Information and Knowledge Management
ISSN 2224-5758 (Paper) ISSN 2224-896X (Online)
Vol.10, No.7, 2020

Improving Cybersecurity: Factoring User Privacy and Security Concerns Into E-Service Product Design in an E-Government System

Azaabi Cletus
St. John Boscos College of Education, P.O Box 11, Navrongo, Ghana.
Email: cleinhim@yahoo.com

Aluze-Ele Simon Hilary Ayindenaba
St. John Boscos College of Education, P.O Box 11, Navrongo, Ghana.
Email: aluzeesh@hotmail.com2

Abstract
The adoption and provision of e-services in e-governance systems is on the increase. However, the privacy and security expectations of users (citizens) are not always factored into the design and development of the product or service leading to reduced acceptability, reduced trust and unfavorable attitudes of the users towards the products or services. The objective of the study was to explore this phenomenon in detail and to suggest a Participatory-Based Approach in e-service product development that solicits user experiences into the development of the electronic product or service. A qualitative Research Method was adopted using semi-structured interviews with five (5) departments in Ghana offering e-services to the citizenry. The data gathered was analyzed using grounded theory to ascertain the level of involvement of user expectations in the security and privacy aspect of e-service product development. The results showed that e-product development is a multi-stakeholder project and has an effect on e-product development, user privacy and security expectations is passively considered and with variety of challenges in actively infusing and actively involving users in e-product development. Based on the results, a Participatory-Based Approach was proposed for adoption by the e-government system owners to include users and their expectation in the development of e-service products to ensure improved security and privacy culture among all stakeholders in the E-service value chain in E-governance systems.
Key words: usability, E-service, Privacy, Security.

DOI: 10.7176/IKM/10-7-09
Publication date: October 31st 2020

1.0 Introduction

The growth and expansion of technology in general and the internet in particular is in ascendancy [1] . This has led to a massive adoption of technology in the provision of services due to its efficiency, effectiveness, cost reductions and others [2]. According to [1], over half of the world population is currently online and of this number, 51.2% representing, 3.9 million people are using the internet. Even though this is a monumental step towards global cyber-inclusiveness, it also poses a security threat to the users of this online services, who are usually vulnerable to cyber exploitation [3].

The provision of government services and information in electronic form to citizens and other relevant stakeholders known as E-government has become the new modus operandi in the digital revolution [4, 5]. It plays a complementary role to the traditional government activities and provides flexible services, 24/7 presence, interactivity, among others.

E-service systems owners, realizing the ubiquity of the users (citizen) of the internet, have developed e-services and products for the citizens with its attendant problems of security and privacy of users. However, many of these products and services do not incorporate the user security and privacy expectation into the development of the products [6, 2, 7,8].

A lot of calls have been made to developers of e-service products and services to involve user experience in privacy and security design [9, 10]. This call is necessitated by the fact that, it will foster value for the product, increase acceptability and to prevent user resistance to the service provided. [8] opined that, user involvement could be consultative, informative and or participative (figure 1) and that user involvement has the advantage of leading to system acceptance, user understanding and increased participation.

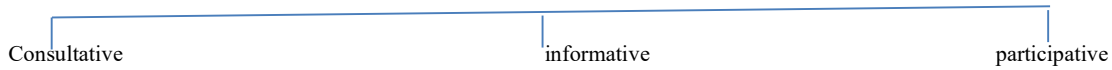

Figure1. How users are involved

Notwithstanding the fact that privacy and security issues have been highlighted in the development and delivery of e-services, little is done in engaging users and including their expectations in the security and privacy design of the services [11, 12]. This often leads to the development of e-services that do not capture the needed security and privacy issues of users. Thus, the study sought to explore the phenomenon of user involvement in the privacy and security aspect of the e-service or product development.

To be able to effectively explore this phenomenon in detail and solve the problem, the researcher asked a broad question, "Are user privacy and security expectations factored into the design and development of E-service products and services?" This broad question was broken down into three sub research questions as follows:

a. To what extend are stakeholders involved in the design and development of e-service/product?
b. How are user security and privacy expectations captured and infused into the design and development of e-service/product?
c. Why are user security and privacy concerns not explicitly obtained and infused into the design and development of e-products/services?

The rest of the study is structured as follows; section 2 is the methodology, section 3 is the results of the study, section 4 is the discussion of the study, whiles section 5 is the policy proposal, section 6 is the conclusion of the study and finally, the references are in section 7.

2. Methodology

In an attempt to address the problem and the research questions posed, the researcher adopted an exploratory qualitative research, which is an approach focused on a specific case of a department offering e-services. The idea behind qualitative research is to gain experience into the construction of reality; abstracting the world as it is seen or felt or experienced and or interpreted by the people in their daily lives [13]. We concentrated on five (5) departments offering e-services to the citizens of Ghana using a case study research. A case study is a detail study of a situation and it is used to evaluate the veracity or authenticity of an issue[3, 14]. It involves detailed study and analysis of a particular object or an occurrence such as an individual, a system, an entity or a group. [15] contends that, it is ideal in using the "falsification" test, i.e. if one of the observed phenomenon does not fit with the proposition, it is not considered for generalizations. Notwithstanding the fact, that the phenomenon under study is not usually under the control of the researcher, the case study strategy provides relevant knowledge and insights about a given phenomenon in real-life context [16]. It provides an in-depth understanding of a case and the interaction between the case and the phenomenon [17]. The sources of data used in case study research are documents, observations and the use of interviews to get a deeper understanding of the case under study. Thus the approach was consequently adopted and sample selected for the study.

2.1 Sampling and Sampling Technique

Data gathered in the qualitative domain are usually extensive; the need to be deciphered [18]. A number of methods can be used to gather data for a qualitative study including non- probabilistic sampling technique i.e. purposive, snowballing, theory-based, criterion-based, random, triangulation and mixed sampling methods [19,20]. The probabilistic methods such as random sampling and its variants and others are used in the quantitative settings.

This study used the purposive sampling technique which is one of the non-probabilistic methods used in selecting a population for a study. Five heads of departments who are involved in the development and creating the e-service products and services were chosen. Purposive sampling is where the researcher chooses a sample because of the characteristics of that sample [21]. Based on this, heads of e-service products of these departments were chosen and included in the study. The participants were chosen because they all possessed both intrinsic and extrinsic knowledge about the phenomenon under study; they were actively involved and leading the teams that design and develop e-products and services for the public in the E-governance systems and hence were recruited for the interview process.

2.2 Conducting the Interview

Questionnaires can be used in both quantitative and qualitative settings. However, interviews are the most dominant tool in qualitative research [22]. They stated that it is used to obtain research related data mainly about

attitudes, opinions, motivations and knowledge of people. Interview can be structured, semi-structured, and open-ended and or closed ended. We adopted the semi-structured by asking general questions and narrowing it to specifics of interest also known as the Funnel method. [23]. We used semi-structured interviews based on a compact list of three fairly generic themes covering the three research questions. We adopted this method because of its flexibility, ability to gain in-depth knowledge and ability to focus on a specific area. Participants were asked to fill a biodata form to enable us obtain demographic features such as gender, age, job specifications etc. We asked general questions which involved work experiences and then narrowed down to the specific broad themes of our study research questions on how an e-service product is developed; inception of the idea, stakeholder involvement in the entire process. We asked how requirements are gathered and who are involved during the requirements gathering stage and why? We asked whether user security and privacy expectations are factored into the design and development and whether user security satisfaction was considered important and finally whether there are privacy and security challenges during the design and development of e-service products and services.

The interviews were conducted remotely using zoom and face-to-face interviews and was recorded and later on transcribed. To ascertain the veracity, reliability and the validity of our interview items, a focus group pilot study was carried out using two experts in e-product design and development. This made us to spot errors and mismatches in our tool a priori before the main full scale interviews were conducted.

2.3 Data Analysis

Data analysis process in qualitative study included, data reduction, data display and drawing conclusion. The form of analysis usually adopted for the qualitative researcher is basically content analysis [13]. He opined that the aim is to extract meaning from what the respondent have said and this can be done using the intuitive or holistic-intuitive in which the researcher immerses himself or herself in the data gathered by reading the entire recording of the interview repeatedly to decipher the real meaning of the respondent. On the contrary, another method is that, the entire recorded data is broken down into smaller statement units (deconstruction) also called atomistic logical approach. These units are later recombined by meaning and thematic headings (Reconstruction). For the purpose of this study, we adopted both approaches to analyze the data. The interview responses were transcribed adopting grounded theory and making use of the procedure proposed by [24]). The interview and the analysis were both carried out by the researchers during their regular meetings where holistic–intuitive and atomistic logical approaches were used. The results from it were compared, reviewed and disagreements and differences ironed out and the final results written down according to themes.

2.4 Ensuring Reliability and Validity

To ensure that the findings of a qualitative research is accepted, the reliability and the validity of the study questions must be ensured [25]. [26] stated that many authors regard the findings from qualitative study as more interesting than quantitative, but the analysis of the gathered data remains a problem and that qualitative data is “an attractive mess”. Reliability of a qualitative research can be equated to stability [27]; reproducibility of the study by a qualified researcher. It is also called confirmability [8]. [29] stated that validity is same as accuracy; it truly represents the features that were set out to be studied. [27] added truthfulness to accuracy, [28] emphasized credibility while [30] added usefulness as shown in the table below:

Table 1: Reliability and validity in qualitative research studies

Property	Characteristic	Description
Reliability	Stability	The procedure could be reproduced by another researcher
	Confirmability	Another researcher would obtain similar results
Internal Validity	Accuracy	The representations of the object of study and the findings are not distorted
	Truthfulness	The project is presented without being biased by the researcher’s preconceptions
External Validity	Credibility	The findings make sense to knowledgeable Observers
	Usefulness	The practical implications of the findings are spelled out in a realistic way

Adopted from Cropley(2019)

We therefore ensured that, our study had reliability (stability and confirmabilty), internal validity (accuracy and truthfulness) and external validity (credibility and usefulness) as proposed by [13].

3. Results

The study was conducted using Administrative Department in Ghana that provides e-services to the citizenry. The identified staff who are in-charge of e-products development and deployment were chosen because they provide electronic services to the people of Ghana and are in charge of e-product development (Epayslip). The E-pay slip system was chosen because many people who take their salary from Government are all hooked up in that system, the system has led to fraud emanating from the user point of view and is susceptible to other kinds of frauds. The department has about 2000 staff and about million users (citizens). We focused on the delivering of e-pay slip because many staff are on the platform and there are reported cases of security breaches in that regard.

3.1 Stakeholder Involvement in the Development of E-Service

We found out that, the development and deployment of an e-service is a multi-stakeholder affair comprising many actors such as the system analyst, chief-Directors, programmers and key staff of the IT department. They use different development paradigms including prototyping and other agile methodologies for their product and services. It was realized that, the concentration of the stakeholders in the development of the e-service has been ease of use, functional requirements of users, legal and regulatory efforts. There were consideration of security issues with little involvement of users' expectations at this stage.

3.2 Trust, Privacy and Security Concerns of Users

All the people interviewed agreed that, trust, privacy and security of users were crucial for user acceptance of the e-product/service. They indicated that, they know what security features users need and thus, without consulting them (users), they can develop the product/service to meet their user expectations. The system has a provision for cyber training, end-end encryption and incident reporting systems but these are not explicitly known by the users.

3.2.1 Building Security Culture

We employed the participants about how they factor security and privacy issues in the development of e-service products. Our study showed that 4 people out of five think that security is mainly considered as an issue for only the technical team in the organization. One respondent indicated that, the team (technical team) knows everything and that they were responsible for security & privacy matters and thus they could take care of it.

3.4 Security and Privacy Challenges in E-service Product Development

All five participants mentioned limited budgets, lack of skills by the teams, limited time frame, lack of education, cost of internet, availability (high rate of downtime), etc. leading to project creeping or scope overruns with its resultant effects.

4. Discussion

The study was conducted to ascertain how the privacy and security expectations of users are factored into the design and development of e-products/ services using the qualitative research approach. Factoring users or their privacy and security expectations into the design and development of products is key to the success and acceptability of the product as this promotes trust and acceptability of the provided service. A product can be a service, physical product or even an idea. [31]. When a product is developed without the explicit involvement of users and or their expectations, such products fail to achieve its intended commercial purpose. This is what the study sought to explore by looking at level of stakeholders' involvement in the life cycle of an e-product.

The extend of stakeholder involvement, our results and findings indicated that, there was some level of involvement of stakeholders which is in tandem with [32]. However, the involvement was passive because the team were of the view that, the privacy and security consideration of the e-product was the preserve of the technical team and that there was no need to directly involve the real users and their expectations. This stand is counterproductive since products developed without the active involvement of the real users (stakeholders) may lead to products and services that do not meet user expectations and not achieve commercial success [33]. It may also lead to products with vulnerable security and privacy loopholes that can be exploited by cybercriminals with its adverse consequences. It stands to reason that, if security and privacy issues of users are not explicitly factored into the development of the e-product and services, it can lead to security breaches if cybercriminals adopt social engineering attacks strategies since social engineering uses more of the vulnerability inherent in users. [12, 34]. Thus, stakeholders affect decision-making process and if the user who is the ultimate beneficiary of the service is not actively involved, it can make even the product development quite cumbersome leading to failed products [35].

On whether user Security and privacy is factored into the design of e-products, the study showed that even though stakeholders held that view that, security and privacy is key in the product development to maximize acceptability and usability, they considered it as a preserve for only the technical team members; this assertion is flawed since security and privacy involves everybody who is connected to the system's value chain, and most especially the users; hence considering it as purely a technical issue to be handled and managed by only technical teams alone will lead to incomplete security with high level of vulnerability [34,]. Surface it to say that, users by nature may not know what they want until they see and use the system, thus for the tech team to suggest that, they know what user security and privacy issues are and therefore no need to actively involve the user may lead to developing products and services that have low usability, low acceptance, and in most cases, complete refusal to use the product or service. Hence user involvement is crucial in such product development to ensure user satisfaction, favorable attitudes towards the systems and high acceptability [2, 36].

On why privacy and security issues not usually factored into the design of e-products and services, our findings suggest that, a number of problem exist in the design and development of e-service including but not limited to budgeting constants, lack of skilled privacy and security experts in the e-service departments, illiteracy of users (citizens) etc. It is however worthy of note that, as a multi-stakeholder project, issues of communication among teams is bound to be a problem. This often leads to misunderstandings resulting in ineffective e-products/services. E-service project owners sometimes see security as a trivial component of the process and thus assign less resources to that effect. This has the potential to affect the development team's budget and lead to them glossing over serious functional security and privacy requirements. Again, since e-product design and development involves many groups with differing expertise, motivations and constraints, it poses a challenge to have all of them agreeing to implement the required security and privacy controls in the e-service development phases, often leading to the making of assumptions.

5. Policy proposal

Based on the results and findings of our study, it was realized that active involvement of users and or their expectations in the development of e-products is beneficial in creating useful and usable products. Hence, we proposed that security and privacy of users is key in developing e-products that have high usability, acceptability and favorable attitude of users. This can only be achieved if the real users of the products and or their expectations are actively involved using the participatory development process where the user needs and the users are actively catered for. Specifically, we propose the following:

a. The need for consideration of user security and privacy concerns to be fully integrated and fully involved in the product life cycle of e-services to ensure usability, acceptability and to reduce user resistance to e-products/service offered to the citizens.

b. Instead of few people handling the product development from start to end, there is need for diversification of skill set including security & privacy expert to be part of the life cycle of the e-services and including the users at every stage to provide their input in the language of their own.

c. There is need for education of product development teams to appreciate and infuse user cyber security and privacy expectations into the development of e-products using the mixed user involvement paradigm: informative, consultative and participative forms during the life cycle of the product。

6. Conclusion and Future Research

Our study was about the infusion of user security and privacy expectations into the design and development of e-products/services using a case study. It was concluded that e-product development is multi-stakeholder in nature and this has an impact on decision-making process. The results highlighted the need for appropriate stakeholder involvement in the entire e-product life cycle including privacy and security. we argued that, there is need for a systematic approach that is participatory in nature to harness all the expertise and skills set of all stakeholders and users in the security and privacy design and development of e-products. It was concluded that user security and privacy expectations were not explicitly and clearly factored into the design process and this leads to products that do not meet its intended commercial success due to low usability, unfavorable attitudes toward the system, cyber exploitation of security and privacy vulnerability in the products. We identified that a couple of challenges exist in the design and development of the e-services /products relative to security and privacy and that there is a need to explicitly involve users in the design and development of e-products and services to enhance user acceptability, favorable attitudes towards e-products and overall user security and privacy. Thus, while e-products will continue to dominate society due to the exponential growth in digitization and digitalization, involving and including the security and privacy and expectations of users in the development of these products will lead to secure products, and higher acceptability of these products. In future, a study on the user perception on e-service products and

services is needed to ascertain the level of users in the context of privacy, security and user data integrity and protection.

References

1. Global cybersecurity Index 2018, ITU Report 2018
2. Kenneth C. Laudon and Jane P, Laudon (2010). Management Information Systems Managing the digital firm, Pearson international. 10th Edition.
3. George Chalhoub, Ruba Abu-Salma, Ivan Flechous, Ellie Tom, and Norbert Nthala (2019). Factoring User Experience into the Security and Privacy Design of Smart Home Devices: A Case Study. CHI 2020, April 25 – 30, 2020, Honolulu, HI, USA.
4. Darrell MWest. 2004. E-Government and the Transformation of Service Delivery and Citizen Attitudes. Public Administration Review 64, 1 (2004), 15–27.
5. E-government Development index (EGDI), 2018
6. Isis Chong, Aiping Xiong, and Robert W. Robert W. Proctor. 2019. Human factors in the privacy and security of the internet of things. Ergonomics in Design 27, 3 (2019), 5–10.
7. Taherdoose, H (2017): understanding of e-service security dimentions and its effect on quality and intention to users. Information and security, vol 25 no. 5, pp535-539
8. Leela Damodaran (1996). Gehavour and Information Technology, 1996, vol15, no, 6, 363-377
9. Claire Rawland and Martin Charlier. 2015. User Experience Design for the Internet of things. O'Reilly Media.
10. Razvan Nicolescu, Michael Huth, Petar Radanliev, And David De Roure. 2018. State of The Art in IoT – Beyond Economic value. London. (2018).
11. Ka-Ping Yee, (2004). Aligning security and usability. IEEE Security and privacy
12. Joanna Mehtälä and Marko Nieminen. 2019. Combining Design Science and User-Centred Methods in M-Government Service Design in Namibia. In 31ST AUSTRALIAN CONFERENCE ON HUMAN-COMPUTER-INTERACTON (OZCHI'19), December 2-5, 2019, Fremantle, WA, Australia. ACM, New York, NY, USA, 11 pages.
13. Cropley, A. J. (2019, 2nd updated, revised, and enlarged edition). Qualitative research methods: A practice-oriented introduction for students of psychology and education. Riga, Latvia: Zinātne. (open access – doi: 10.13140/RG.2.1.3095.6888)
14. Yin, R. K. (2017). Case study research and applications: Design and methods (6th ed.). Thousand Oaks, Ca: Sage.
15. Glyvjberg, B. (2004). Five misunderstandings about case-study research. In Sale,
16. Baxter, P., Jack, S. (2008). Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. The Qualitative Report, 13(4). Retrieved September 9, 2019 from http://www.nova.edu/ssss/QR/QR13-4/baxter.pdf
17. Randolph, J. J. (2007). Multidisciplinary methods in educational technology research and development. Retrieved February 9, 2019 from http://justus.randolph.name/methods
18. Jarkko Sohunen (2009). Scientific methodology in computer science
19. Gobo, G., Gudrium, F., Silverman D. (Eds.) Qualitative Research Practice. Sage Publications
20. Miles, M. B., Huberman, A. M. (1994). Qualitative Data Analysis: An Expanded Sourcebook (2nd. Ed.). London: SAGE Publications
21. Ted Plays (2003). Research Decisions: quantitative and qualitative perspectives (3rd edition). Thomson nelson
22. Cohen, L., Manion, L., Morrison, K. (2000). Research Methods in Education (5th ed.). London: RoutledgeFalmer
23. Charles F. Cannell, Peter V. Miller, and Lois Oksenberg. 1981. Research on interviewing techniques. Sociological methodology 12 (1981), 389 – 437
24. Juliet Carbin and Anselm Strauss (2008).basic of qualitative research: techniques and procedures for developing grounded theory
25. Johnson, R.B. & Christensen, L. (2007) Quantitative, qualitative and mixed approaches. Retrieved March, 2019
26. Bryman, A. and Burgess, R. G. (Eds.). (1994). Analysing qualitative data. London: Routledge. (Overview of methods of data analysis.)
27. Altheide D.L.& Johnson JM(2011). Reflections on interpretive Adequacy in qualitative research. In N. K. Denzen&Y.S Lincoln. The SAGE Handbook.
28. Lincoln Y. S. & GUBA EG (1985). Naturalistic inquiry. New York, CA, Sage
29. Creswell, J. (2003). Research design: Qualitative, quantitative and mixed methods approaches (2nd ed.).Thousand Oaks, CA: SAGE Publications

30. Hansen EC (2006) Successful Qualitative Health Research. Maidenhead, Open University Press.
31. Kahn K.B. (2006). New product forecasting: an applied approach's,. ME. Sharp
32. Majava, J., Harkonen,J., and Haapasalo, H., (2015). The relation between stakeholders and product development drivers: practitioners, perspectives, international journal of innovation and learning, vol17,no.1.,pp59-78
33. Simula, H. (2012), management of commercialization- case studies of industrial, business-to business product innovations. Doctoral dissertation, Aalto University, department of industrial engineering and management.
34. Ron Britton, Kobi Boymgold, Rami Puzis, Asaf Shabtai(2020). Evaluating the Information Security Awareness of Smartphone Users, CHI, 2020
35. Bendjenna, H., Chare, P., and Zrour, N.E.(2012), "using multi-criteria analysis to prioritize stakeholders", journal of systems and information technology, vol.14,no3pp264-280
36. Joe Valacich and Christoph Scneider (2010). Information system today; managing in the digital world. Pearson.