Human Computer Interaction on Enterprise Information Systems

[1]Christine Sarah Anne Ashbrook
[1,2] Faculty of Science, University of Copenhagen, Kobenhavn, Denmark
[1]sarahanne_brook@aol.com

ArticleInfo
International Journal of Advanced Information and Communication Technology
(https://www.ijaict.com/journals/ijaict/ijaict_home.html)
https://doi.org/10.46532/ijaict-2020034
Received 25 May 2020; Revised form 20 July 2020; Accepted 03 October 2020; Available online 05 November 2020.

Abstract - Safety and pliability, for Enterprise Information Systems (EIS), are fundamental aspects in business. These data systems incorporate the human users with the required behaviours, experiences, and capabilities. In that regard, they have to be pliable, usable and secure. Pliability necessitates the capability to adapt and prepare to handle the perpetuating transforming conditions, which are meant to restore the complete capacity of the incidents and the attack in EIS. In this research is purpose to discuss pliability, security and the Information Systems (IS) problems in the EIS. The problem necessitates the consideration of ergonomics of efficiency, effectiveness and interactions of obligation realization, user trust and user satisfaction, including human emotions when utilizing the secured services. This paper also proposes a technique centred on the socio-technical paradigm and systems meant to model the kinds of interplays between usability, security and pliability. We provide a discussion, based on case study, meant to display the projected approach and focussing on the user-experience centred on the design structures.

Keyword - Enterprise Information Systems (EIS); Information Systems (IS); Usability; Security; Pliability.

1. Introduction

The kind of services delivered by the Information Systems (IS), have widely influenced our modern life since they play a vital role due to the advent of technology. Enterprises, organizations and individual users acknowledge this assumption as well since many security issues are evident in many services. Considered as a quality attribute, the implication of security has incredibly transformed, and the initiatives in the organizations and in the information standards have considerably adapted to this form of transition. In Information Technology (IT), these initiatives are widely centred on safeguarding the perimeter. As for the Information Systems (IS) and the prolonged enterprises, the technologies have evolved into assuring security strategies in a detailed manner. To enhance the security strategies in details, a methodological model has been proposed to operate on the creation of the member canvas of the relevance industrial stakeholders. In that case, there is a considerable necessity for novel approaches focusing on the human aspects incorporating the usability aspect to ensure the security of a system. Actually, humans run and utilized systems; however, they are more automated.

It has been showed that the human resources are presently at the cornerstone of wide-range business models and has indicated that human factors are considered as the major source of operational banking risks. Now, the research trends in usability and security have widely achieved the required attention. The researches present sophisticated human aspects that are meant to achieve security measures. Many initiatives are structured on a certain security remedies. We consider that the absence of researches on the general engineering of privacy concerns originates from the perspective of Human Computer Interaction (HCI) [1]. In this research, we provide an introduction of the first socio-technical concepts of systems as an engineering methodology. We also provide an explanation of the security, usability and pliability based on the application of the socio-technical model approach. We also provide an introduction of the socio-technical model pliability approach based on the design pattern that is centred on the experience of the users. The case analysis on the medical assumption and laboratory is utilized to effectively highlight the applications of our projected approach.

The Travistock Institute in the late 1950s formulated the aspect of socio-technical framework in the context of the labor analyses in London. The significance of cognition (communication) was handled in the context of social relations. The socio-technical frameworks focus on modelling the technical, social and human capabilities in utilizing and handling the value-added values. The socio-technical frameworks are defined as the multi-stakeholder cyber-physical frameworks, which content with the transitions and complexities in physical and cyber worlds. The socio-technical techniques can aid in the designing of the organizational processes and business structures, which also includes the technical frameworks. It is significantly acknowledged that frameworks that are advanced using the socio-technical methods are more likely to be acknowledged to the end users since they are capable of delivering the actual values to the stakeholders. There are fundamental differences between the socio-technical frameworks and the IT frameworks engineering and modelling approaches in relation to their interactions [2].

- IT frameworks modelling concentrate on the technical definition of the system components and the kind of interactions between them to effectively deliver the required services.
- The social frameworks incorporate all the human cooperation and interactions, on the cultural and social values.
- Data systems incorporate all the users' interactions with the IT frameworks, integrating their enterprises, management and implementation frameworks.
- Social-technical frameworks recommend a way of comprehending all the human interactions with the different IT frameworks, their elements, including the cooperation with other frameworks [3].

The socio-technical framework approaches are known for their interaction between the different systems, stakeholders and their enterprises, including the complete socio ecosystem, which include the physical and cyber worlds. These dimensions define the datasets based on the interactions among the different actors that include social reliance (which means that the actors depend on others to accomplish their tasks) and the data exchange (where actors transform the essential data). Many security problems come from the evident interactions between the different actors, and the accessibility of the exchanged data. In that case, the user-experience element is a fundamental concern when it comes to the analysis of security issues.

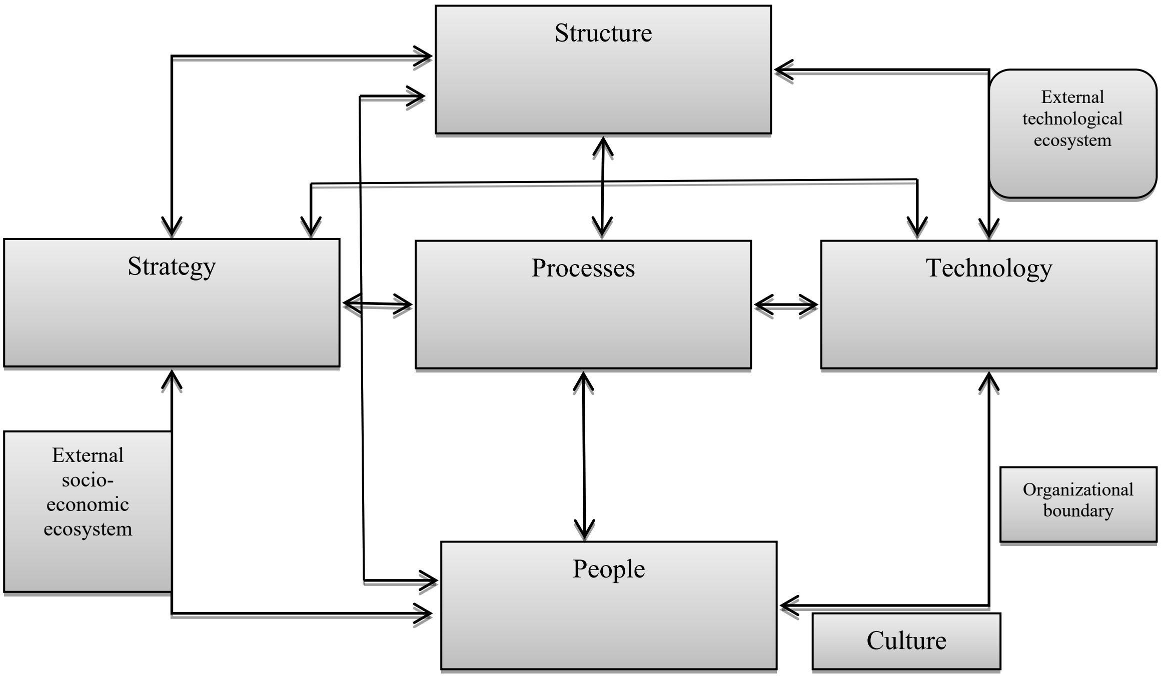

Fig 1. Socio-technical model representation

The privacy and security measures in the socio-technical frameworks include a set of automated and human agents that interact to accomplish a specific task based on the essential objectives. These have the required characters diverging and converging characters or potentially conflicting the objectives. The human emotions and other conflicting situations are transposes into the socio-technical frameworks [4]. In other terms, the system users can be animated based on their malicious intents. This happens to the hackers who identify their potential playgrounds in the socio-technical model. At the same moment, the frameworks process individual data, sensitive information and private character information. The obligations and the datasets are sensitive and significantly valuable. In the socio-technical model, privacy necessitates special attentions based on confidentiality [5]. This is one of the sole objectives of security application. Another key mandate of security is to assure the safety of users, the reliability and integrity in the processing aspect of various tasks. The challenges of security in socio-technical frameworks come from ensuring these objectives, due to two fundamental reasons:

- Remedies of security (based on constraining utility) might include the privacy vulnerability or might potentially prevent the accomplishment of the established tasks.
- The users' behaviours (unintentional and error actions) might include the security vulnerability. The human factors are the major sources of operational risks in enterprises, and the users'

trust in the socio-technical framework is fundamental.

The socio-technical frameworks expose the users to the social and technological problems. The users potentially resort to technology to handle the social problems. Usability is an element, which is dependent on the interactions among environments, tasks, systems and the potential users whereby the processes are operated in both the physical and cyber worlds [6]. The human factors are the major source of the operational risks evident in many enterprises. Note that the usability aspect is connected to the human factors. Usability is not considered a specific property of things and persons that we might evaluate by using the usability thermometer or to assess using the standardized scientific formulas. Usability issues are based on individual human elements; evaluating the attitude and behaviours captured when users finish their tasks; evaluating the capabilities of the frameworks to issue adequate conditions for undertaking the pending tasks.

The remaining part of the paper is organized as follows: Section II presents a background analysis of the research. Section III provides the socio-technical approach whereas Section IV is the analysis of the relevant case study connected to the research. Finally, Section V concludes the paper.

2. Background Analysis Of The Research

This section is meant to define the concepts of pliability and how it is applied to socio-technical frameworks, security and usability aspects, including the interplay between the two concepts.

Pliability in the Socio-Technical Models

Pliability is a fundamental concern in the modern age of business since it potentially prevents potential accidents and restores secure environments by mitigating intentional problems. Pliability, based on the concerns of accidents, is applicable in many domains such as the socio-technical model engineering. Pliability is retrieved through the capability to effectively monitor the edge conditions of the performance metrics, and its capabilities to adapt to the behaviours of operation in systems to enhance their performance [7]. Four essential functions of pliability have been defined in the past literature: avoidance (which is the capabilities to anticipate); resistance (the capacity to absorb); adaption (capabilities to reconfigure); and to recover (the capabilities to restore). Fig 2 below shows pliability, in defence, applied as an active virtue incorporated in systems and operations.

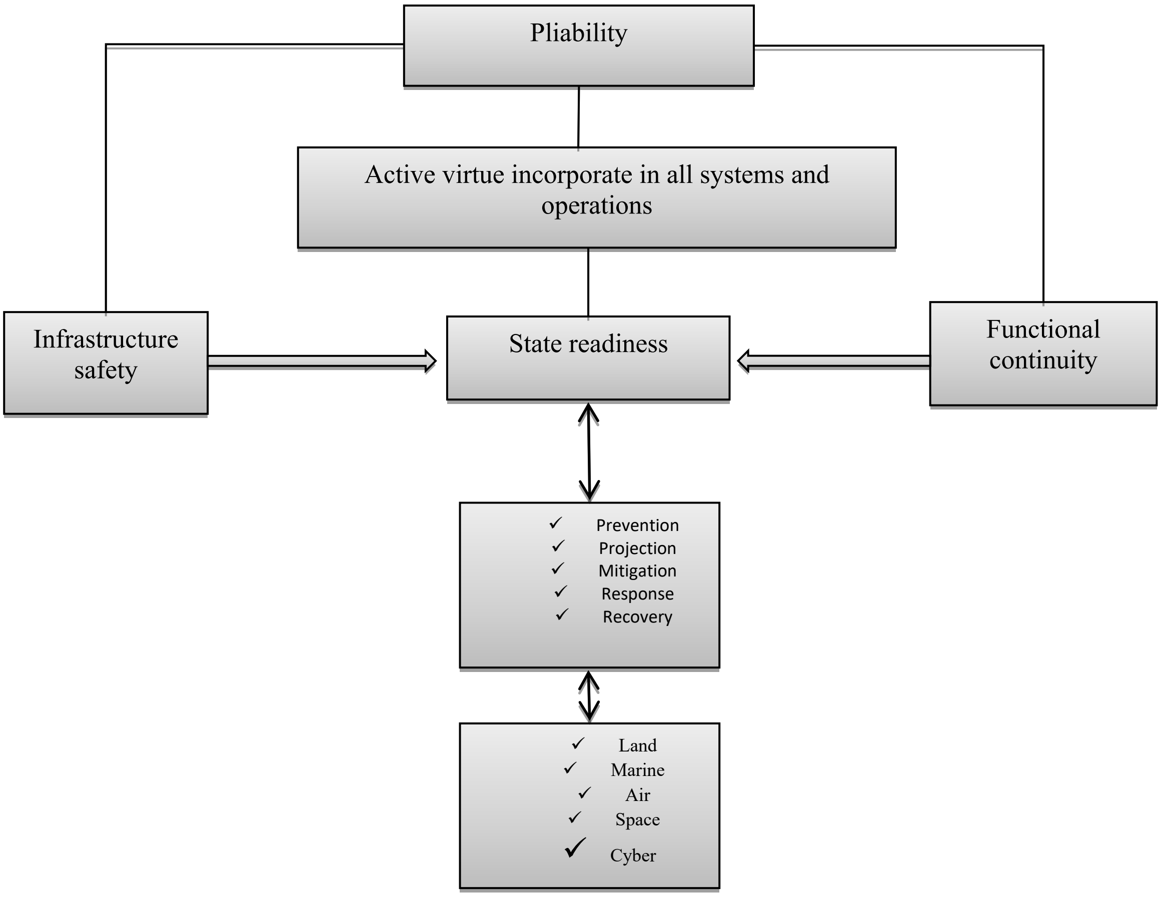

Fig 2: Pliability in the field of defense

Pliability is applicable in IT and security. In that regard, pliability is illustrated as the capability to effectively go through the potential incidents (intentional faults and unintentional accidents) and to retrieve back to the usual condition). In this aspect, we discuss pliability as the capability to adapt and prepare handling the perpetuating evolutionary conditions and to potentially restore the complete capability after an attack and accident.

Usability Systems

Up to now, many literature sources have been presented in relation to the usability studies. According to the research done by researchers, cultural aspects can be incorporated in usability studies. From the research, it is suggested that incorporating safety and flexibility to formulate comprehensive quality-of-usage system. A two-dimensional system of usability was proposed and associated to the massive number of system properties based on the activities of users. In the socio-technical model, the rhymes of usability with the absence of usability issues and the evaluation of effectiveness, satisfaction and efficiency are considered as well. Usability incorporates the ergonomic human and computer interaction quality irrespective of the forms of access media. Based on the ergonomic necessities, ISO has specifically formulated some of the standards: ISO 9241 12, which were possibly published in 1998 to define seven fundamental principles for data presentation [8]. We provide a brief definition to them:

- Clarity (which defines the kind of content displayed accurately and quickly);
- Discriminability (which is the data potentially being distinguished);
- Brevity (which is the data essential tasks being displayed);
- Consistency (the actual data presented identically on the complete application);
- Detectability (which is the data being encoded in its actual place;
- Readability (the data easy to read and comprehend); and
- Comprehensiveness (information that is understandable)

ISO 9241 110, which were published in 2006, define seven fundamental principles for the designing of the potential dialogues: task suitability, controllability, user-expectation conformity, self-descriptiveness, error tolerance, individualization suitability and the learning suitability. From the standard, three critical criteria were proposed to evaluate usability: evaluation of tasks, satisfaction of the users, and the cost of the overall usage. For the task performance, we evaluate the efficiency and effectiveness of interaction. Interactions are fundamental when users can effectively perform them successfully. The interaction is effective when the users can complete the tasks effectiveness within a specific duration of time with the usage of the acceptable resources. The users' satisfaction during the process of interaction is based on the performance of the subjective emotions and the tasks. The cost of usage considers, over to the usage of the acknowledged resources, the implication of the interaction on the safety and health of the potential users, and to the reputation integrity of the users present in the socio-technical models. The models have to adapt to the users in the predefined population, with no distinction of ethnicity, age, size, linguistic or educational level, including those with challenges with cognitive or physical operations [9]. This form of adaptation has to comply with the security measures.

Privacy and Security Models

The ISO 2700-x family of standards is dedicated to the data security aspect, which includes the organizational dimension (both the public and private companies). These standards present the manner to improve, maintain, implement and establish a management framework for data security. The standard system security based on availability, integrity and confidentiality of data are based on the application of the risks management processes. They provide the interested parties (socio-technical, operators and users systems) the required assurance that privacy risks are appropriately managed. Contrary to that, we notices the manner in which security risks are properly managed using the required harmonized procedures; secondly, we noted the three essential criteria of security, which include availability, integrity and confidentiality of data. Briefly, we develop every of the four essential points:

- The procedure includes the interested groups and their essential requirements. It also considers the dependencies and interfaces between the organizational activities and their relevant stakeholders in the extended enterprises.
- Confidentiality (data has to neither be made present nor disclosed to any unauthorized processes, entities or users.
- Integrity (information needs no modification, destroyed or altered under any unauthorized conditions).
- Availability (accessibility by an organization, authorized processes or users to the kinds of services being provided by the socio-technical frameworks, which have to be possible [10]. This also includes the operations to illegally occupy the processing timeframe, which has to be detected.

Other essential properties of the privacy of IS, such as Authenticity, Traceability and Proof is determined using certain criteria. The privacy criteria characterise the properties or constraints on the system assets, defining their privacy needs. The process provides answers, handling the organizational issues, which include legal, regulatory, branding, financial and human. Researchers define the procedure for engineering the security of EIS in seven fundamental activities based on the security act. The first two, which are the business assets and the definition of security goals to be achieved) evaluate the privacy needs on the assets of the business. Other international protocols also address the privacy and privacy risks of IS. This is the instance of the ISO 15408, which defines common criteria focussing on three essential audiences, which are users, evaluators and producers [11]. We have also identified the local norms and standards as Cramm, Ebios, Mehari and Octave. The basic approach of security remains unchanged, and incorporated to the various attributes and properties of security such as trust, privacy, authentication, identification, non-repudiation, trace and proof. In socio-technical frameworks, the attributes of Trust and Privacy undeniably link to security. According to freedom and privacy concerns for businesses in the modern age, privacy is defined as the requests for institutions, groups and individuals to determine what, how and when information concerning them can be communicated.

At this extent, every individual is continuously engaged in custom adjustment process whereby the balance for the required intimacy is achieved with the required communication and disclosure measures. Apart from that, privacy is considered a legal theme with essential issues being evaluated, since privacy disruption comes with the implementation of criminal laws. Privacy is utilized as the integrity and confidentiality of data based on privacy aspects of enterprises, groups and individuals in the community. In research, various views on security and privacy concerns are limited to a single set (which is the extent to which we identified each other and to the measure to which others have the physical accessibility to us). Privacy, considered as a control measure of data (which is over the limit of what other people known about us implies custom autonomy meaning that we can possibly control data in a more meaningful manner). The availability of respect for the privacy standards develops consumer confidence. Researchers define the aspect of trust as a psychological status incorporating the intentions to acknowledge vulnerability in reference to positive expectations of the behaviours and intentions of another. Reliability (trustworthiness from the perspective of security) illustrate the property of the model that performs the elements that are required (but not for interruption of the ecosystem, individual errors human operations and threats from hostile intruders).

Experience of Users in Socio-Technical Models

The socio-technical model approach actualizes the formulation and identification of the users' experience. A positive user-experience is normally centred on the aspect of convenience (reduced physical, timesavings and mental work), confidence (which means that the socio-technical framework operates effectively) and the ideology of usefulness. The ideology of 'operates effectively' instils and implies that trust has to be included. In reference to researchers, the users' experience considers all the usability approaches, which the incorporation of additional factors to EIS. Researches emphasize the absence of scholastic assumption on the designing of the technical remedies for IT and communication in the aspect of security and users' experience [12]. In summary, the privacy objectives are to prevent, eradicate or evaluate the attacks, faults and errors. In such occurrences, pliability aims are to outdo and tolerate the implications and to assure services in the degraded mode in reference to the service conditions of the service layer agreement. The purpose of pliability and security has to be ensured whereas maintaining positive measure of experience to the users. We consider that effective usability (positive user experience) has to promote the success of pliability and security. However, this can be considered vice versa.

3. Socio-Technical Approach

A pliable Approach on Design Patterns

In the modern age, many of the security built-in models are not usable. The users who have to utilize these models bypass the privacy devices and this condition produces the privacy gaps. The problem is to provide a replacement of the security built-in model approach using a pliable built-in socio-technical model using a design pattern. The socio-technical methodology considers the interdependencies between usability and security. In that manner, this methodology permits the adaptation facing the perpetuating evolutional utility status and the usability issues. Fig 3 shows the underlying procedures in the recommended approach. We utilize the patterns meant to illustrate the issues and remedies of usability and security issues.

There are patterns structured and considered in many human endeavours, which necessitate the combination of training and skills. In the late 1970s architecture, the identification, naming and usage of patterns was pioneered whereas operating on urban planning. In the late 1980s, computer experts operating in the field of object-oriented designed the Alexanders' works, which adapted the design patterns to specific software. It is argued that security engineering can potentially benefit from the application of the patterns, but is failing to present certain patterns meant to accomplish this mandate. The open group has also edited sources on privacy design patterns; however, it has not addressed the alignment between security and usability [13].

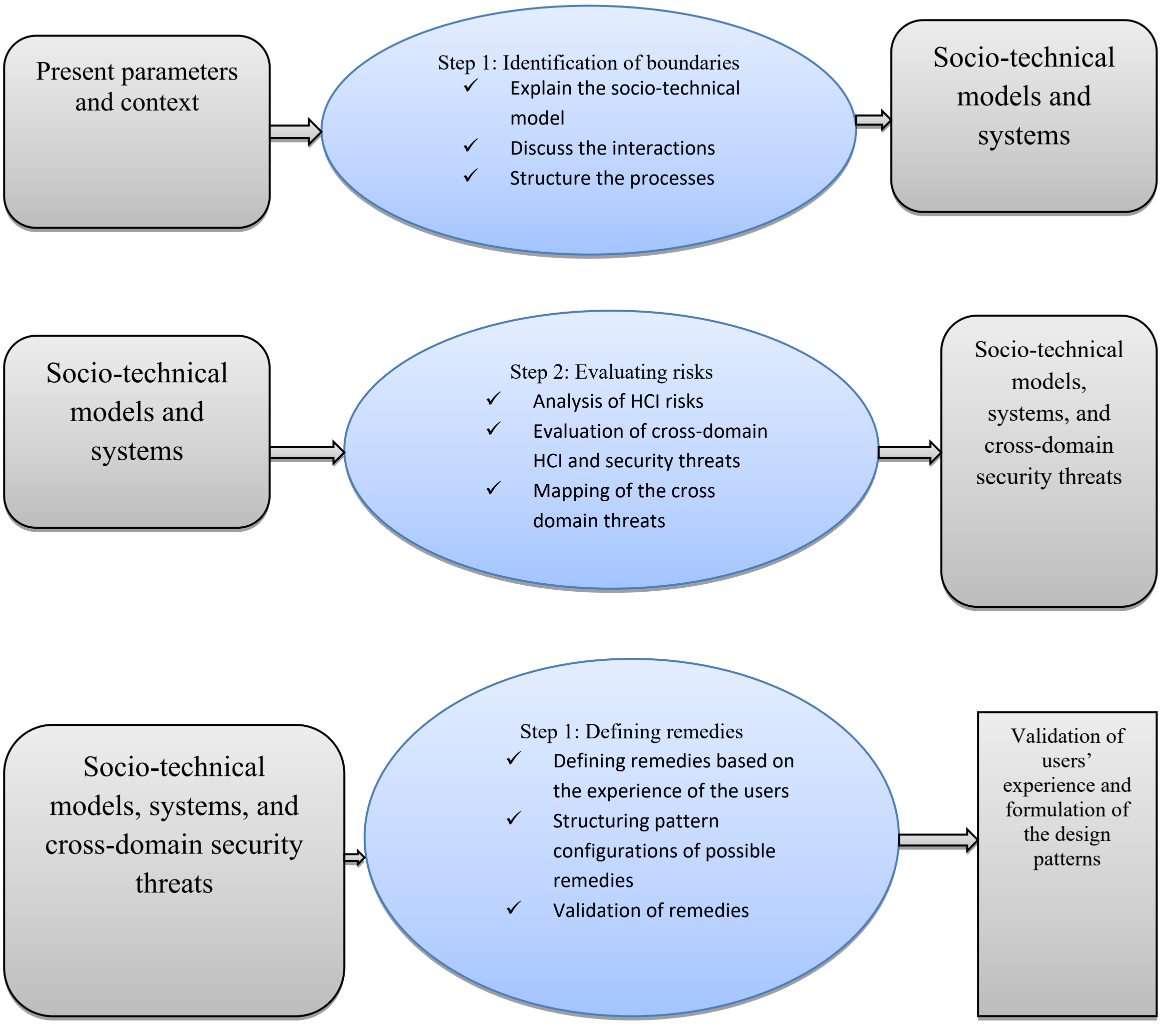
Present parameters and context
Step 1: Identification of boundaries
✓ Explain the socio-technical model
✓ Discuss the interactions
✓ Structure the processes
Socio-technical models and systems
Socio-technical models and systems
Step 2: Evaluating risks
✓ Analysis of HCI risks
✓ Evaluation of cross-domain HCI and security threats
✓ Mapping of the cross domain threats
Socio-technical models, systems, and cross-domain security threats
Socio-technical models, systems, and cross-domain security threats
Step 1: Defining remedies
✓ Defining remedies based on the experience of the users
✓ Structuring pattern configurations of possible remedies
✓ Validation of remedies
Validation of users' experience and formulation of the design patterns

Fig 3: Users' experience based on design patterns

The pliable approach on design patterns incorporates a number of stages:

Stage 1: Identification of Boundaries
In this stage, a definition of the boundaries on the environment is done, whereas incorporating the complete social ecosystems and their different actors. We effectively incorporate their interactions in both the physical and cyber worlds, based on the application of the Business Process Model Notation (BPMN) to structure the custom tasks, activities and processes done by every actor included in the process. The detailed definition of the kind of interaction between the technical elements of data systems is illustrated using the UML diagrams, which includes the use of cases. The available links between UML and BPMN diagrams (unused cases) are defined in this stage).

Stage 2: Evaluating Risks
At this stage, a list of the potential issues is recommended. We utilize the various approaches to evaluate the definition of the socio-technical model produced during the past stages incorporating cognitive walkthrough, petri nets, cross-domains and the risk analysis techniques. The risks incorporate security problems such as identity usurpation, blackmail, frauds and faults, which also incorporate the usability issues. The amount to the malfunction, denial of services and tampering with the socio-technical models [14]. The research focusses on the issue, reasons and origins, which also includes the consequences or not enhancing some aspects. This research highlights the connections of interdependence and proximity between the security or privacy and EIS. Our research utilizes a multi-domain approach of risks evaluation, and focusses on the evident human factors. Issues are documented based on the application of the storytelling technique defining the experience of the users, its potential enhancements and failures points (techniques present in literature). Issue documentation is centred on operational and learning feedback concerning other forms of incidents handling the potential risks.

Stage 3: Defining Remedies
In the last stage, we resort to the experiences of users to effectively define the remedies, which mitigate the points highlighted during Stage 2. In fact, we consider the best potential enhancement of the users' experience, which

underlies the identified points. The relevant query addressed here is "What specifically makes remedies visualized as effective or worse as a design factor, from the usable privacy point-of-view?" In that regard, it is fundamental to determine how to detect a worse design to rectify it. The actions in this stage are based on various experiments, which are based on both academic and industrial research. As mentioned earlier in this research, there are seven security standards, which constitute the engineering of data security. However, various researches have evaluated the usable privacy designs, with some of them proposing guidelines that focus on the non-trivial issues certain to the usable privacy designs; active authorization, path based on resistance, active authorization, self-awareness, revocability, trusted paths, visibility, expressiveness, identifiability, relevant boundaries and foresights. This stage incorporates the documentation of patterns following a specific format.

- Definition of the issue (category of the issues)
- Analysis of the potential remedy
- Consequences of implementing the design remedy
- Verification of the remedy

Qualitatively, the patterns have to enhance the experience of the users. The patterns have to enhance the measurable path that compromise security measures and usability. The patterns of the design for pliable built-in socio-technical framework have to effectively integrate both security and usability issues to formulate usable and efficient privacy models. The design frameworks have to finish other tasks handling the security models of the systems.

4. Case Analysis

This case analysis is known as FI MedLab, which is connected to the data systems in the clinical laboratory (Medical Laboratory (MedLab)). The fundamental credibility of the clinical lab is essential to the safety and health of the patients depending on the test services given in these labs. The international standards in usage, in the modern day accreditation services, are the ISO 15189, which is based on the requirements for competence and quality. The lab does the tests on medical specimen to retrieve data on the health of the patients as related to prevention, treatment and diagnosis of illnesses. Such form of data is incredibly security-sensitive whereby any faults might have significant implication on the safety of the patients, which also affects the reputation or the privacy of the lab. A data system is used in many labs today hence allowing healthcare professionals to gather essential data on patients interpret test results and test potential records.

Data security and the risks of privacy have advanced significantly with the significant development in forms and number of people who have a critical role in providing the usage and accessibility of data and clinical records. The tension typically exists between the usability needs, privacy controls, and security controls. For instance, access to data systems might be delayed by the necessity of the first authenticate to assure legitimacy, and to issue the right measure of accessibility to the system the users request. Some data has to be present to the professionals in case of emergencies, but might not been communicated widely, due to the fact that is handles privacy or health measures. Contrary to that, disclosing such data is illegal in many states. This can also be said about any person who purposes to enter information in the systems. Information entry errors due to usability problems have fundamental implication on the integrity of information that is key aspect of privacy and security. The application of the approach in the case study is projected under stages:

Stage 1: Identification of Boundaries

FI MedLab represents a socio-technical model that includes operators (internal and external), patients, medical professionals, laboratories, suppliers of medical tools, IT services and data centres. The socio-technical model includes different Business Processes (BPs), which are classified into three different classes: Analytical, Post Analytical and Pre-analytical process. A number of operators have accessibility to some forms of data, but this is not the case for some other ones. This is dependent on the authorization levels and the authentication of users. In that case, within the business, users with certain responsibilities and roles have to be defined categorically.

Stage 2: Evaluation of Risks

This stage provides an explanation of three sub-processes, which have been mentioned earlier in this paper. In this stage, we utilize the explanation to illustrate how we have evaluated risks of security, privacy and usability in the socio-technical model of FI MedLab. These forms of risks are because of the interdependency between security and usability. Users have to access data, operate differently obligations and tasks. However, modalities to access this data is dependent on the context of tasks (outdoor or indoor and pressure of time). Other contexts involved as well include the quality of the privacy devices, adequacy to obligations and their different contexts.

Stage 3: Developing Remedies

The past three instances define the experience of the users, whereby each highlights the usability privacy or security issues. This stage illustrates a normal issue of confidentiality and privacy because of the possible misunderstanding of the utility structured of data requested to users (responsible medical practitioners or patients). This stage presents the remedy to this issue. The issue is considered more complex with different interrelated aspects, such as:

- Ineffective usability of the prevailing biometric authentication frameworks
- Non-effectiveness of the emergent processes
- Issues in comprehending the emergent processes by the business managers
- Determining the possible barriers that are bypassed by the managers

5. Conclusion And Future Directions

In conclusion, different equipment and tools have been recommended to provide usable interfaces for a certain privacy concern or applicable security initiatives. Nonetheless, there is a requirement to implement the engineering techniques for the formulation and application of the usability and security trade-offs. We purpose to issue a remedy to this deficiency in research. In this paper, we have presented a socio-technical technique to engineer the prevailing compromise between usability and security, which is termed as a sub-factor of privacy concern. The socio-technical framework links the systems and the various services with the stakeholders, users and people incorporated. We recommend using UMI and BPMN to illustrate and model the different interactions in socio-technical frameworks. Such a description is utilized then to identify potential security issues and usability, including the potential remedies. We project to utilize patterns to structure the remedies and design pliable built-in socio-technical models.

One essential benefit of the recommended socio-technical model approach is that the users and their experience are considerably involved. This will possibly overcome the absence of the experiences and training in security, the absence of security based on the corporate strategies (proceedings and operations) and the challenges of communicating the security problems. One of the problems is to create awareness and fundamentally convey good usability sense as a privacy attribute, which facilitates weighted consideration of privacy in the activities, decisions and thoughts structured. With that regard, future research is based on the involvement of users' experiences for the relevant stakeholders of the socio-technical models (managers, operators, and end-users). The patterns will therefore be extended to effectively integrate measures of subjective approach, privacy and trust criteria evaluating the experience of users and the emotions of users.

References

[1]. W. Rouse, "Enterprise Transformation ^|^mdash; Implications for Enterprise Information Systems", *IEEJ Transactions on Electronics, Information and Systems*, vol. 126, no. 9, pp. 1069-1072, 2006. Doi: 10.1541/ieejeiss.126.1069.

[2]. L. Liang, "Earnings forecasts in enterprise information systems environment", *Enterprise Information Systems*, vol. 2, no. 1, pp. 1-19, 2008. Doi: 10.1080/17517570701846539.

[3]. T. Kobayashi and N. Komoda, "Business Process Design Method Based on Business Event Model for Enterprise Information System Integration", *IEEJ Transactions on Electronics, Information and Systems*, vol. 124, no. 5, pp. 1068-1075, 2004. Doi: 10.1541/ieejeiss.124.1068.

[4]. A. Waheed and J. Yang, "The Effect of Mobile Marketing and Email Marketing on Exploratory Information Seeking (EIS) Behavior of the Consumers", *International Journal of Enterprise Information Systems*, vol. 13, no. 4, pp. 76-89, 2017. Doi: 10.4018/ijeis.2017100105.

[5]. V. Cheutet, J. Laval and C. Cherifi, "Towards the measurement of enterprise information systems agility to support EIS improving projects", *International Journal of Agile Systems and Management*, vol. 11, no. 3, p. 222, 2018. Doi: 10.1504/ijasm.2018.10015581.

[6]. F. Xhafa, "Advanced knowledge discovery techniques from Big Data and Cloud Computing", *Enterprise Information Systems*, vol. 10, no. 9, pp. 945-946, 2016. Doi: 10.1080/17517575.2016.1198965.

[7]. J. Warfield, "Systems science serves enterprise integration: a tutorial", *Enterprise Information Systems*, vol. 1, no. 2, pp. 235-254, 2007. Doi: 10.1080/17517570701241079.

[8]. I. Mandal, "Machine learning algorithms for the creation of clinical healthcare enterprise systems", *Enterprise Information Systems*, pp. 1-27, 2016. Doi: 10.1080/17517575.2016.1251617.

[9]. G. Swanson, "Material flow, material information, and the analytics of integrative enterprise information systems", *Enterprise Information Systems*, vol. 2, no. 1, pp. 21-31, 2008. Doi: 10.1080/17517570701846570.

[10]. K. Tseng, "Special issue: Bio-sense Information Systems", *Enterprise Information Systems*, vol. 14, no. 2, pp. 157-158, 2020. Doi: 10.1080/17517575.2020.1717002.

[11]. M. Arenas and M. Schwartzbach, "Information systems preface", *Information Systems*, vol. 34, no. 7, p. 577, 2009. Doi: 10.1016/j.is.2009.06.001.

[12]. P. Ciaccia and M. Patella, "Metric information filtering", *Information Systems*, vol. 36, no. 4, pp. 708-720, 2011. Doi: 10.1016/j.is.2010.09.007.

[13]. R. Bose, "Understanding management data systems for enterprise performance management", *Industrial Management & Data Systems*, vol. 106, no. 1, pp. 43-59, 2006. Doi: 10.1108/02635570610640988.

[14]. L. Raymond and F. Bergeron, "Enabling the business strategy of SMEs through e-business capabilities", *Industrial Management & Data Systems*, vol. 108, no. 5, pp. 577-595, 2008. Doi: 10.1108/02635570810876723.