INFORMATION SYSTEMS MANAGEMENT

Sergio Joao Teixeira Congo

Program in Science & Technology Studies, Korea University, Seoul, South Korea

ABSTRACT

Social navigation can be considered as an effective approach for supporting information management issues particularly privacy and security concern that prevail in the management of information systems. Any of these management information system security issues are a matter of critical acknowledgement for knowledge management systems as well. This paper outlines multiple privacy and security risks that can be applied to information systems in general. Including examples from different sectors such as health care, public information, and e-commerce, these management information issues provide an outline of the present situation. It also observes the key concerns of information system executive in these areas, highlighting the identification and explanation of regional differences and similarities. Selecting on a current issue in management information system the paper provides a detailed amount of knowledge on the possible reasons for the issues such as factors of economic development, technological status, and political/legal environment. The paper concludes by providing a revised framework for the management information issues formulated with effective literature searches. This is going to be effective enough for the studies that will more likely support such reasoning in the future.

KEYWORDS

Information Systems, Management, Framework, Encryption, Authentication, Privacy and Security

1. INTRODUCTION

Information system management and departmental considerations are important enough to take into account. Nowadays, organizations face multiple challenges in today's rapidly changing market due to the fact that the competition is high. Global environment is consistently changing as well to cater to the needs and requirements of high-tech techniques. One strategy to have an understanding of the challenges faced by information system departments is to have an executive and management level survey to outline which systems and methods lack innovation and systemic development (Bocij, Greasley, and Hickie, 2008, p. 40). In the United States, this method of evaluation initially started over a decade ago and has further stretched to several other countries.

One of the major, current issues in management information systems is the privacy and security of user interface. Information technology organizations and companies take into account that the

DOI:10.5121/ijitcs.2016.6302

developmental aspects, project teams, and departments heavily rely on multiple information system notions (Bocij, Greasley, and Hickie, 2008, p. 40). These elements are responsible for reusing and sharing knowledge about project plans, projects, intuitive solutions, procedures, technical complications, and additional functional procedures. However, there are some gaps and dysfunctional traits present in the system that can fail to product optimum privacy and security considerations. Managers responsible for securing information system assets are presented with multiple challenges (Bocij, Greasley, and Hickie, 2008, p. 40). From the viewpoint of different practitioners, it is feasible to notice that these challenges may be determined as the functional key issues that that are to be solved (Berisha-Namani, and Badivuku-Pantina, 2009, p. 555). This information indicates that there is an increasing need of organizational dependency on technical reforms for protecting information systems from multiple threats.

This research has different aims and objectives. Initially, it aims to highlighting and identify the emerging issues that information system and security organizations are currently facing, or believe they will face in the future aspects. The information also incorporates project management activities and development functionalities including design, requirements, tools used, procedures and standards (Berisha-Namani, 2013, p. 48). Moreover, there is a discussion provided to make sure that information system's privacy and security issues in organizational technicalities are explained from different market sectors. Another aim is to present an elaboration for differences in the key issues based on variables that are influencing different fields (Berisha-Namani, 2013, p. 48). Although, considering a specific field can provide substantial information in terms of organizational information system management, a comparative analysis can consider additional variables as well. The significance of this paper involves the frameworks discussed for all mechanisms that should relate and functionally assemble knowledge, or support services for multiple individuals consistently.

2. LITERATURE SEARCH STRATEGY

This paper implicates a secondary data analysis for the purpose of gathering useful information on the topic. Using the outcomes of studies from the past and present that have been conducted by MIS theorists and scholars in different regions, it elaborates what are some major privacy and security issues presently challenging the management information systems of different organizations. Secondary data analysis is from different literature papers, peer-reviewed articles, and journals providing knowledge for the current state of these issues in the area of information systems management.

This form of data gathering allows the researcher to work with the prevailing knowledge, avoiding any misinterpretations and gaps in information. Building on current findings, these literature searches provide an extensive amount of information, and allow comparison of data across fields and studies. The purpose is fulfilled with additional information from different reports and events that have aggravated the situation of privacy and security concerns in information systems.

It is a general observation that managing secure information and privacy options for different components is the most critical of all the tasks to maintain and implement effectually.

Considering present business models and literature perspectives that are network-centric, it is becoming difficult in an increasing manner to control access, validate user's identity, and conserve privacy and integrity of information. Security issue is a multi-faced factor which entails additional evaluations of the complete factors presenting vulnerability for the systems including business infrastructure. The literature identified aspects of authorization, authentication, and encryption to encompass all prospects of information management. These three areas are considered to have main concerns and issues. With the help of suitable explanations and articulations from the literature, elements of these concepts can be mediated in a useful manner. The literature search carried out included material based on the topic and keywords from 2001-2015 for the validation.

3. PRIVACY AND SECURITY ISSUES

Privacy and security issues of information systems management are critical enough to understand the process of negative information technology use. For instance, in the year 2005, hackers disintegrated Career Development Center of Stanford University, having accessibility of financial information, records of social security, resume, credit card details, and administrative knowledge for approximately 10,000 recruiters and students (Bélanger, and Crossler, 2011. P. 1040). During similar time, 380,000 alumni, learners, employees, administration staff, and new students of San Diego University were influenced; the website was hacked through four servers of the university's financial and business services department; they had complete control over social security details and driver's license numbers which affected the individuals in the most negative way possible (Bélanger, and Crossler, 2011. P. 1042). In January 2005, similar notions of hacking were repeated in campus card identity servers of George Manson University. Unauthorized personnel attained links to the photos, social security details, names, and college ground identity details of about 59,000 former, current, and future students, along with former and current staff and faculty.

There is a list of such incidents present in the literature, denoting no academic, health, or e-commerce organization are immune (Figure 1). For multiple organizations, events as such have served as a wakeup call to comprehend and outline a comprehensive information security and privacy strategy (Bélanger, and Crossler, 2011. P. 1042). The process is not simple enough and there are a lot of technicalities and managerial aspects involved. However, incorporating a culture of openness with a requirement of privacy and security is optimum enough.

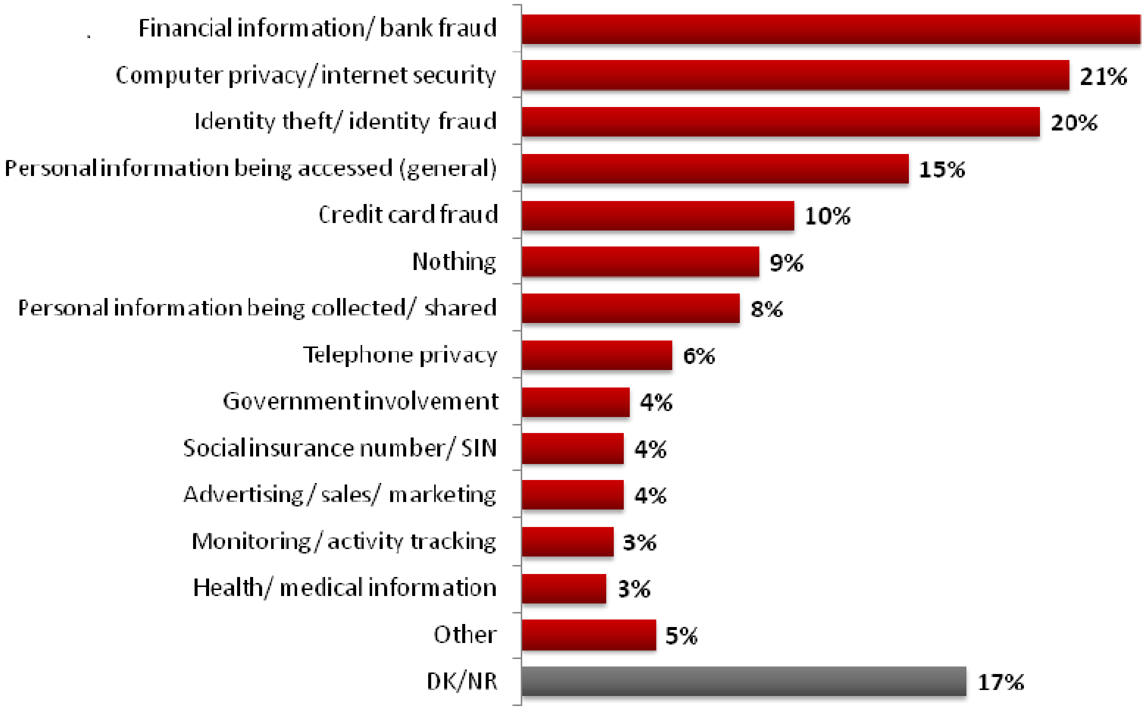
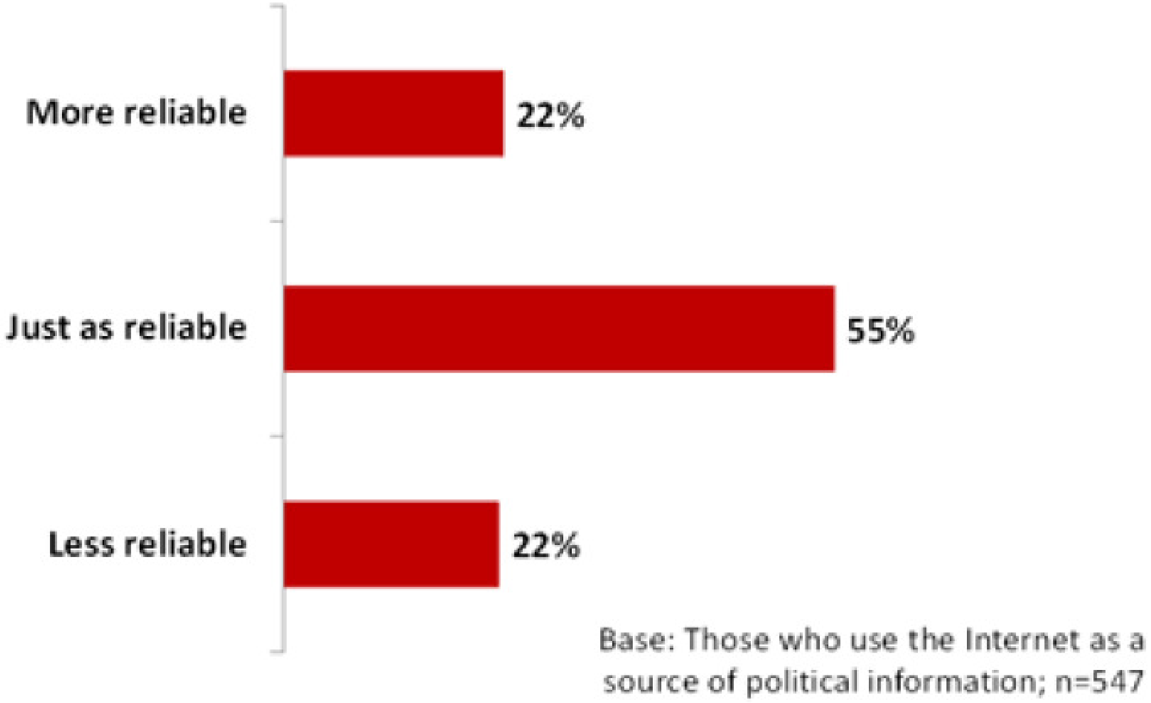


Figure 1: Emerging Privacy and Security Issues (Galliers, and Leidner 2014, p. 405)

The emerging issue is privacy and safety concern for multiple, diverse stakeholders including students, parents, health care professionals, alumni, staff, business professionals, faculty, and third parties of associated organizations (Galliers, and Leidner 2014, p. 405). At times, competing interests and management of cultivated strategies is difficult enough. There are different requirements for different field areas. However, the completion of these tendencies and functionalities is useful and vital for future outcomes. Community expectations, regulations, feasibility of accessing records, and increased online-threats demand a competitive strategy sometimes while having heavy cultural trade-offs and financial costs (Galliers, and Leidner 2014, p. 405). Effective privacy and security management along with ethical use of information requires an understanding on both human and technical levels. It also induces introduction of the requirement that users may have for the information systems (by regulation) and also the elements anticipated from the community.

Privacy and security issues of information systems are mainly involved with computer applications and systems which were not predicted until after a considerable time passed in the past decade (Galliers, and Leidner 2014, p. 405). As the computer age has progressed, and advancements of systems are incorporating technology into every aspect of life, these issues have increased even more (Figure 2). The issue of privacy involves the computing techniques and community of information system in association with the management of general knowledge on every citizen in advanced logarithms and record systems (Galliers, and Leidner 2014, p. 405). The process outlines the individual rights regarding personal information approach, and the processing, storage, dissemination, and use of this information to make suitable decisions. The last prospect is considerably critical out of them all in terms of social and legal issues that have been linked with the information system fields. Digital use of information systems is more effective and diligent than the conventional process that they have altered; these methods allow connections of information storage systems in an improvised manner (Galliers, and Leidner 2014, p. 405). However, individual security threats, outcomes from traditional information arrangements have possibly improved in digital/electronic ones.



Base: Those who use the Internet as a source of political information; n=547

Figure 2: Perception of Availed Information (Galliers, and Leidner 2014, p. 405)

Security is another aspect which involves the technical and procedural measures requiring prevention of illegal access, use, modification, along with distribution of information stored or analyzed within computing systems (Galliers, and Leidner 2014, p. 405). The requirements of control access are specifically important in multi-programmed and time-shared systems in which several users are connected simultaneously.

Privacy and security are one of the most current and discussed issues of management information systems (Rainer, et al. 2013, p. 120). These comprise of two essential components: electronic and physical. Physical security involves all of the external components and personnel involved in the process. Information security points mainly to securing of information that is stored electronically within networks. Security and privacy options of information systems, from an operational, routine viewpoint, involve supporting network users from cyber-attacks such as hacking, spam, and identity theft. It involves educating and informing the user community along with the development of authentication and authorization elements to supplement technicalities and innovative strengths (Rainer, et al. 2013, p. 120). The elements of privacy and security issues can be outlined by the components of effective information system solutions (Figure 3). These involve operations such as updating, adding sharing and providing knowledge and information. Moreover as the information systems are developing, a critical solution for technical personnel is to be derived, generally due to the significance of information and data that is stored.

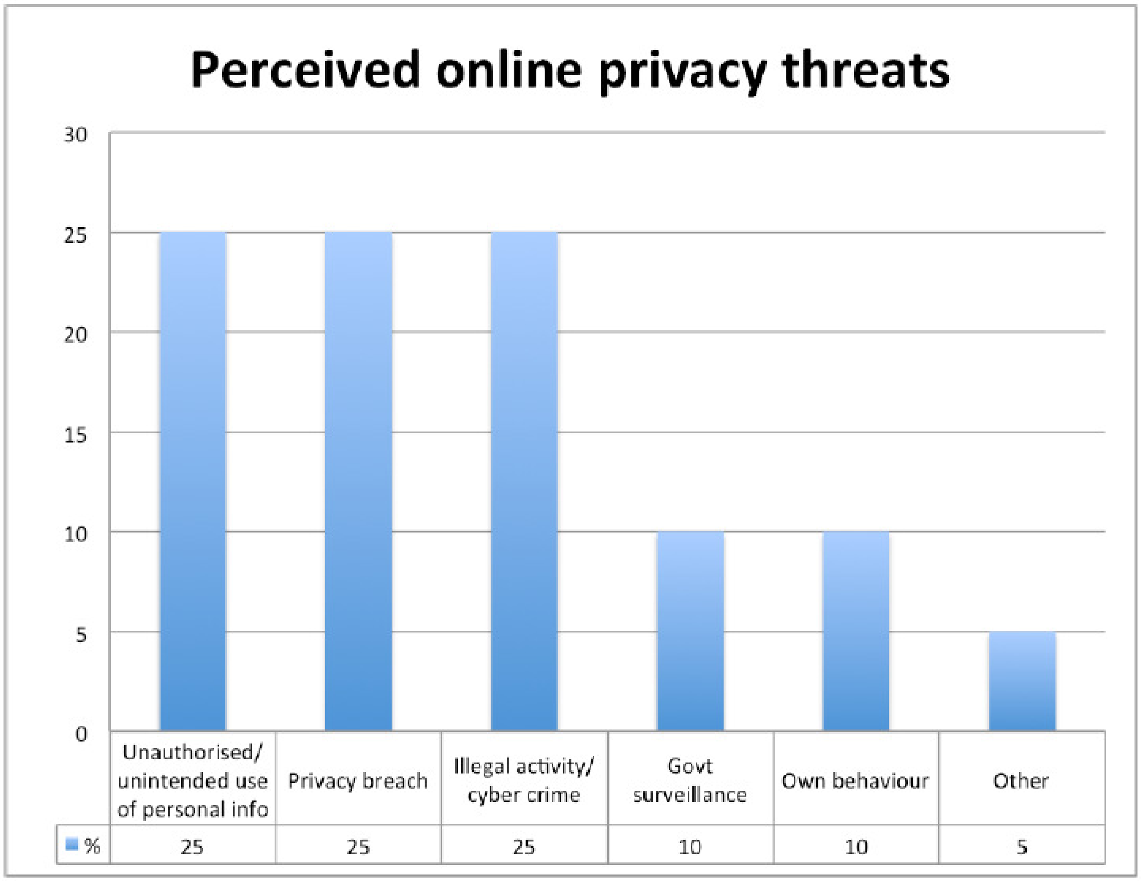


Figure 3: Perceived Online Risks (Rainer, et al. 2013, p. 120)

In general, information in any organization may exist in business procedures, process documents, technical support help information, applications, technical design documents, forums along with software tools and system user manuals (Rainer, et al. 2013, p. 120). These processes need to be context specific to be appropriate and relevant enough. Although both the elements of current issue are important, privacy is a complex process to take into consideration.

Privacy involves securing sensitive information in both electronic and physical forms. Procedures and policies regulated by system improvements can substantial outline protection of sensitive information, usually implied or identified by community expectations or federal laws. Privacy factors are even more important now due to the fact that data links and access are readily available now (Rainer, et al. 2013, p. 120). Examples of sensitive information that potentially be at risk include academic grades, social security numbers, financial aid, health records, research papers, donor information, student or employee information, email content, credit card numbers, network logins and even personal addresses.

Personal information is involved with the system modifications and automations to a limited extend being a matter of procedures and policies that fundamentally administer human involvement (Rainer, et al. 2013, p. 120). Violations of privacy are not projected or disclosed publicly; they are instead stated to regulators in many academic institutions. Concerns associated to these traits range from initial matters to potential criminal violations (Rainer, et al. 2013, p. 120). Examples involve access to voicemail and email, hacking, access to data on loaned or borrowed systems, salary questions, disability needs, any private medical information.

Multiple areas of concern in maintenance and suitability of information systems are common to security and privacy options: communication, policy establishment, training and enforcement, notification of victims, procedures, discovery/detection of instructions, and intrusion responses (Rainer, et al. 2013, p. 120). These, however do not have similar origins as overlapping of these components is substantial. Security of an information system maintains the protection of virtual and physical components. Information of sensitive nature in a form that could have public access can be protected in a beneficial manner (Rainer, et al. 2013, p. 120). However, security methods conventionally do not support things that are not documented and personal. These matters are to be protected with the help of designed frameworks and privacy regulations.

Privacy and security matters involve the technical and procedural elements that are needed for to protect information systems from any possible modification, illegal access, and distribution of private and discrete information. The requirements of access control are specifically critical in multi-programmed, time shared systems in which multiple users are providing services. Privacy and security issues initiated as problematic areas in the field of computer in mid 1970s. Since then, multiple paper and researches have evaluated the causes, challenges, barriers and offered solutions (Stair, and Reynolds 2013, p. 45). There is a presence of a consensus now that the legislative approach, instead of relying on self-policing, is a contributing approach to improving the issues of privacy. Different actions have been reported and applied in regions to solve the privacy and security issues in information systems.

According to the current literature present in the field, several reasons provide favorable objectives of organizations focusing on privacy and security (Stair, and Reynolds 2013, p. 45). First, organizations and their constitutional factors require a single source of responsibility, accountability, and ownership. Without this consideration, no suitable communication can be carried out. There should be a method directed to report issues. With the consistent support of information privacy and security leadership, multiple departments of an information system can coordinate and optimize activities in a beneficial manner. The literature outlines several legal mechanisms that focus on the topic. Several legislatives are needed to protect discretion of information systems (Stair, and Reynolds 2013, p. 45).. For instance, the Family Educational Rights and Privacy Act (FERPA) of 1974, integrates electronic and physical support of student information for education institutes (Stair, and Reynolds 2013, p. 45).. The Gramm-Leach-Bliley

Act in similar functions provides financial information protection. Health records can also be secured under the federal Health Insurance Portability and Accountability Act (HIPAA) (Stair, and Reynolds 2013, p. 45).

Some of the researches provide useful outcomes of these regulatory outcomes considering potential law suits from students, health patients for violations of rules. Understanding these structures of importance and recognizing community's expectation of privacy is of critical importance.

4.1. Privacy and Security Framework

There are different strategic systems functioning for providing privacy and security options that are updated and coordinated. There can be a code measured for the cause of evaluating suitable framework for privacy and security options. Both the code and its details of the concept can associate with the extensive requirement of privacy and security elements (Figure 4). These regulations have to be in accordance with the legislative and lawful structures present in the region; its applicability will be significantly applied (Chen, and Zhao 2012, p. 648). The fundamental values of the coding mechanisms are similarly implementable to individual knowledge recording purposes in the governmental fields and for other remote conditions.

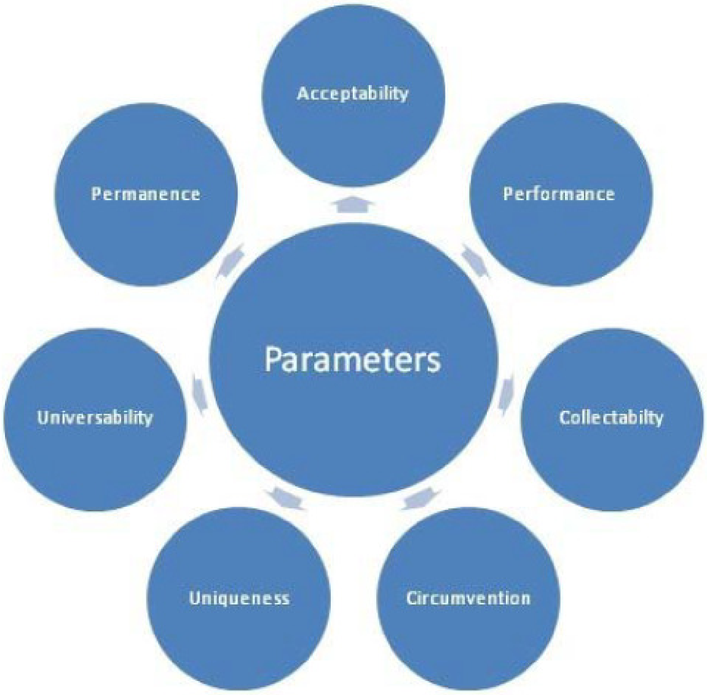


Figure 4: Framework for Privacy and Security Issues (Chen, and Zhao 2012, p. 648)

In addition to providing a legally modified code system to provide privacy and security options, additional techniques and reference points can be combined for maintaining computer associated options (Chen, and Zhao 2012, p. 648). Regardless of the field using these techniques can result in developing new products, along with finance, marketing, and planning for computing devices.

Authentication

Authentication is a process that seeks support and guarantee for the identification options for systemic users. This method can be derived for the purpose of maintaining and improvising the old-fashioned method of password and user ID (Ren, et al. 2012, p. 70). The conventional authentication methods are not as professional or adequate enough considering present times where security is a main concern for larger organizations and information systems. Authentication models these days are frequently required for the basic and intermediary application of the security policy.

Businesses and health care databased require an authentication framework to incorporate a feasible, updated, and maintained structure of information management (Ren, et al. 2012, p. 70). Its components can be updated from time to time due to the deficiencies found in the algorithms or system alterations for specific identification (Ren, et al. 2012, p. 70). Two important frameworks that prevail presently to enable websites and applications to implement multiple models of authentication are Generic Security Services Application Programming Interface (GSS-API) and Pluggable Authentication Module (PAM).

GSS-API

This software provides application control of privacy and security. A programmer implementing the application can make information available that disregards the details of limiting or securing network data (Ren, et al. 2012, p. 70). This type of functionality can also provide a structural improvement that allows security services to function in a generic manner, which maintains multiple technologies, such as Public Key Mechanism or Kerberos.

PAM

PAM is a process of authentication involving system capacity notions like rlogin, telnet and login to be altered to induce required modifications for any program. Considering framework options provided by PAM, several technicalities and verification software can be customized, this does not involve any patterns or structures including the programs, therefore securing prevailing environmental systems (Ren, et al. 2012, p. 70). PAM approach is implemented to incorporate login contributions having multiple verification codes, for instance DCE, Kerberos, smart-card based systems and RSA. For this reason, the application supports network technologies to have balanced and strategic placement. Several applications can be derived with the help of introducing trusted context in an application server as well.

Authorization

Besides authentication complexities, servers and websites also go through issues of unauthorized access to important or private information (Ren, et al. 2012, p. 70). Authorization management and updating is essential to make sure that every user has the suitable access privilege. For instance, an organizational CFO may need a different authorization interface for being more assisting with the financial knowledge on a professional term than a department manager who does not have complete access. Resourceful and fine-grained authorization methods allow organizations to have access in a managed manner to control any permissive actions for a user based requirement.

IDS and DB2 have implied a solution to limiting system contact for official personnel; it is known as Role-Based Access Control (RBAC). This is further supported by Mandatory Access Control (MAC) and Discretionary Access Control (DAC). These provide effective distribution of functions in an organization where the roles are formed for multiple job functions users have (Ren, et al. 2012, p. 70). With the help of these functions, the information in systems is present for users depending on the security clearance levels.

Encryption

Encryption outcomes are not directly associated with authorization and authentication but they have an important influence on data protection, during transfer or otherwise (Zissis, and Lekkas 2012, p. 590). Network protocols for instance SMTP, HTTP, and FTP do not support adequate system characteristics for protection of important information sent across the networks. The information transferred is vulnerable to network attacks like hacking, data tampering, non-repudiation, and capture-replay (Zissis, and Lekkas 2012, p. 590). Encryption provides Secure Socket Layer (SSL) provides additional outcomes than conventional protocols. Processes as such ensure integrity and confidentiality of data transmission on the network. For some applications, encryption of data can be used as an additional security measure such as support column level encryption (CLE) (Zissis, and Lekkas 2012, p. 590). Most of the issues related to data security can be controlled by suitable access control and authentication, making sure only professional and authorized personnel can approach data. These can be beneficial for setting password for a session only.

The formation and adaptations of information systems are increasing in a tremendous manner and so are the interpretative considerations. The greater the ability to build individually customized information applications and functions will be, the more the potential for communication between disparate devices increases (Zissis, and Lekkas 2012, p. 590). In addition, customer data stored in systems can be used to gain competitive advantage in the market to the benefit businesses.

Even if the information is freely available, individuals are typically not as good as large firms at capitalizing on large amounts of information. The effect of privacy and security on this problem is ambiguous. Increasing interoperability will give each firm in the market more information. This may increase competition between them but decrease the overall welfare of all consumers (Zissis, and Lekkas 2012, p. 590). Alternatively, one firm may be better at capitalizing than another, and use their advantage in information to substantially increase their market power, reducing both competition and consumer welfare. The development of objects connected to the internet can facilitate the development of any innovative applications. These objects can enable businesses to collect data and perform transactions on their behalf. In addition, the cost of deploying such applications will be lower since the use of devices and sensors will be replaced with web services.

Communication comes with both power costs as well as monitory costs. In addition, sending a message requires time on the part of the sender. On the other hand, the receiver must take the time to read and interpret the message (Zissis, and Lekkas 2012, p. 590). Since information systems consist of many devices, it means that the cost of processing power will be high. In addition, if the communication between devices is not well managed, the system's noise-to-signal ratio could be high, thus causing communication to be poor (Zissis, and Lekkas 2012, p. 591). This is not always a serious problem. Several online programs and devices in the market are designed and developed by a single vendor, which eliminates the problem of interoperability. However, for open systems, the potential for problems could be great. The potential for change and revolution of devices in the information systems is enormous. However, it is important to first determine whether two devices should exchange data (Zissis, and Lekkas 2012, p. 591). As a matter of fact, a world where every device communicates with every other device is impractical. For example, lights in a room and a coffee pot need not to share data or communicate with each other.

The best design approach for personal use information systems is to ensure that such systems operate as stand alone. This will allow only internal communication between applications in the system and reduce the risk of an attack overwhelming a myriad of applications.

4. CHALLENGES AND BARRIERS OF PRIVACY AND SECURITY ISSUES

Conducting the literature search, it was identified that there are multiple challenges and barriers associated with the implementation of privacy and security components in information systems. Most of these issues are significant enough to successfully approach management information system in a successful manner (Manshaei, et al. 2013, p. 25). Incorporating the privacy and security checks in the system can be defined as the same meaning as success factor; in order to approach a better understanding these can also be termed as critical success factors (CSFs). CSFs for the information system management and protection are essential as established for multiple contexts such as Information System planning, requirement analysis, and project management. Most of the literature of information system has identified the concern of privacy and security for technical assortment of ideas. Authors such as Nah, Lau and Kuang (2001, p. 288) stated 11 factors that were critical to the implementation plan success; their explanations included suitable security options for management information systems. Moreover, investigations from Motwani, Subramanian, and Gopalakrishna (2005, p. 530) evaluated the factors inhibiting and facilitating the success of information system projects and highlighted these critical success factors. For an enterprise resource planning (ERP), critical success factors such as security and privacy of information systems were considered essential by Lucey (2005, p. 300).

For the purpose of having privacy and security factors managed and coordinated, the studies provided valid information on the challenges and barriers. Organizations of different fields may come across these challenges of cybercrime at some point. Having a proper outlining of these factors will provide improved modifications and contributions in the future.

Design

Professionals often mention that effectual security and privacy options are a critical component of the information system design. Still, website designers and developed have focused more on features and applications than security, taking into account the economic reasons (Manshaei, et al. 2013, p. 25). There are many future security requirements that cannot be predicted. With the advancements and computing options available, it gets difficult for web developers to form an interface that has strong authorization and authentication system.

Incentives

Another important barrier for the information system security and privacy issues is the structure of economic incentives. These notions for online support have been considered partial or even pertinacious (Manshaei, et al. 2013, p. 25). Cybercrime is often considered as profitable, cheap, and comparative supportive for criminals. In comparison, the security and privacy options can be expensive for the organizations to implement; the economic returns on investments are often uncertain as well.

Consensus

Different stakeholders and organizational professionals do not completely understand the concept and significance of privacy and security in information systems (Manshaei, et al. 2013, p. 25). It means different things to different members, and has no common agreement on implementation, meaning, and risks. Main cultural impairments that are linked with these agreements have also affected the progress negatively (Manshaei, et al. 2013, p. 25). These arguments exist between fields and even organizational structures.

Environment

Internet can be regarded as the rapidly changing technology space in global history, considering both properties and medium (Manshaei, et al. 2013, p. 25). Advanced and emerging applications and properties, particularly mobile computing, social media, cloud computing, big data and the Internet of things, additionally challenge the environmental dynamics.

Education and Knowledge Abuse

There is little or almost no information present in the literature in describing navigation points and social awareness planning to promote security and privacy issues of information systems (Schumacher, et al. 2013, p. 245). Computerization of routine business functionalities has provided new opportunities and new methods of rules violations such as falsification of records, embezzlement, identity theft, and even fraud. In alignment with different cybercrime cases, it is feasible to observe that employees who design or manage information systems, develop application programs, or functionally mediate the equipment have acquired skillset for criminal acts (Schumacher, et al. 2013, p. 245). These individuals tend to pass down the information for fictitious payments, deposits of unauthorized payments into different accounts, and manipulation of credit scores.

This form of education and knowledge distribution should be used in a positive manner protecting the computer-based systems, and data/information that is provided. Communication aspects must be provided in organizations and institutes when needed to ensure secrecy of knowledge and viable techniques.

Although these actions are extensive enough to mediate, executive actions and legislative components can have significant influences (Schumacher, et al. 2013, p. 245). For instance, resource and development for privacy and security may influence the designing aspects of information systems, penalties may change the incentive structure, effective frameworks may have positive alterations, and federal regulations for cloud computing and other emerging components may assist in the advancement of cyber security.

6. FUTURE IMPLICATIONS

The security and privacy challenges of management information system where smart devices and objects are connected on an interoperable framework are among the key concerns of current research (Ifinedo, 2012, p. 83). Significantly, the development of management information system research in view of pervasive applications that include critical technology drivers and the expected outcomes of applications is an area that requires further research. The web architecture research will need to conduct further considering that management information system technologies are progressively evolving and being improved.

Significantly, development of productive technological change integrates a synergetic relationship between organizational and technical innovations. However, disconnect in the pace of development between technical infrastructures and organizational functions exist. Management information system technologies develop and change at a faster rate when compared to organizational and social innovation which is often left behind (Ifinedo, 2012, p. 83). Research should focus on the development of strategies that will ensure organizations and human resources will change at the same pace with technology.

New technologies such as smart cars, smart homes and smart phones will all be connected in the internet of things. The research outcomes identify the key drivers of the new information systems phenomena. He notes that wireless sensor networks, physical cyber systems, mobile computing and pervasive computing are the main elements that will be interconnected in the management information system (Ifinedo, 2012, p. 84). Effective and secure information systems will allow users to perform real-time computing in an internetworked environment consisting of numerous interconnected systems. The initial narrow definition for the individual technologies will therefore not be appropriate in the new application areas of management information system. For instance, smart visions in management information system will embrace a myriad of technologies from computer engineering, computer science and electrical engineering.

7. CONCLUSIONS

It has been argued that the management information system will bring about enormous qualitative changes in our modern society. For instance, smart taxis and cars will be transformed through the use of smart phones that have sensors. This will ensure safety in transportation. On the other hand, health services will be transformed by patients with smart phones that allow doctors to locate the patient and monitor his or her wellness remotely. The management information system is therefore a system- of –systems that intends to synergistically harness the power of independent applications by integrating them to form a larger platform.

However, the research notes that significant research will be required in different areas. The massive scaling of existing applications will require researchers to re-think issues such as security, openness, reliability and robustness. This is due to the fact that in an interconnected world, failure or any form of compromise will adversely affect personal life as well as national economies. The management information system also poses new challenges to system developers and integrators. As a result, new frameworks need to be developed to support the implementation of the new systems and also modification of existing ones to cope with the new challenge.

The management information system is a new technological paradigm for information communication technologies especially management information systems in business environments. The internet has enabled interconnectivity of people and devices across multi-networks irrespective of their geographic location. The connection of things creates intelligent systems that aid in the management of critical systems in business, health care, security and other applications. While a significant percent of the components that make up the management information system are not new, it is developing at a pace that most people and firms are unable to keep up. Essentially, the sophistication, scale and application of management information system presents various challenges that people and firms are yet to overcome; hence the need for more research towards the identification of solutions. A multi-disciplinary outlook is required to identify and challenge critical assumptions with respect to the implementation, designs and outcomes of security and privacy.

The management information system presents numerous opportunities for businesses; however, the potential security and privacy threats to transmitted data cannot be overlooked. The issue of open systems that devices can connect without restrictions could derail the development of management information system since people and organizations will be reluctant to send or receive critical data on the premise of its integrity being compromised along the way. However, once the issues of privacy, security and data integrity are solved, management information system will present a critical value adding resource.

REFERENCES

[1] Belanger, F. and Crossler, R.E., 2011. Privacy in the digital age: a review of information privacy research in information systems. MIS quarterly, 35(4), pp.1017-1042.

[2] Berisha-Namani, M. and Badivuku-Pantina, M., 2009. Information society and knowledge economy. Getting the Internal CNCSIS Accreditation B LESIJ is indexed BDI by EBSCO-CEEAS Database, p.555.

[3] Berisha-Namani, M., 2013. Information Systems Usage in Business and Management. Business Innovation, Development, and Advancement in the Digital Economy, p.48.

[4] Bocij, P., Greasley, A. and Hickie, S., 2008. Business information systems: Technology, development and management. Pearson education.

[5] Chen, D. and Zhao, H., 2012, March. Data security and privacy protection issues in cloud computing. In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on (Vol. 1, pp. 647-651). IEEE.

[6] Fui-Hoon Nah, F., Lee-Shang Lau, J. and Kuang, J., 2001. Critical factors for successful implementation of enterprise systems. Business process management journal, 7(3), pp.285-296.

[7] Galliers, R.D. and Leidner, D.E., 2014. Strategic information management: challenges and strategies in managing information systems. Routledge.

[8] Ifinedo, P., 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), pp.83-95.

[9] Lucey, T., 2005. Management information systems. Cengage Learning EMEA.

[10] Manshaei, M.H., Zhu, Q., Alpcan, T., Bacşar, T. and Hubaux, J.P., 2013. Game theory meets network security and privacy. ACM Computing Surveys (CSUR), 45(3), p.25.

[11] Motwani, J., Subramanian, R. and Gopalakrishna, P., 2005. Critical factors for successful ERP implementation: Exploratory findings from four case studies. Computers in Industry, 56(6), pp.529-544.

[12] Rainer, R.K., Cegielski, C.G., Splettstoesser-Hogeterp, I. and Sanchez-Rodriguez, C., 2013. Introduction to information systems: Supporting and transforming business. John Wiley & Sons.

[13] Ren, K., Wang, C. and Wang, Q., 2012. Security challenges for the public cloud. IEEE Internet Computing, (1), pp.69-73.

[14] Schumacher, M., Fernandez-Buglioni, E., Hybertson, D., Buschmann, F. and Sommerlad, P., 2013. Security Patterns: Integrating security and systems engineering. John Wiley & Sons.

[15] Stair, R. and Reynolds, G., 2013. Principles of information systems. Cengage Learning.

[16] Zissis, D. and Lekkas, D., 2012. Addressing cloud computing security issues. Future Generation computer systems, 28(3), pp.583-592.