Asian Journal of Information and Communications 2018, Vol. 10, No. 1, 114-122

KISDI KOREA INFORMATION SOCIETY DEVELOPMENT INSTITUTE

Asian Journal of Information and Communications

Managing cyber security risks in Nepalese organizations

Dwarika Upreti*
Nepal Megha College

Sudarshan Giri**
Research scholar

Abstract

The internet is constantly changing the way we live and conduct business. E-service encompasses a series of necessary steps for institutions to develop and administer to ensure successful implementation of services at large. This paper discusses the growth trend of e-service, cyber security and challenges to overcome the situation for effective service delivery. Content analysis and survey approach was used to generate data in the case study. The study has claimed that the virtual nature of the internet, and its recreational aspects, can blind young people and novice users to its considerable capacity to do harm in e-service. The study has concluded that e-service is essential for managing future complications and responding to current and past incidents to build trust from people. The insight on reducing current and future vulnerabilities, the probabilities of a threat, and the costs associated with potential outcomes support their mitigation. Some of the issues related to e-service can be regulatory, legal, technical and procedural measures as well as customer education, capacity building and licensing.

Keywords: cyber security, e-service, critical infrastructure, information communication and technology, electronic transaction

1. Introduction

The world is rapidly transforming into one society driven by an outstanding increase in the amount of communication between civilizations. It has really become information driven society, in which information and communication technology is playing important and indispensable role. Keeping up with the twenty-first century, governments around the world are embracing Information Technology (IT). In every region of the globe - from developing countries to industrialized ones - central and local governments are putting critical information online, automating bulky processes and interacting electronically with their citizens (KIPA, 2006). The arrival of new information and communication technologies (ICTs) has significantly enhanced our capabilities to collect, process, and distribute information (Heeks, 2003). Almost all developing countries regard ICTs as an important factor while preparing their national development plans. This paper discusses about the area which has been given outstanding attention regarding the use of ICT in the quest of good governance, usually termed as e-governance.

E-government has been considered as a narrower discipline dealing with the development of online services to the citizen, more the 'e' on any particular government service - such as e-tax, e-transportation or e-health

* Corresponding author: dwarikaupreti2000@gmail.com
** advosudarshan@gmail.com

(Danish Dada, 2006). E-governance is a wider concept that defines and assesses the impacts technologies are having on the practice and administration of governments and the relationships between public servants and the wider society, such as dealings with the elected bodies or outside groups such as not for profits organizations, NGOs or private sector/corporate entities. E-governance encompasses a series of necessary steps for government agencies to develop and administer to ensure successful implementation of e-government services to the public at large.

There is a widespread curiosity among citizens about e-government. E-government encompasses to explain the relation and benefits through e-government to provide various kinds of services to its people via public administration from bureaucracy to service provider (MOE, 2013).

2. E-government implementation in Nepal: the country context

There are many dimensions streamlined and drivers identified to make our New Nepal dreams come true. One of such dimensions is the reformation of the government. Governance and its service process have been felt to be well reengineered to fulfill the aspirations of its citizens. Information and communication technology and its tools may help its effective and efficient transformation.

In regard to this, the government of Nepal has prepared e-Government Master Plan (eGMP) Consulting Report, which is an attempt to lay the ground work for e-government transformation. E-government vision has been to fulfill citizen-centered service, transparent service, networked government and knowledge based society. The mission statement has included "Improve the quality of people's life without any discrimination, transcending regional and racial differences, and realize socio-economic development by building a transparent government and providing value added quality services through ICT".

Although there are some missing elements in the eGMP, it may lead to a successful e-government in Nepal. All plans are continuously evolved so that the eGMP can be evaluated and updated. Establishing good coordination between government organizations to make seriously committed environment may help implement e-government successfully.

3. Problem statement

There has been growing demand and use of IT in the organization systems and most of the documents have been used and stored in digital form. The problem has been raised in the preservation and proper storage as well as prevention of misuse of electronic documents to protect from their manipulation. The problem statement of this study has been set as: To what extent the cyber security risks have been managed in Nepalese organizations?.

4. Objective

The major objective of the study was to analyze the cyber security risks and their management in Nepalese organizations.

5. Methodology

The study was conducted based on the document review and inquiry methods. The study was under the qualitative method perspective including critical interpretive approach. The data collected were coded and decoded for the textual presentation. The paraphrasing was carried out as and when required in the texts.

6. Literature review

The internet is constantly changing the way we live and conduct business. These changes are occurring both in the ways that we currently experience (e-commerce, real-time information access, e-learning, expanded communication options, and so forth), and in ways we have yet to experience. Convergence of voice, video and data is on anvil and existing communication networks are paving way to all IP enabled Networks such as Next Generation Networks (NGN). Therefore as a society we are just beginning to unlock the potential of the internet.

A growing percentage of access is through broadband connections, and users and organizations are increasingly interconnected across physical and logical networks, organizational boundaries, and national borders. As the fabric of connectivity has broadened, the volume of electronic information exchanged through what is popularly known as cyberspace has grown dramatically and expanded beyond traditional traffic to include multimedia, process control signals and other forms of data. New applications and services that use ICT infrastructure capabilities are constantly emerging. With the rapid growth of internet, network security has become a major concern for policy makers and regulators worldwide. A private network when connected to the internet is connected to more than 50,000 unknown networks and all their users (CIA, 2010). The development of robust IP networks with possibility of one billion connected people increases the security threats further. Protection of services and the consumers from data theft, fraud, denial of service attacks, hacking, cyber warfare, terrorist and antinational activities becomes a challenge (Pariyar, 2007). Some cyber-attacks like those against systems controlling infrastructure would have debilitating effect. According to an international estimate one in 295 emails is virus infected and 3 in 100 emails carry malware (Kwon, 2015). Sophos Labs tracked and analyzed 95,000 malware pieces every day in 2010, which is nearly twice the number of malware pieces tracked in 2009. More than 3500 malicious websites are blocked per day and 89.4% of mails are spam. The majority of the attacks (32%) are phishing followed by virus (29%) and network scanning/probing (18%) (CAN, 2010). Thus cyber security may become of paramount importance as broadband may not be limited to provide vital services to citizens but will also be used as core to provide various citizen centric services.

Social network attacks are coming up and expected to be one of the major sources of attacks in near future because of the volume of users and the amount of personal information posted. Users' inherent trust in their online friends is what makes these networks a prime target. For example, users may be prompted to follow a link on someone's page, which could redirect users to a malicious website.

Social engineering techniques on social networks are on the rise. Social engineering is a term for psychological tricks used to persuade people to undermine their own online security. This may include opening an email attachment, clicking a button, following a link, or filling in a form with sensitive personal information. All sorts of scams, and many methods used to spread malware, make use of social engineering techniques, and target human desires and fears as well as just plain curiosity to get past the caution one should be exercising when online (InfoDev, 2008).

Since the introduction of the iPhone, the popularity of smart phones has grown over the last several years. More and more users of smart phone get involved in several online activities thereby creating a potential shift

in cyber attacks as cyber criminals may target end users via mobile platforms. As with other platforms, the attackers would like to explore where the most users are, and where these users are the least protected. Cloud computing refers to a type of computing that relies on sharing computing resources rather than maintaining and supporting local servers. Cloud computing is a growing trend due to its considerable cost savings opportunities for organizations. The growing use of cloud computing will make it a prime target for attack.

Migration from legacy network to next generation network will provide platform for development of many useful applications and sharing of information. The critical data of an organization containing personal data, critical enterprise resources etc. are potential source of attack because of following two main reasons:

1. First is the ubiquity of the Internet. Access to vulnerable devices will continue to increase with growing number of devices connected on the Internet.
2. Second is the popularity of easy-to-use operating systems and development environments. Overall ingenuity and knowledge required by hackers is drastically reduced and for a hacker it is much easier to create applications that can be distributed on the Internet (InfoDev, 2008).

7. National information technology center (NITC) as an e-government implementation hub

Use of e-governance is to raise the quality of services delivered by governments to citizens and businesses. Most governments in the developed world have moved towards implementation of IT to deliver services to the citizens as well as better govern their internal programs. Today wide ranges of e-governance projects are being implemented at different parts of the country including the projects designed to reduce digital divide in rural areas that have been ignored in the past.

E-governance has been a radical concept that covers wide range of IT enabled reforms including

1. Prioritize the governments need to use IT and the Internet to provide services between government agencies, citizens, and business
2. Improve the democratic values of the government process and administrations through more transparency, accountability, and involvement
3. Make the internal operation of public administrations more efficient
4. Change the mindset of the administration for successful implementation of e-governance
5. Create awareness of IT in the top bureaucracy
6. Expand access of IT to the common people through establishment of self sustaining tele-center in rural part of the country

NITC co-locates servers of different governmental organizations and agencies in Government Integrated Data Center (GIDC). There are large number of Nepal governmental organizations that have been hosting their servers in GIDC. NITC is the main implementing body of e-government in Nepal. Developing human resource in the field of IT is the first and foremost need to implement e-government. It is difficult to implement e-government without IT literate human resource. To empower the ICT literacy NITC has been conducting basic, advanced and expert level computer training courses along with ICT awareness training programs and workshops inside and outside the Kathmandu valley. NITC has already trained more 2,350 people from different government agencies and NGOs (NITC, 2016). NITC provides consultancy and advisory service about ICT to all the government organizations and departments within the country. NITC conducts research and development work relating to ICT for the development of ICT sector in Nepal.

The approach to tele-center was instigated in order to shrink the digital divide that evolved from the situation in which substantial number of citizen in the developing country lack to obtain the rights of developmental progress. In general, through the concept of tele-center, it is aimed to provide the deficit community with the ease of modern information technological services such as internet, email, fax, photocopy, scan etc. in order to help them reach the realm of development.

Establishment of tele-center helps to reduce the information and knowledge poverty, consequent trivial boundary relation in developmental effort to showcase major changes in modern information and communication sector. At present, it is strongly felt that with the establishment of tele-center, developmental methodology based on information and communication technology should also go hand in hand. Tele-centers can also be used in local level to be integrated with government services. The local level employees can be trained to use e-government services such as land registration, tax records etc.

8. Findings and reflections

Cyber crime has been one of the fastest growing areas of crime. More and more criminals are exploiting the speed, convenience and anonymity that modern technologies offer in order to commit a diverse range of criminal activities. These include attacks against computer data and systems, identity theft, the distribution of child sexual abuse images, internet auction fraud, the penetration of online financial services, as well as the deployment of viruses, botnets, and various email scams such as phishing.

In the past, cybercrime has been committed by individuals or small groups of individuals. However, we are now seeing an emerging trend with traditional organized crime syndicates and criminally minded technology professionals working together and pooling their resources and expertise.

This approach has been very effective for the criminals involved. In 2007 and 2008 the cost of cybercrime worldwide was estimated at approximately USD eight billion. As for corporate cyber espionage, cyber criminals have stolen intellectual property from businesses worldwide worth up to USD one trillion (ADB, 2007).

Nepal's cyber world is ruled by Electronic Transaction Act (ETA) 2063 that protects users online against cyber crimes. Though the cyber law is present but due to lack of proper monitoring and updates it serves little use in protecting users online. The dynamics of internet has grown phenomenally where the ETA has been fixed and constant. Internet provides easy accessibility and other facilities but at the same technology also threats the nation in lack of proper mechanism and policies which needs to be researched and worked on.

Nepal has seen ups and downs in its technology but due to its limited policies and regulation Nepal faces a huge hindrance in the coming days. Technology has been passed on but with little governance, and lack of proper mechanism and measures to cater the need at time of emergency, Nepal faces a huge threat or challenge in overcoming the online threat. Cyber laws have become essential in view of the rapid developments in information technology. Online communication has given rise to a new global commerce in ideas, information and services. Information Technology is changing almost all aspects of human activity like communication, trade, culture, education, entertainment, and knowledge. With the rapid advances in computer technology over the past few years, there has been increasing concern in many countries for the need to develop and modernize the law in order to take full advantage of technological improvements and at the same time to guarantee that states can respond to computer crime and related criminal law issues associated with these developments. The cyber law encompasses a wide variety of legal issues which include intellectual property, privacy, freedom of expression, and jurisdiction.

Prior to 2004, the government of Nepal dealt with cyber crimes under the Public Offence Act. Nepal Police dealt with cyber crimes but they were not aware about the technical aspects of these crimes, which meant that the sanctions were not effective and relative to the crime. Later The Electronic Transaction and Digital Signature Act 2004, also known as the cyber law, passed. This law was forecast to be landmark legislation for the development of the IT industry in Nepal. Under Act of 2004, hacking, deleting data, stealing e-documents, software piracy and posting defamatory information invite criminal and civil sanctioning to individuals and institutions. Under this law, the government can punish cyber offenders with up to five years of imprisonment and/or a fine of up to fifty thousand rupees. However, much depends on the severity of the crime. The law has tightened the security for banking transactions through electronic means, which should boost the economic activities across Nepal via the Internet.

The biggest challenge before the cyber law is its integration with the legacy system of laws applicable to the physical world. The unique structure of the Internet has raised several legal concerns. While grounded in physical computers and other electronic devices, the Internet is independent of any geographic location. While real individuals connect to the Internet and interact with others, it is possible for them to withhold personal information and make their real identities anonymous. If there are laws that could govern the Internet, then it appears that such laws would be fundamentally different from laws that geographic nations use today. Since the Internet defies geographical boundaries, national laws will no longer apply. Instead, an entirely new set of laws will be created to address concerns like intellectual property and individual rights. In effect, the Internet will exist as its own sovereign nation.

9. Electronic transaction act and its implementation

It is means to make legal provisions for authentication and regularization of the recognition, validity, integrity and reliability of generation ,production, processing, storage, communication and transmission system of electronic records by making the transactions to be carried out by means of electronic data exchange or by any other means of electronic communications, reliable and secured, and where as, for controlling the acts of unauthorized use of electronic records or of making amendment in such records through the illegal manner.

A digital signature is an electric signature, just like your handwritten signature, which is used to authenticate your identity. Public-key cryptography makes this possible. Public-key cryptography involves the use of two cryptographic keys, one private and one public. Whatever the public key encrypts, the private key can decrypt, and vice versa. The user keeps his private key and the public key is available to anyone.

10. IT policy and emerging challenges of e-government

Policies are used to set a standard for performance. Through policy, an organization can develop clear expectations for students, parents, teachers and administrators. It provides a framework for consistent actions regardless of district or school in a region, or even state-wide. Federal and state laws set a policy framework for the use of technology within the school system. All states and school districts are required to have technology plans in compliance with federal policies.

First and foremost, proper policies protect the institution from non-compliance with the law. Clear organizational guidelines allow organizational leaders to avoid overlooking any legal imperatives which might otherwise go unnoticed. In addition, ensuring that persons with disabilities are able to communicate and learn

is a moral responsibility. Accessibility benefits everyone, not just people with disabilities. The world's least developed countries including Nepal have availed themselves of the opportunity to rapidly develop education, health, agriculture, tourism, trade and various other sectors using information technology. Hence, it has become essential to formulate a policy at the earliest for developing information technology with a view to boosting up national economy. The information technology policy shall be formulated to make information technology accessible to the general public and increase employment through this means, build a knowledge-based society and establish knowledge-based industries.

Depending on a country's economic, social, and technological reality, before an e-government program can progress, it must overcome a series of challenges, including low internet penetration, infrastructure restrictions, digital divide, and concern regarding privacy and security, limited number of qualified IT specialists, unavailability of payment gateway, lack of digital signature and lack of IT literacy among the citizens.

IT policy is a significant and important step in the right direction towards the developing the ICT sector and representing the society as knowledge based society. However several challenges have beset Nepal's efforts aiming at building upon the initial momentum that it gained in the ICT domain. As the lack of political constancy deterred Nepal from effectively capitalizing on the promise unleashed by digital opportunities, the country found itself confronting a host of competing priorities ranging from the ones posed by security challenges to that of endemic poverty and poor governance. In the planning process, the government expressed its desire to meld Nepal into a knowledge-based society. The broad objective for the IT sector was to promote IT as a tool for social and economic development; to promote social development by using IT to improve agricultural, health, education, and other services and sectors; to promote economic development by establishing an IT park to produce and export low-cost software and eliminate the poverty from country which is one of major problems in Nepal.

We have the experience of failure in completely implementing the policy and over the last few years with scarce resources tied up in security efforts, and implementation of the IT Policy has slipped from the government's priority list. Although the institutional provisions have been put in place, the key implementing body is too under-resourced to effectively oversee implementation. We know that e-governance in Nepal is enhancing but still not fully developed. But we can assume this process of finalizing the IT policy was a long but inclusive one. So from learning the lesson from previous chapter of implementing and developing IT Policies we have to address every aspect that reflects IT Sectors. An implementation involving both the government and private sector still needs to be encouraged and supported to maximize the potential of IT in Nepal.

11. Critical infrastructure and its protection

Every day, products and services that support our way of life flow, almost seamlessly, to and from our homes, communities, and government. Making this possible are the systems and networks (the roads, airports, power plants, and communication facilities) that make up the infrastructure for our society, an infrastructure often taken for granted. If just one of these systems in the infrastructure is disrupted there could be dire consequences. Some elements of the infrastructure that are essential for operations of the economy and government are the minimum termed as critical infrastructure. As per ITU, critical infrastructure means the computers, computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data, content data and/or traffic data so vital to a country that the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on security, national or economic security, national public health

and safety, or any combination of those matters. Today, there are many critical sectors whose operations depend on ICT in a big way and therefore it becomes very important to protect these sectors from cyber threat.

12. Conclusion and way forward

The virtual nature of the internet, and its recreational aspects, can blind especially young people and novice users to its considerable capacity to do harm in e-governance. The consequence can be horrendous both for organisations (companies, administrative or community organisations) and individuals who fall victim to it. Controlling the technological risks means more than hunting down hackers or setting up technological barriers in enhancing the governance system. The most serious consequences are sometimes due to sheer negligence resulting from incompetence, misconceived or poorly implemented technology, excessive authority for system administrations, mismanagement etc.

It is important to make all internet stakeholders aware of the importance of the security issues involved and of the basic measures which, if clearly stated and intelligently implemented, will strengthen then user confidence in data processing and communication technologies, including the Internet. The internet should be an asset for everyone and not of exclusive benefit to criminal activity. Steps must be taken to foster a culture of multidisciplinary approach to security and to control the risk that information technologies will be used to criminal ends. Both states and organisations must have a strategic vision of these problems. Heightening awareness of security issues must not be limited to promoting a culture of security. There must first be an information technology culture. The stakeholders must also be given the means to learn to manage the technological, operational and information-related risks they incur in using the new technologies. Cyber security concerns cannot be dealt with easily by market forces or by regulation but require a novel mix of solutions. These concerns are not the exclusive domain of economists, political scientists, lawyers, business policy or management experts, or computer specialists or even of national security experts or telecom regulators. Rather, a highly diverse group of stakeholders or key actors-working in their own domains and in concert-has a potential role in orchestrating the set of functions that in aggregate result in an effective cyber security policy.

E-governance is essential about managing future risk and responding to current and past incidents and attacks to build trust from people. Managing future risk requires insight into current and future vulnerabilities and how to prevent or reduce them, the probabilities of a threat, and the costs associated with potential outcomes and how to mitigate them. Responding to current and past incidents and attacks requires knowledge of what has happened, methods of preventing similar incidents from being successful in the future, and possible legal or other remedial actions against the perpetrators. Some of the issues for consideration related to e-governance can be licensing and regulatory measures, legal measure, technical and procedural measures and customer education and capacity building.

References

ADB(Asian Development Bank) (2007). *Aide Memoire of ICT Development Project,* Fact-Finding Mission.

CAN (2010). *National IT Workforce Survey 2005,* Computer Association of Nepal. United Nations e-government survey, 2010

CIA (2010). The world fact book. Retrieved from https://www.cia.gov/library/publications/the- world-factbook/geos/np.html

Dada, D. (2006). The failure of e-government in developing countries: a literature review. *The Electronic Journal of Information Systems in Developing Countries, 26*(1), 1-10.

Heeks, R. (2003). *Most E-Government-for-Development Projects Fail: How Can Risks be Reduced? (Vol. 14).* Manchester: Institute for Development Policy and Management, University of Manchester.

InfoDev (2008). *The E‐Government Handbook for Developing Countries ‐ A Project of InfoDev and the Centre for Democracy and Technology.*

KIPA (2006). *E‐government Master Plan Consulting Report.* Government of Nepal.

Kwon, G. H. (2015). *Electronic Government, E-government and E-Policy.* Graduate School of Governance, Sungkyunkwan University.

MOE (2013). *ICT Master Plan.* Government of Nepal, Ministry of Education, Kathmandu, Nepal.

NITC (2016). *The Information Communication and Technology Master Plan.*

Pariyar, M. P. (2007). E-government initiatives in Nepal, challenges and opportunities. *ACM International Conference Proceeding Series; Vol. 232, Proceedings of the 1st International Conference on Theory and Practice of Electronic Governance,* 280-282. Retrieved from www.egovernance.wordpress.com/2006/10/11/niit-singapore-joint hands for e-governance