Available online at www.sciencedirect.com

ScienceDirect

Procedia Technology 16 (2014) 710 – 717

Procedia Technology

CENTERIS 2014 - Conference on ENTERprise Information Systems / ProjMAN 2014 - International Conference on Project MANagement / HCIST 2014 - International Conference on Health and Social Care Information Systems and Technologies

Data protection in services and support roles – a qualitative research amongst ICT professionals

Pedro Ruivo[a]*, Vítor Santos[a], Tiago Oliveira[a]

[a]*ISEGI, Universidade Nova de Lisboa, Campus de Campolide, 1070-312 Lisbon, Portugal.*

Abstract

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 ICTs 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. This qualitative research studied which recommendations service and support professionals should follow in their daily tasks to ensure customer data protection. It present 12 recommendations: Data classification (three categories: low, medium and high business impact), Encryption security tools, Password protection, Services tools for data collection and storage, Who access data, How many access data, Testing customer data, Geographic rules, Data retention, Data minimization, Escalating issues, and Readiness and training. This paper is intended to help ICTs how to apply key data protection principles on their daily work. Provides important data protection recommendations that ICTs are expected to apply when handle customer data. By handling customer data safely, ICTs firms build trust and loyalty.

Peer-review under responsibility of the Organizing Committee of CENTERIS 2014.

Keywords: Data protection; data classification; privacy; security; ICT; support; services.

1. Introduction

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

*Corresponding author. Pedro Ruivo Tel. +351210491063
E-mail address: pruivo@isegi.unl.pt

Peer-review under responsibility of the Organizing Committee of CENTERIS 2014.
doi:10.1016/j.protcy.2014.10.020

the future of information and communications technology (ICT) firms [1-3]. 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 [4,5].

Ensuring the privacy of customer information is a key driver of trust [1]. Moreover, protecting privacy is required by law, and it helps ICTs firms avoiding fines and regulatory actions [6,7]. Customers' trust is win by making sure that their information is collected, used, and stored with the utmost care and respect. As more and more ICTs firms are evolving from a purely focus on software and communications to services providers, privacy and security are critical factors in winning customer trust and data protection is the root [8-10].

Reputable ICTs firms such as Microsoft, SAP, Portugal Telecom, ONI-Communications and Vodafone have built a strong foundation of privacy and security practices [11]. The past decade has brought immense changes in technology, requiring ICTs firms to continually evolve and reaffirm their commitment to trustworthy computing. Hence is a must to continue to meet privacy demands to meet regulations, customer expectations, and consumer perceptions [9,12]. Instead of solely studying situations handled by privacy or security professionals this paper target situations what professional services face every day in their roles filling a gap in the literature [9].

2. The fundamentals of data protection

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 [5,8,13,14]. 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 [1,15,16]. 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 [17-20]. 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) [8,16]. 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 [1,3,9,12].

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 [3,12,13,16]. 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 [14,21-23].

Although very few, there are some norms around the protection of customer data: I) ISO 27001 [24] 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 model clauses [25] 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) [26] business associate agreements, are contractual obligations that ICTs are required to sign with customers to do business in the US market.

This paper aims to systematize the above norms and industry practices to meet commitments on data protection in ICTs business. In order to protect customer data appropriately, it is essential to know what type of data is been handled and the first step in protecting data is to classify the data.

3. Methodology and Results

Value propositions can be identified either through a literature review or by exploratory interviews. This work focusses on exploratory interviews. The research approach refers to the structure and the explanations from Malhotra and Brigs [27]. Supported on the existing literature in the field of data privacy and security, which is still at the

beginning, the research method chosen was 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.

An inductive approach was used and the data analysis method selected was the "content matrix analysis" [27], particularly suitable for the exploratory phase of a research because it represents a key instrument in the creation of appropriate factors.

The face-to-face interviews were conducted between September 9th and November 15th 2013. Each lasted approximately 20 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 [28,29] and OECD [11,30].

In short we followed five steps in the analysis of the interviews: 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 final outcome from the analysis resulted that customer data needs to first be classified into one of these three categories of security designations:

1) 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.

2) 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.

3) 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

4. Analysis and recommendations

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.

Recommendation 1 - Data classification, is the first step that ICTs must take to ensure security and so forth privacy by categorizing customer data accordingly.

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.

Accordingly with all interviewed experts – after classify customer data it is important to protect customer data by following these data handling requirements:

Recommendation 2 - Encryption, is one of the most important steps that ICTs personal can take when protecting customer's data. 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.

Recommendation 3 - Passwords. Always follow password protection best practices. 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.

Recommendation 4 - Approved tools. Use only ICT services-approved tools for the collection and storage of customer data. Using only approved tools ensures 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.

Accordingly with all interviewed experts – after ensuring customer data protection it is important to define how and who access to customer data by following these requirements:

Recommendation 5 - Access controls. Define the appropriate controls to have when accessing customer data. 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.

Recommendation 6 - How many access to customer data. Define how many people can be accessing customer 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.

Moreover accordingly with all interviewed experts it is important (mainly for support and services ICT teams) consider four additional rules when handling customer data:

Recommendation 7 - 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.

Recommendation 8 - Geographic rules. Consider geographic location when transferring data – data should not be sent between countries without checking with the customer and legal representatives.

Recommendation 9 - Data retention. ICT personal must always consider data retention timelines when storing data - 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.

Recommendation 10 - Data minimization. Only collect the customer data that is strictly needed to complete the task. Only collect data that actually is going to be used to support customers.

The above recommendations about data classification, data protection and handling are the privacy principles defined by these 17 experts that ICT personal must take into account in daily work. Next follows the expert's recommendations about the obligations that ICT personal have put in place in order to respect the privacy rights of customers.

Recommendation 11 - Escalating issues, ICT personal is likely to engage customers every day that may require to access, collect, or manage customers' personal information. 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.

Recommendation 12 - 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. When preparing trainings, use approved generic company names and always use dummy data.

Non-compliance with the above 12 recommendations systematized in Fig.1, exposes ICTs to compromise of systems, disruption of services, and non-compliance with regulatory requirements (above four norms defined in section 2). The result of which can lead to financial and legal penalties to ICT firms. In contrary, by protecting data ICTs firms build trust and loyalty [3,8,12,16].

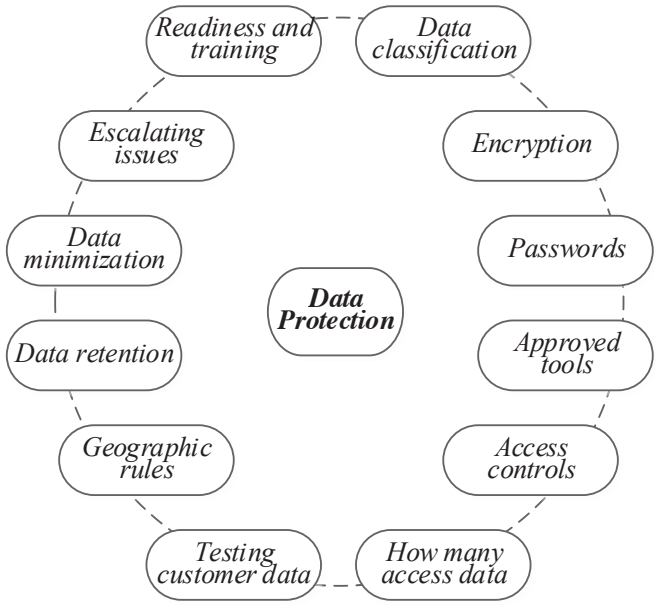

Fig.1 – Experts framework/recommendations for data protection in services and support roles

5. Conclusion, Limitations and future work

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 professional teams. Although still few literature, the current understanding of data protection is largely fragmented. The existing literature shows that there is a lack of empirical research about data protection discipline-dependent on services and support teams amongst ICT firms. From research perspective, this exploratory research has made a first attempt. To the best of our knowledge, there is the first methodological grounded research that studied which recommendations service and support professionals should follow in their daily tasks to ensure customer data protection. The overall conclusion is that accordingly with the ICTs experts, data protection is the main piece of privacy and therefore is everyone's responsibility, however is a process that services and support teams much embed in their roles. Their daily actions greatly impact on their firm's trustworthiness and reputation. Hence, customer data must be classified and encrypted. Controls must be in place to prevent unauthorized access to data. They should never underestimate the sensitivity of "back end" data like server logs and IP addresses. Must enable encryption security tools on all devices, and know where customer data is stored and how it is secured.

Although through different paths, the results obtained are partly convergent with ISO 27001 [24], EU clause [25] and HIPPA [26]. The results this empirical-qualitative research greatly complement these norms through real-life examples and scenarios as well as adding a field study to the IS literature into the non-common perspective of the ITC's point of view. Hence, this paper present 12 recommendations that is : 1) Data classification (with three categories LBI, MBI and HBI), 2) Encryption security tools, 3) Password protection, 4) Services tools for data collection and storage, 5) Who access data, 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.

These 12 recommendation have not been confirmed in an end-customer context. Therefore a future work would be to develop an empirical-quantitative research [31-33] base on the proposed framework presented above, with the aim of validating suggested expert recommendations 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. Hence, we welcome further research on this matter.

References

[1] Bansal G, Zahedi FM, Gefen D. The impact of personal dispositions on information sensitivity privacy concern and trust in disclosing health information online. Decision Support Systems 2010;49(2):138–50.
[2] Frye NE, Dornischa MM. When is trust not enough? The role of perceived privacy of communication tools in comfort with selfdisclosure. Computers in Human Behavior 2010;26(5):1120–7.
[3] Dinev T, Xu H, Smith JH, Hart P. Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. European Journal of Information Systems 2013;22(3):295–316.
[4] Liu C, Marchewka JT, Lu J, Yu C-S. Beyond Concern-A Privacy-Trust-Behavioral Intention Model of Electronic Commerce. Information & Management 2005;42(2):289-304.
[5] Culnan MJ, Armstrong PK. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. Organization Science 1999;10(1):104-15.
[6] Milberg SJ, Smith HJ, Burke SJ. Information Privacy: Corporate Management and National Regulation. Organization Science 2000;11(1):35-57.
[7] Okazaki S, Li H, M.Hirose. Consumer Privacy Concerns and Preference for Degree of Regulatory Control. Journal of Advertising 2009;38(4):63-77.
[8] Bélanger F, Crossler RE. Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. MIS Quarterly 2011;35(4):1017-41.
[9] Pavlou PA. State of the Information Privacy Literature: Where are We Now and Where Should We Go? MIS Quarterly 2011;35(4):977-88.
[10] Slyke CV, Shim JT, Johnson R, Jiang J. Concern for Information Privacy and Online Consumer Purchasing. Journal of the Association for Information Systems 2006;7(6):415-44.
[11] OECD. OECD Internet Economy Outlook 2012: OECD Publishing; 2012.
[12] Hong W, L.Thong JY. Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies. MIS Quarterly 2013;37(1):275-98.
[13] Dinev T, Hart P. An Extended Privacy Calculus Model for E-Commerce Transactions. Information Systems Research 2006;17(1):61-80.
[14] Bélanger F, Hiller JS, Smith WJ. Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes. Journal of Strategic Information Systems 2002;11(3):245-70.
[15] Malhotra NK, Kim SS, Agarwal J. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. Information Systems Research 2004;15(4):336-55.
[16] Smith HJ, Dinev T, Xu H. Information privacy research: an interdisciplinary review. MIS Quarterly 2011;35(4):989-1015.
[17] Poindexter JC, Earp JB, Baumer DI. An experimental economics approach toward quantifying online privacy choices. Information Information Systems Frontiers 2006;8(5):363–74.
[18] Hui KL, Teo HH, Lee TSY. The value of privacy assurance: an exploratory field experiment. MIS Quarterly 2007;31(1):19–33.
[19] Son JY, Kim SS. Internet users' information privacy-protective responses: a taxonomy and a nomological model. MIS Quarterly 2008;32(3):503-29.
[20] Awad NF, Krishnan MS. The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. MIS Quarterly 2006;30(1):13-28.
[21] Pietro RD, Mancini LV. Security and privacy issues of handheld and wearable wireless devices. Communications of the ACM 2003;46(9):74-9.
[22] Acquisti A, Grossklags J. Privacy and Rationality in Individual Decision Making. IEEE Security & Privacy 2005;3(1):26-33.
[23] Skinner G, Han S, Chang E. An Information Privacy Taxonomy for Collaborative Environments. Information Management & Computer Security 2006;14(4):382-94.

[24] ISO. ISO/IEC 27001 - Information security management; 2013; Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en.
[25] Commission E. Model Contracts for the transfer of personal data to third countries; 2010; Available from: http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm.
[26] HIPAA. Understanding Health Information Privacy. 1996.
[27] Malhotra N, Birks D. Marketing Research: An Applied Approach. 3rd ed. Edinburg: Financial Times Press; 2007.
[28] Amatruda R. Worldwide Data Protection and Recovery Software 2013–2017 Forecast and 2012 Vendor Shares. IDC 2013.
[29] Arend C. MarketScape: European Data Protection Software 2012 Vendor Analysis. IDC 2013.
[30] OECD. OECD Information Technology Outlook 2010: OECD Publishing; 2010.
[31] Ruivo P, Oliveira T, Neto M. Examine ERP post-implementation stages of use and value: Empirical evidence from Portuguese SMEs. International Journal of Accounting Information Systems 2014;*15*(2):166-84.
[32] Ruivo P, Oliveira T, Johansson B, Neto M. Differential effects on ERP post-adoption stages across Scandinavian and Iberian SMEs. Journal of Global Information Management 2013;21(3):1-20.
[33] Ruivo P, Oliveira T, Neto M. ERP use and value: Portuguese and Spanish SMEs. Industrial Management & Data Systems 2012;112(7):1008-25.