that we identified a plausible set of factors with average value of higher than 3. Data Protection experts responding to the first round were sent feedback showing the results of the first round so that individual judgments may be modified or refined. The feedback included between the rounds included the mean ranks of items, Kendall’s W coefficient achieved and expert’s prior responses. As suggested by Delphi researchers (Okoli & Pawlowski, 2004; Paré, et al., 2013; Schmidt, 1997) new factors are included only if they were suggested independently by at least three respondents. Since this criterion was not achieved, the suggested factors were not included. The aggregate ranking was used to reorder the list of factors. Factors were presented in order of importance as determined by mean rank. The results and analysis are presented in next Section.

RESULTS AND ANALYSIS

In this section, we present and analyze the results obtained in each phase described in the section before in order to answer to our research question.

Phase I – Expert interviews

We analyzed the collected data accordingly with the five steps process as proposed by Malhorta and Brigs (2007) and obtained a list of 12 factors identified by the 17 experts from ICTs in regards to data protection. The following 12 factors aren't listed in any particular order, other than by category.

Data classification - Accordingly with all interviewed experts the data classification can and must be done by adding a symbol, pop-up warning, or any other visual element to that data which in turn can capture the attention to ITC's professionals about data protection. Data needs to be classified into one of these three categories: i) High Business Impact (HBI) - If HBI data is disclosed, severe or catastrophic material loss could occur. Access and use must be strictly controlled and limited on a "need-to-know" basis. ii) Medium Business Impact (MBI) - If MBI data is disclosed, serious material loss could occur, potentially causing damage to the reputation of ICT firm. Access and use must be limited to those who have legitimate ICT business need. iii) Low Business Impact (LBI) - If LBI data is disclosed, limited material loss could occur.

These three categories as well as the recommendation to protect the data are next explained based on interviews evaluations. It should be noted, that for the definition of the categories no theoretical assumptions were made. Since the formation of the categories was inductively abstracted from the singular representations, the definitions are a merger of different verbal dictions with the same meaning. The direct contact with the participants, experts from ICTs named above with specific knowledge about the development, strategy and customer needs of data protection as well expertise in customer support and services, ensured the quality of data for this research. This is especially true, as these participants are permanently in contact with customers, absorbing their needs

More precisely, accordingly with all interviewed experts the LBI classification must be assigned to customer data where unauthorized disclosure would have limited material loss. Examples of LBI could include: First or Last name only, Gender or Country of residence. Is also need to note that any of these examples of LBI could become MBI or HBI when aggregated with other data.

In view of all interviewed experts the MBI classification must be assigned to customer data where unauthorized disclosure would cause serious material loss to ICT firm, the information owner, or other parties. Examples of MBI include account information, customer name, address, phone or number, email address and IP address. In regards to customer data includes any information that is sent from ICTs customers such as; case notes, network traces, diagnostic data, system configuration and business engagements. On other way, customer personally identifiable information include any information that identifies or can be uses for identify, contact or locate the person to whom such information pertains.

Accordingly with all interviewed experts there are generally three types of HBI classification that must be assigned to customer data where unauthorized disclosure could cause severe or catastrophic material loss to ICT firm, the information owner, or other parties. These three types are: i) Data that is kept secret for security purposes, or that can lead to identity theft. Examples including passwords, certificates (private keys), secret passphrase, bank/financial account information, citizen ID/security ID/governments IDs, real-time location or credit card numbers. ii) Data that is high value to the customer. Examples including files containing detailed customer strategic plans, customer security vulnerabilities, technical specifications or trade secrets. iii) Data that can be used to discriminate. Examples including healthcare/medical information as well as racial or ethnic origin information, political filiation, religious beliefs, physical or mental health or condition, sexual life, any proceedings for any fiscal, civil, criminal or sentencing decisions made by any non-legal or legal entities such as courts.

Access controls - All interviews claim that, site, file, application or tool owners must set appropriate permissions on the sites they control. Must assign users to the least privilege that they need to fulfill their job functions. Must only grant privileges to a site, file, application or tool if the user has a valid business need to access the project information.

Approved tools - Use only approved/certified tools to ensure that customer data is collected and stored securely, and that appropriate data protection requirements are in place by following ISO 27001. Never store any customer data on tools such as DropBox, OneDrive or GoogleDrive.

Passwords - Accordingly with all interviewed experts ICT personal must always protect passwords. Never share or give password to anyone. This includes their supervisors and other computer support personnel. ICT personal should not ask anyone for their password, including customers. Must change passwords periodically, or immediately when disclosed. Must protect all devices with passwords or other authentication credentials. It is important to construct effective passwords. It can be done do this by following the following rules for complex passwords – do not use: login name in any form; a first or last name in any form; information easily obtained about ICT personal, such as telephone numbers, sports teams, child's names, or words out of the dictionary. Instead, it must use mixed-case letters with non-alphabetic characters.

Encryption - For all data ICT personal must use encryption security tools such as BitLocker, TrueCrypt or Seagate's FDE on laptops, desktop or other devices, including portable media, such as USB flash drives or external hard drives. For MBI data, ICT personal must encrypt data while it is being sent. For files, use a secure file transfer tool, never e-mail. For HBI data, ICT personal must encrypt in transit and at rest.

How many access data - For LBI and MBI, depends on the business need. ICTs must re-evaluate each individual with access every 90 days. For HBI, as few people as possible. Accordingly with the interviewers as a best practice: If adding 20 plus people it should be escalated to upper management level for review.

Escalating issues - When customer's inquiries' ICT professionals about access, collect, or manage customers' personal information, there should be a process in place to handle it accordingly. Examples of these situations might be encountering a customer that asks about their privacy rights, or asks that their data be deleted, changed, modified, or for access to or a copy of their data. That is, any reference to privacy or data protection would also indicate a need for special attention. The key words or phrases a customer may use that may indicate that the request needs special attention include: “Access”, “Change” and “Deletion”. Accordingly with expert verbatim, some examples of customer communications where ICT professionals should escalate the issue to a privacy specialized team include: “I am concerned about my privacy. I want you to remove all of my information from your sites.” This would be an example of a request for deletion. “You've violated my privacy rights in the contract terms.” This would be an example of a general inquiry about privacy. “Please change my original account email address, and do not send the updated email account information to my old email address.” This would be an example of a request to change or modify data. “I want a record of the data your firm has saved and shared about me.” This would be an example of a request for access to information. “I believe you transferred my data in violation of the US-EU Safe Harbor program.” This would be an example of an inquiry about data transfer across geographies.

Readiness and training - Avoid using the name of a customer, customer data, or any information that could identify the customer in a presentation, readiness or training sessions. This includes workshops, case studies or other training regardless of size, internal or external audiences.

Geographic rules - Data should not be sent between countries without checking with the customer and legal representatives.

Data retention – for support and services tasks purposes only, all customer data must have a retention timeframe. For files or most HBI data, delete after 90 days. For tickets, case notes or most MBI data, delete after 120 days. For LBI data, delete after 18 months.

Testing customer data - When testing customer data services and support personal must use ICT´s firm labs and only use production data in a test environment with customer approval and only for the purpose of troubleshooting customer issues.

Data minimization - Only collect data that actually is going to be used to support or service customers.

Table 1 shows the evolution of the factors during the Delphi study sorted by their position in the final round. This position was obtained using the average rank of each factor. For each round, we present the number of respondents (N), the Kendall's coefficient of concordance (W) and the Spearman's rank-order correlation coefficient (Spearman's rho). The average rank (AVG), standard deviation (SD) and Rank position are shown for the 12 factors. The Delphi study was terminated at the second round with a total of 20 respondents, 75% of the initial group; a W>0.50 and a Spearman's rho = 0.929.

Table 1. Results of the ranking-type Delphi of the two rounds

Factors	**Round 1**			**Round 2**		
	AVG	**S.D**	**Rank**	**AVG**	**S.D**	**Rank**
Encryption	3.83	1.11	5	4.09	0.87	2
Approved tools	3.90	0.88	3	3.82	0.73	4
Passwords	3.87	1.01	4	3.83	0.73	3
Data classification	4.27	0.64	1	4.32	0.72	1
Access controls	4.20	1.00	2	3.86	0.83	5
How many access data	3.77	1.07	6	3.68	0.78	6
Testing customer data	3.63	1.03	11	3.59	1.01	7
Geographic rules	3.80	1.00	9	3.55	0.86	8
Data retention	3.67	1.09	10	3.68	0.84	9
Data minimization	3.63	1.10	12	3.05	0.79	10
Readiness and training	3.70	1.27	8	3.41	0.96	12
Escalating issues	3.80	1.12	7	3.59	0.85	11
Respondents number (N)	25			20		
Kendall (W)	0.433			0.532		
Spearman's Rho	-			0.929		

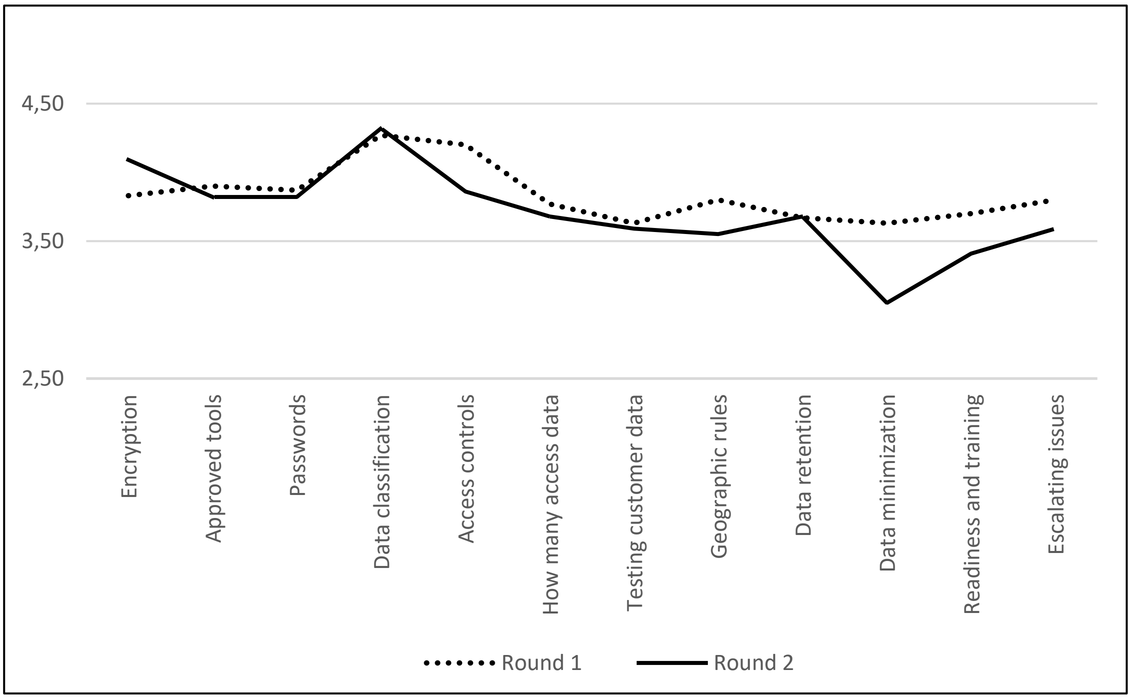
Phase II – Delphi method

In terms of analysis of the Delphi method we use a set of measures of tendency, dispersion, association and non-parametric statistics as proposed by several Delphi researchers (Okoli & Pawlowski, 2004; Paré, et al., 2013; Schmidt, 1997). We also performed a consensus measurement to assure through a wide and acceptable range of measures not only the group consensus but also the stability of the answers.

In the first round, 25 experts completed the survey. The most important factors ranked were Data classification and Access controls (AVG rank > 4). The highest standard deviation reached was 1.27 in Readiness and training's factor, which indicates a lack of consensus among experts. In general, the factors presented high standard deviations, which explain the Kendall's W of 0,433, indicating a poor degree of consensus (Schmidt, 1997). Hence, we conducted a second round (Table 1) to improve the level of concordance among experts. A total of 20 usable answers were received. In terms of concordance, the Kendall's W increased to 0.532, which represents an acceptable degree of consensus. Nonetheless, the Data classification factor maintained the first position in terms of average rank, followed by now by Encryption. Regarding dispersion, Testing customer data registered the highest standard deviation (SD = 1.01). At this time, we assessed our chances of continuing the study, since the panelists were not inclined to continue the exercise and a moderate level of consensus had already been reached. Before deciding to terminate the study, we assessed the stability of the results by examining the measures of central tendency (such as the average ranking between rounds), dispersion (standard deviations) association and group comparison between rounds.

By analyzing the average ranking differences between both rounds, we were able to conclude that there was a degree of stability between rounds. We calculated measures of dispersion for the rank scores. To determine whether any Data Protection factors were particularly controversial, we examined the standard deviations to provide a more precise way to measure rank score consensus (Figure 1). The standard deviation of the rank scores represents the average of the differences between experts' scores and the group's average score. Standards deviations should decrease between rounds. To achieve a perfect consensus, standard deviations should be zero. Table 1 shows how the standard deviations changed over the ranking rounds. Overall the majority of factors reduced their dispersion across the rounds. As shown in Table 1, standard deviations were between 0.64 and 1.27. The major dispersion is observed in the last factors ranked by experts. We believe that this dispersion is due to the sample. The

Figure 1. Average ranking differences between ranking rounds



last factors are operational factors which our experts were not so familiar with. Overall, this dispersion analysis suggests that the ranking of factors is not controversial and that the level of consensus achieved is usual.

To finalize the consensus measurement we have applied association measures (Nie, Bent, & Hull, 1975). We chose to use Spearman's rank-order correlation coefficient (Spearman's rho), in order to measure whether consensus was being achieved, or otherwise, between rounds. A coefficient of 0.929 was obtained, meaning we achieved a high degree of consensus. Table 3 shows that mean rankings and standard deviations are relatively stable, as the rank position did not change significantly between rounds. Therefore, we believe that these small differences do not affect the results of the study and we decided to complete the study at this point.

In addition, we performed a complementary analysis to understand the evolution of the factors position between the rounds as followed by several authors (Okoli & Pawlowski, 2004; Paré, et al., 2013; Schmidt, 1997). It can evidenced that 6 groups of factors arise from the 12 factors. Taking in consideration the top factor (Data classification) which was ranked as the most important factor in both rounds, we can conclude that this factor by itself represent the first group which is associated with the fundamentals of data privacy (Hui, et al., 2007). Factor 1 - Data classification, is the first step that ICTs must take to ensure data privacy by categorizing customer data accordingly. That is, customer data needs to first be classified into one of these three categories: i) High Business Impact (HBI), ii) Medium Business Impact (MBI), and iii) Low Business Impact (LBI).

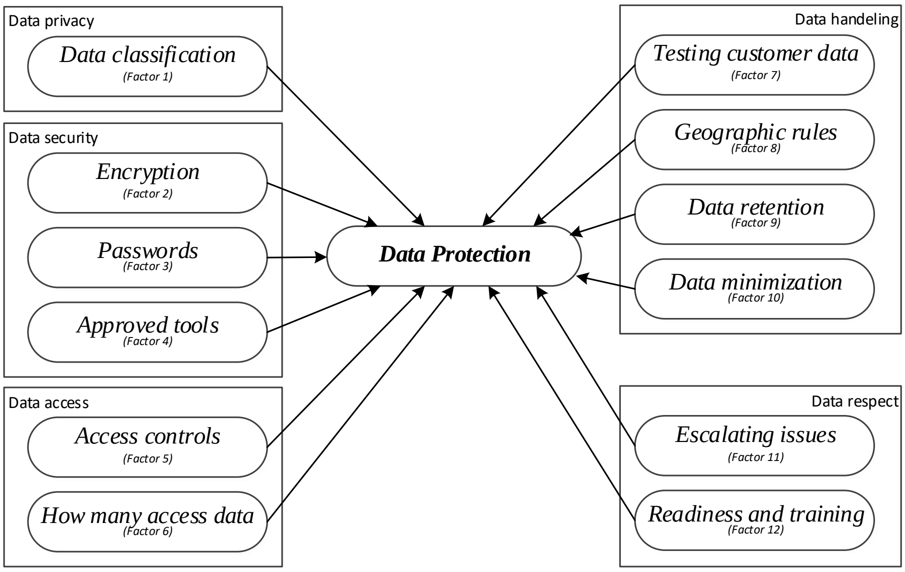
By observing the second group of 3 factors in the third round, we can conclude this set of factors are associated with data security (Bélanger, et al., 2002). After classify customer data it is important to protect customer data by following these security requirements: Factor 2 - Encryption, is one of the most important steps that ICTs personal can take when protecting customer's data. Factor 3 - Passwords. Always follow password protection best practices, and Factor 4 - Approved tools. Use only ICT services-approved tools for the collection and storage of customer data.

A third group of 2 factors is noted to data access (Slyke, et al., 2006). After ensuring data classification and encryption it is important to define how and who access to customer data by following these requirements: Factor 5 - Access controls. Define the appropriate controls to have when accessing customer data, and Factor 6 - How many access data. Define how many people can be accessing customer data.

Another group (the fourth) of 3 factors is noticed associated to data handling (Skinner, et al., 2006) particular important for support and services ICT teams consider four additional rules when handling customer data: Factor 7 - Testing customer data. Testing customer data only in test environment and only for the purpose of troubleshooting. Factor 8 - Geographic rules. Consider geographic location when transferring data. Factor 9 - Data retention. ICT personal must always consider data retention timelines when storing data, and Factor 10 - Data minimization. Only collect the customer data that is strictly needed to complete the task.

The remaining group (the fifth) of two factors is interconnected with data respect (Frye & Dornischa, 2010). Data protection demands the obligations to ICT personal put in place in their everyday live in order to respect the privacy rights of customers by following these requirements: Factor 11 - Escalating issues, ICT personal is likely to engage customers every day that may require to access, collect, or manage customers' personal information, and Factor 12 - Readiness and training. When preparing readiness and trainings, ITCs must use approved generic company names and always use dummy data. Having said this, the answer to our research question "on what are the critical factors and their importance on which ICTs professionals in support and services roles should follow in their daily tasks in order to ensure customer's data protection?" is systematized in Figure 2.

Figure 2. The 12 critical success factors for data protection in ICT services and support roles



These 12 critical success factors are grouped into five groups of data protection domain and their importance is ranked from factor 1 to 12. Non-compliance with the 12 factors, exposes ICTs to compromise of systems, disruption of services, and non-compliance with regulatory requirements (as defined in section 2). The result of which can lead to financial and legal penalties to ICT firms. In contrary, by implement these factors to protecting customer's data, ICTs firms build trust and loyalty (Bélanger & Crossler, 2011; Dinev, et al., 2013; Hong & Thong, 2013; Smith, et al., 2011). Moreover the set of these grouped factors provides a framework that can serve as a benchmark for organizations. For that reason it was not our intention to reduce the set of factors but to validate and rank them.

CONCLUSIONS, LIMITATIONS AND FUTURE RESEARCH OPPORTUNITIES

Data protection concerns is an area of study that is receiving increased attention due to the huge amount of enterprise and personal information being gathered, stored, transmitted, and handled by services and support professionals. Although still few literature, the current understanding of data protection is largely fragmented (Pavlou, 2011). The existing literature shows that there is a lack of empirical research about data protection discipline-dependent on services and support professionals amongst ICT firms. This exploratory research has made a first attempt. To the best of our knowledge, this is the first methodological grounded study that answer to which are the critical success factors and their importance that service and support professionals should follow in their daily tasks to ensure customer data protection.

Unlike conventional research, we combined the traditional interview and Delphi methodologies into two phases. Whereas traditional interviews surveys identify ‘‘what is,’’ Delphi address ‘‘importance’’(Paré, et al., 2013).

The results of this empirical-qualitative research greatly complement the norms ISO 27001, EU clause and HIPPA , through real-life examples, scenarios and expertise, as well as adding a field study to the IS literature into the non-common perspective of the ITC's point of view.

The analysis of the results lead us to identify and rank the importance of 12 factors: first ICT personal must ensure 1) Data classification (with three categories LBI, MBI and HBI), then use 2) Encryption security tools, 3) Password protection, 4) Approved tools, 5) Access controls, 6) How many access data, 7) Testing customer data, 8) Geographic rules, 9) Data retention, 10) Data minimization, 11) Escalating issues, and 12) Readiness and training.

This paper also present the categorization of these 12 factors into 5 groups: whereas Data classification is the main piece of data privacy (group 1), Encryption, Passwords, and Approved tools are pieces of data security (group 2). While Access controls, and How many access data are the main pieces for data access (group 3), Testing customer data, Geographic rules, Data retention, and Data minimization are the main pieces to data handling (group 4). Lastly the data respect (group 5) is mainly composed by Escalation issues, and Readiness and Training factors.

The overall conclusion is that, beyond security and privacy, data protection is at the core of ICT business (Pavlou, 2011), and therefore is everyone's responsibility, however is a process that services and support professionals much embed in their roles. Their daily actions greatly impact on their firm's trustworthiness and reputation.

These 12 recommendation have not been confirmed in an end-customer context. Therefore a future work would be to develop an empirical-quantitative research (Ruivo, Oliveira, Johansson, & Neto, 2013; Ruivo, Oliveira, & Neto, 2012, 2014) base on the proposed framework presented above, with the aim of validating these factors from the costumer's perspective.

In order for support and services professionals to uphold and maintain customer trust and protect ICTs firms' reputation, all data protection incidents must be reported, handled, and brought to a resolution as quickly as possible. Data protection incidents include the exposure, breach or theft of customer or personal data, unauthorized access or use of customer or personal data, the threat of a lawsuit, or press contact, or a regulatory inquiry. This calls also for further study.

In a complementary perspective, social media websites and applications have emerged as an important source for personal and business networking. They connect with business associates, customers, friends, family, and even complete strangers based on interests, hobbies, and affiliations. Because of the design of many of these sites, personal and business networks often intersect, so it's important to always be careful about how ICT professionals interact with them. More precisely, ICT professionals should not assume their work and contributions to social/professional networking sites are private. Even if they employ data protection settings (such these 12 identified in this research), friends or followers can forward items and make them public which can have a detrimental impact on the reputation, professional status and employment prospects of ICT professionals. Hence, we welcome further research on this matter.

REFERENCES

Acquisti, A., & Grossklags, J. (2005). Privacy and Rationality in Individual Decision Making. *IEEE Security & Privacy, 3*(1), 26-33.

Akkermans, H. A., Bogerd, P., Yücesan, E., & Van Wassenhove, L. N. (2003). The impact of ERP on supply chain management: Exploratory findings from a European Delphi study. *European Journal Of Operational Research, 146*(2), 284-301.

Amatruda, R. (2013). Worldwide Data Protection and Recovery Software 2013–2017 Forecast and 2012 Vendor Shares. *IDC*.

Arend, C. (2013). MarketScape: European Data Protection Software 2012 Vendor Analysis. *IDC*.

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly 30*(1), 13-28.

Bansal, G., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity privacy concern and trust in disclosing health information online. *Decision Support Systems, 49*(2), 138-150.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017-1041.

Bélanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *Journal of Strategic Information Systems, 11*(3), 245-270.

Casado-Lumbreras, C., Colomo-Palacios, R., Ogwueleka, F. N., & Misra, S. (2014). Software Development Outsourcing: Challenges and Opportunities in Nigeria. *Journal of Global Information Technology Management, 17*(4), 267-282.

Colomo-Palacios, R., Casado-Lumbreras, C., Soto-Acosta, P., Misra, S., & García-Peñalvo, F. J. (2012). Analyzing human resource management practices within the GSD context. *Journal of Global Information Technology Management, 15*(3), 30-54.

Colomo-Palacios, R., Leeney, M., Varajão, J., & Ribeiro, A. T. (2011). Information Systems Outsourcing in Large Companies: Evidences from 20 Ireland Companies.

International Journal of Information Technology Project Management, 2(4), 44-58.

Commission, E. (2010). Model Contracts for the transfer of personal data to third countries, from http://ec.europa.eu/justice/data-protection/index_en.htm

Cruz-Cunha, M. M., & Portela, I. M. (Eds.). (2015). *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance*. Hershey, PA, USA: IGI Global.

Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science, 10*(1), 104-115.

Daniel, E. M., & White, A. (2005). The future of inter-organisational system linkages: findings of an international Delphi study. *European Journal of Information Systems, 14*(2), 188-203.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61-80.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems, 22*(3), 295-316.

Frye, N. E., & Dornischa, M. M. (2010). When is trust not enough? The role of perceived privacy of communication tools in comfort with selfdisclosure. *Computers in Human Behavior, 26*(5), 1120–1127.

HIPAA. (1996). Understanding Health Information Privacy.

Hong, W., & Thong, J. Y. L. (2013). Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies. *MIS Quarterly, 37*(1), 275-298.

Hui, K. L., Teo, H. H., & Lee, T. S. Y. (2007). The value of privacy assurance: an exploratory field experiment. *MIS Quarterly, 31*(1), 19–33.

ISO. (2013). ISO/IEC 27001 - Information security management, from https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

Linstone, H. A., & Turoff, M. (1975). *The Delphi method: Techniques and applications* (Vol. 29): Addison-Wesley Reading, MA.

Liu, C., Marchewka, J. T., Lu, J., & Yu, C.-S. (2005). Beyond Concern-A Privacy-Trust-Behavioral Intention Model of Electronic Commerce. *Information & Management, 42*(2), 289-304.

Malhotra, N. K., Birks, D. F., Palmer, A., & Koenig-Lewis, N. (2007). Marketing Research: an applied approach. *Journal of marketing management, 27*, 1208-1213.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research, 15*(4), 336-355.

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information Privacy: Corporate Management and National Regulation. *Organization Science, 11*(1), 35-57.

Nie, N. H., Bent, D. H., & Hull, C. H. (1975). *SPSS: Statistical package for the social sciences* (Vol. 421): McGraw-Hill New York.

OECD. (2010). *OECD Information Technology Outlook 2010*: OECD Publishing.

OECD. (2012). *OECD Internet Economy Outlook 2012*: OECD Publishing.

Okazaki, S., Li, H., & Hirose, M. (2009). Consumer Privacy Concerns and Preference for Degree of Regulatory Control. *Journal of Advertising, 38*(4), 63-77.

Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: an example, design considerations and applications. *Information & Management, 42*(1), 15-29.

Paré, G., Cameron, A.-F., Poba-Nzaou, P., & Templier, M. (2013). A systematic assessment of rigor in information systems ranking-type Delphi studies. *Information & Management, 50*(5), 207-217.

Pavlou, P. A. (2011). State of the Information Privacy Literature: Where are We Now and Where Should We Go? *MIS Quarterly, 35*(4), 977-988.

Pietro, R. D., & Mancini, L. V. (2003). Security and privacy issues of handheld and wearable wireless devices. *Communications of the ACM, 46*(9), 74-79.

Poindexter, J. C., Earp, J. B., & Baumer, D. I. (2006). An experimental economics approach toward quantifying online privacy choices. *Information Information Systems Frontiers, 8*(5), 363–374.

Portela, I. M., & Cruz-Cunha, M. M. (2012). What about the Balance between Law Enforcement and Data Protection? In A. Information Resources Management (Ed.), *Cyber Crime: Concepts, Methodologies, Tools and Applications* (pp. 1548-1565). Hershey, PA, USA: IGI Global.

Ruivo, P., Oliveira, T., Johansson, B., & Neto, M. (2013). Differential effects on ERP post-adoption stages across Scandinavian and Iberian SMEs. *Journal of Global Information Management, 21*(3), 1-20.

Ruivo, P., Oliveira, T., & Neto, M. (2012). ERP use and value: Portuguese and Spanish SMEs. *Industrial Management & Data Systems, 112*(7), 1008-1025.

Ruivo, P., Oliveira, T., & Neto, M. (2014). Examine ERP post-implementation stages of use and value: Empirical evidence from Portuguese SMEs. *International Journal of Accounting Information Systems, 15*(2), 166-184.

Schmidt, R. C. (1997). Managing Delphi surveys using nonparametric statistical techniques*. *Decision Sciences, 28*(3), 763-774.

Skinner, G., Han, S., & Chang, E. (2006). An Information Privacy Taxonomy for Collaborative Environments. *Information Management & Computer Security, 14*(4), 382-394.

Slyke, C. V., Shim, J. T., Johnson, R., & Jiang, J. (2006). Concern for Information Privacy and Online Consumer Purchasing. *Journal of the Association for Information Systems, 7*(6), 415-444.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS Quarterly, 35*(4), 989-1016.

Son, J. Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: a taxonomy and a nomological model. *MIS Quarterly 32*(3), 503-529.

Stantcheva, L., & Stantchev, V. (2014). Addressing Sustainability in IT-Governance Frameworks. *International Journal of Human Capital and Information Technology Professionals (IJHCITP), 5*(4), 79-87.