Cybersecurity challenges for Bhutan

Pema Choejey[1], Chun Che Fung[1], Kok Wai Wong[1], David Murray[1], Dawa Sonam[2]

[1]School of Engineering and IT Murdoch University, Murdoch, Western Australia

[2]Druknet, Bhutan Telecom Thimphu, Bhutan

Abstract

Information and Communications Technologies (ICTs), especially the Internet, have become a key enabler for government organisations, businesses and individuals. With increasing growth in the adoption and use of ICT devices such as smart phones, personal computers and the Internet, Cybersecurity is one of the key concerns facing modern organisations in both developed and developing countries. This paper presents an overview of cybersecurity challenges in Bhutan, within the context that the nation is emerging as an ICT developing country. This study examines the cybersecurity incidents reported both in national media and government reports, identification and analysis of different types of cyber threats, understanding of the characteristics and motives behind cyber-attacks, and their frequency of occurrence since 1999. A discussion on an ongoing research study to investigate cybersecurity management and practices for Bhutan's government organisations is also highlighted.

I. INTRODUCTION

The world's dependency on the ICTs and the Internet has been growing. The report, '*In the World 2014: ICT Facts and Figures*', published by the International Telecommunication Union (ITU) indicates that almost 3 billion people (40% of the world's population) will have access to the Internet by the end of 2014. Two third of Internet users will be from the developing countries where the growth rate is expected to double in 5 years, from 974 million in 2009 to 1.9 billion in 2014. Similarly, the number of mobile cellular users is estimated to reach almost 7 billion, where the developing countries will again account for more than three quarters of all mobile-cellular subscriptions. In addition, mobile broadband is considered to be the fastest growing market segment and is estimated to grow at the rate of 26% in developing countries compared to 11.5% in developed countries [1,2].

In today's world, Information and Communications Technologies (ICTs), especially the Internet, have become a key enabler for government organisations, businesses and individuals. Both developed and developing countries use ICT in a variety of ways to provide:

- e-Government services (e.g., online filing of tax returns, and visa applications),
- Online businesses (e.g., buying online goods and products),
- Banking and finance services (e.g., paying utility bills and checking account details)
- e-learning (e.g., online courses and distance learning)
- Effective and efficient management of critical infrastructure (e.g., energy and telecom)

However, with the increasing adoption and use of ICT devices such as smart phones and personal computers, Cybersecurity has become one of the key concerns faced by modern organisations in all countries. Cybersecurity is defined as "*preservation of confidentiality, integrity and availability of*

information in the Cyberspace"[3]. Extended definitions of cybersecurity may also involve other properties, such as authenticity, accountability, non-repudiation, and reliability of information and information systems. Cyber-attacks from both internal and external sources have been making headlines in the world news. For example, BBC News [4] reported a malware known as '*Flame*' that attacked Israel and Iran, and infected over 600 specific targets. This malware attack was believed to be a 'complex targeted cyber-attack' and was 'one of the most complex threats ever discovered' by researchers in 2012. Other cases were the Shamoon virus which attacked Saudi oil company [5], the Duqu malware which attacked Iran's computer systems [6], and the Regin spyware program used for stealing data from ISPs, energy companies and airlines companies [7]. These are a few examples of extremely complex, sophisticated and persistent malware used for attacking individuals, businesses and government organisations. As a consequence, nations across the globe have to face the challenges of cyber threats to ensure the stability of their critical infrastructures and ICT systems in order to sustain and survive from persistent and advanced cyber-attacks and potential cyber threats.

Bhutan may not have reached the level of ICT complexity and sophistication of other developed countries, however, it does face similar Cybersecurity problems as the country's government organisations, businesses and individuals are increasingly dependent on ICT tools and the Internet.

The objectives of this paper are to provide:

- an understanding of cybersecurity incidents in the context of Bhutan's ICT situation;
- an analysis of cyber-attacks, sources of threats, and their motives; and,
- an understanding of the factors affecting cybersecurity management and the associated challenges.

This paper is organized into the following sections. Section I provides general introduction about Cybersecurity issues and potential threats. Section II provides a brief ICT development situation in Bhutan and how it contributes to Cybersecurity challenges. Section III examines the cybersecurity incidents reported in the national media and government reports in order to understand their characteristics and motivations behind cyber-attacks. Section IV provides a brief description of study proposal to investigate cybersecurity management and practices in Bhutan's government organisations. Finally, Section IV concludes with discussion and future direction.

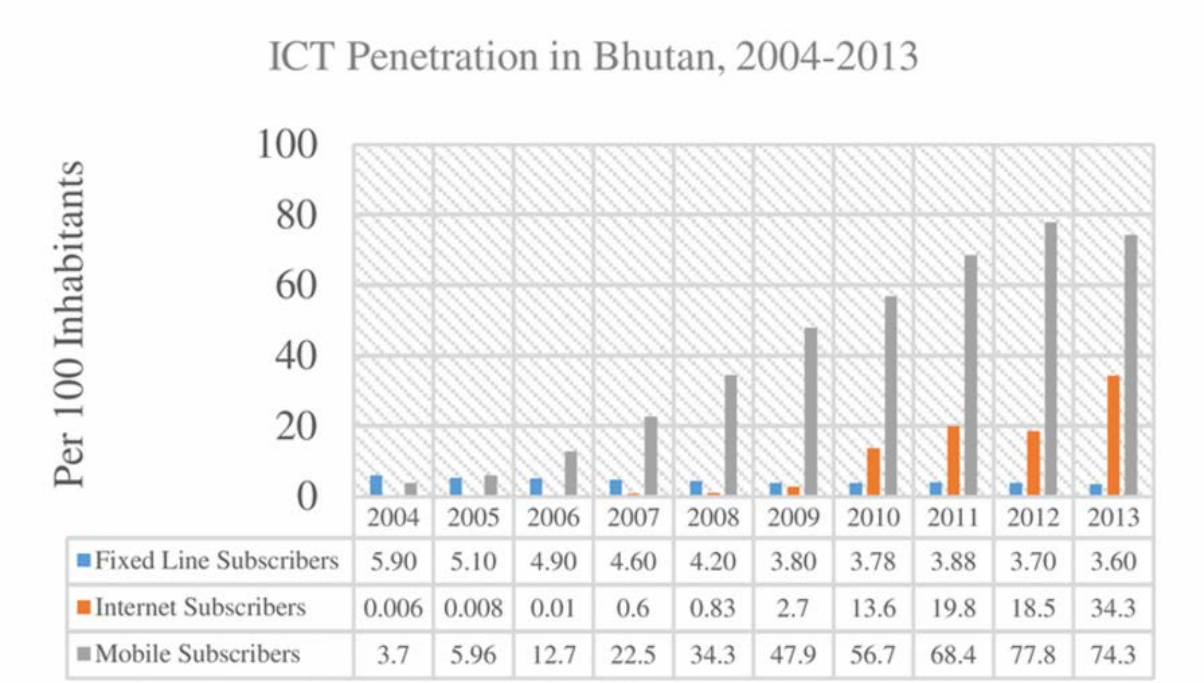
II. BACKGROUND: ICT DEVELOPMENT IN BHUTAN

Bhutan is a small land locked country located in the eastern region of Himalaya. It has a population of about 733,003 people and an area measuring approximately 38,394 square kilometers [8]. Geo-politically, it is surrounded by China and India. For centuries, Bhutan remained isolated until 1960s, when it opened its doors to the outside world.

The engagement with the Internet is relatively recent. Internet was introduced in June 2, 1999 to celebrate the Formula year reign of His Majesty the Fourth King. However, even before the commencement of the Internet, computers were already in use in a number of government offices. There were about 2,500 computers in the country, but few of them were linked. Even fewer were used to share information [9]. Computerisation of government offices started in 1984 with technical and financial support from UNDP [10]. Notwithstanding the fact that computers were introduced earlier than the Internet, their actual use was minimal, modest at best. They were mainly used for basic word processing, database applications and personal communication. The lack of accessibility, cost and very low computer literacy could have been the main obstacles to the proliferation and effective use of computers at that time.

Today, adoption of ICTs, particularly the mobile and the Internet, is widespread in Bhutan. In a very short time span, the number of subscribers using the Internet and mobile services has grown phenomenally. According to the National Statistics Bureau (NSB), there are approximately 557,154 mobile subscribers, which translate into 76 mobiles per 100 inhabitants [8]. Figure 1 shows the rate of ICT penetration in Bhutan from 2004 to 2013. In addition, with respect to the use of social media, there are more than 80,000 Facebook and Social Networking sites users [11]. Furthermore, the annual InfoComm and Transport Statistical Bulletin in 2014 states that the Internet and mobile services are accessible in all 20 *dzongkhags* (or Districts) and 205 *Geogs* (or Village blocks) [12].

Fig. 1. ICT Penetration in Bhutan, 2004-2013, source from [12]



	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
Fixed Line Subscribers	5.90	5.10	4.90	4.60	4.20	3.80	3.78	3.88	3.70	3.60
Internet Subscribers	0.006	0.008	0.01	0.6	0.83	2.7	13.6	19.8	18.5	34.3
Mobile Subscribers	3.7	5.96	12.7	22.5	34.3	47.9	56.7	68.4	77.8	74.3

A. Infrastructure

In terms of infrastructure, Bhutan has extensive fibre-optic-networks connecting all the regional and local headquarters to the central ministries. As a result, nearly every government organisation has established their own local-area-network systems and associated applications such as company websites, web mail and file transfer servers. Bhutan has also established two international gateways - high speed fibre optic cables - to provide reliable and redundant connectivity to the outside world. In addition, about 180 community centres were constructed in the Geogs serving as one-stop-service windows for e-government services [12,13].

B. G2C Services

With respect to content and applications, Bhutan has developed and implemented a number of government-to-citizen (G2C) services such as application for police clearance certificates and business licenses, and submission of income and personal tax returns [14]. This has helped to reduce cost, time and improve transparency of government services.

C. Cybersecurity Challenges

Considering Bhutan's rapid ICT development in a relatively short span of time, it is not unusual to expect the rise in potential cyber threats to information systems, computer networks and data privacy. As interactivity and dependency on ICT devices and network systems grow, proper management of the devices and systems are becoming more complex and sophisticated. While government organisations, businesses and individuals have benefited from the Internet, by way of improving efficiency, productivity and easy access to information and products, the problem of Cybersecurity is becoming more prominent with further development and implementation of ICT programs in Bhutan. For example, the recent incidents of hacking and defacement of a number of Bhutanese websites by external attackers show that information systems and personal information are vulnerable to cyber threats [15,16]. In addition, the ITU's report on "Readiness assessment of Bhutan's Computer Incident Response Team (CIRT)" highlights, even at the government level, a lack of availability of incident handling team for coordination and information sharing with the necessary capabilities and competencies [17]. It was noted that cases of cyber incidents were dealt in ad-hoc manners by computer related departments and there was a lack of documentation on how these incidents were investigated, analysed, remediated and reported.

The following section discusses some of the common cybersecurity threats and cybercrime issues experienced by or affecting Bhutanese ICT networks and information systems, and data privacy

III. CYBER INCIDENTS AND CONSEQUENCES

The available literature on cybersecurity incidents, mostly anecdotal, indicates that Bhutan's government organisations, private businesses and individuals are becoming more vulnerable to many cyber threats. Consequences of cybersecurity incidents range from disrupting access to the internet to the denial of service to online fraud resulting in significant financial losses. Sources of cyber threats originate both from internal and external environments. Hackers and cybercriminals are mainly motivated to display their hacking skills, to cause denial of service and to seek financial gain from the victims. The following describes the common cyber incidents that has affected the Bhutanese ICT consumers and the Internet users.

A. Phishing and Online Banking Theft

Phishing attacks use spam mails or pop-up messages to deceive unsuspecting users into disclosing personal information such as their credit card numbers, bank account information and passwords. For example, Bank of Bhutan reported on botnet phishing scams to warn its customers regarding fake emails sent by international scammers [18]. An example of these emails reads:

Dear Bank of Bhutan (BOB) Customer

Your Account Is Suspended *Your account profile is now outdated, you are required to update your information now. This account (s) has been suspended pending Immediate Activation Below-*

(Activate→) *http://www.bob.beinternet-bankineValid-Activate.asp*

Bob

The botnet scammers in this incident have changed the company's website and the online banking website in a subtle way whereby unsuspecting customers would have considered them to be a real. To counter this targeted phishing attacks, the Bank of Bhutan advised its customers not to respond to the link provided in this email scam and to be wary of such email scams in future.

Phishing attack is likely to become a big concern for financial and banking institutions as more and more banking services are provided online. With increasing sophistication in banking applications, challenges to secure and manage customers' data and sensitive information will increase proportionately.

B. Hacking

Hacking is becoming more prevalent in Bhutan's cyber space. For instance, in 2012 and 2013, a number of cases of cyber hacking and malicious attacks on government websites have been reported. Boaz wrote in his blog site that hackers were taking a "*free joy ride"* to attack government websites including financial banking websites [15,16,19,20]. Table I shows a list of hacked websites of government, corporate and private organisations. Gyalsten [21] reported that "*hackers run amuck in Bhutanese cyberspace"* because of "*vulnerability due to use of open source content management systems"* (e.g., WordPress). Aside from exploiting inherent vulnerability in the content management system, hackers are able to exploit information systems due to failure in updating system patches, and anti-virus definition files on regular basis. Commonly used tools for security breaches were malware, spamware, virus, and phishing. Such incidents are real problems and clearly indicate that Bhutan's information and computer networks are susceptible and vulnerable to cyber threats and attacks.

Table I. List of hacked websites [15]

Government	Education	Corporate and Private
National Soil Services Centre (NSSC)	Bajothang HSS	Bank of Bhutan
National Portal of Bhutan	Jigme Namgyal LSS	Greener Way
Agricultural Marketing and Enterprise Promotion Program, MoAF	Early Learning Centre	Vajrayana Tours and Treks
Climate Summit for the Living Himalayas	Sherub Reldri HSS	Happy Tabi Tours
Construction Development Board (CDB)		Wisdoms Picturs
CCM, Ministry of Health		The Old Students Association of Yangchenphu
The Museum of Monarchy. The Tower of Dzongkha		Genesis Tours
Civil Service Information Systems, Royal Civil Services Commission (RCSC)		Bhutan for Travel
16th SAARC Summit		Travel to Bhutan
		Drukpa Holidays
		Amazing Holidays
		Orgyen Himalayan Expedition

C. Spam/unsolicited Mails

Electronic mail has become the preferred choice for day-to day communication and exchange of information. It is easy, cheap and efficient compared to conventional communication. However, the downside of the increasing use of electronic mail for both personal and official communication is the spam or junk mails. Spam mails are also becoming more prevalent in Bhutan as many Bhutanese users have fallen victims to email scams either out of ignorance or greed. For example, Kuensel [22] reported that "*Recently, a Bhutanese student in India lost nearly a million of his relatives' money, after he was conned into believing that he had won an international lottery. He had received a personal email informing him of his incredible win."* In addition, Chencho [23] reported in Kuensel that "*Bhutanese netizens are being bombarded by spam or unsolicited electronic mail that contain dubious commercial advertisements for products such as Viagra, get-rich-quick schemes, or free access to pornographic sites."* The effects of these unsolicited emails are risk of downloading malware into the computers and reducing the internet speed due to data transfer between the Internet Service Provider (ISP) and the PC users. Furthermore, in a high profile case of internet scam [24], more than 150 Bhutanese in the eastern Bhutan have become the victims of internet scammers known as Unipay2U and Visa. They have lost close to Nu. 10 million (approx. 200,000). Some are said to have lost their entire life savings. Similarly, a Thimphu electronic supply firm, who nearly lost about 191,000 USD in a cyber-fraud case, lodged a criminal case against his supplier in Dubai, United Arab Emirates [25].

D. Viruses

Viruses range from being a simple source of nuisance to creating a major disruptions to the information systems and networks. While cases of virus attacks are more prevalent than any other security incidents in Bhutan, little literature exists on virus incidents. In most cases, incidents of viruses are rarely acknowledged nor reported publicly. However, a case of viruses clogging Bhutan's information highways has been reported in 2010. In his popular blog, ThimphuTech.com, Boaz [26] wrote "*It seems that the number of 'healthy' computers in Bhutan can be counted on a single hand. Many computers that I'm running into show clear symptoms of a sick machine, some of them so terminally ill that the only cure is the IT equivalent of a brain transplant, i.e., re-formatting the hard disk.* "The consequence of viruses attacking so many computers simultaneously is the clogging of the networks connecting to the internet. Schmueli ended his blog asking question "…are *we paying for all those bandwidth-gulping viruses?"* [26]. Thus, it does indicate that the impact is not only limited to disruption to network access, but also the price the subscribers has to pay. The perceptions that Boaz has had and his experiences of stumbling into many computers with viruses may not be a random case, but a normal perpetual incidents shared by many users. However, most of the cases remained unreported as there is no official contact person or authorised entity dealing with such cases.

E. Pornography

Pornography which entails use, consumption or distribution of explicit sexual contents is another contentious issue that has grabbed the Bhutan's attention in recent times. Sexually explicit contents ranging from still images to short video captured using video camera and smartphones were in wide circulation among Bhutanese users. For instance, in 2014, BBS [27] reported that "*Numbers of amateur pornography or obscene clips, especially shot on mobile phones, have gone viral among the local mobile users."* The porn clips were purported to be leaked mainly through using a mobile apps called WeChat, which is freely available for downloads on smartphones. Porn clips were also distributed using the internet. This incident has not only raised serious concern among people, especially women, about their security and privacy, but also made government to think on what measures need to be put in place including who should be made responsible to prevent such incident in future or to protect the safety and security of vulnerable young girls and women.

IV. RESEARCH STUDY PROPOSAL

As in other developed and developing countries, Bhutan is likely to face the same security challenges and issues. The threats to government organisations and information assets from cyber space is foreseen and recognised in the Bhutan's E-Government Master Plan which states [13]:

"With vision of an ICT enabled information society and with increasing ICTisation taking place, our dependence on these ICT systems and services is growing by the day. Consequently, the inherent threats of the cyber world would have not only become a reality but a real danger to our daily lives."

However, the cyber incidents described earlier are mostly anecdotal stories reported in the printed and social media. To the best of the authors' knowledge, no formal empirical studies have been conducted on how Bhutan is actually dealing with cyber issues, what security measures are in place, and how prepared Bhutan is to effectively respond to cyber incidents and implement measures to prevent future cyber-attacks.

Therefore, using a qualitative and quantitative methods, it is proposed to carry out an empirical research study which address this broad research question:

How are Bhutan's government organisations positioned against cyber-threats and cybercrimes, and how can cybersecurity management be improved in order to reduce its risks and impacts as organisations dependency on ICTs grows?

Bhutan offers a unique case study to investigate. First, cybersecurity is a national concern not only from the view point of security to national infrastructure like telecom and energy, but also is the concern from the view point of social and economic security, as Bhutan is geo-politically situated between India and China. Second, Bhutan is a resource poor country with limited resources of its own. Realisation of national development plans and initiatives are dependent on foreign aids from developed countries, non-profit organisations and international organisations such as the World Bank. Therefore, financing cybersecurity program may be a challenge as there are competing priority sectors like health and education. Third, as mentioned earlier in the background, Bhutan's engagement with information society as late entrant provides ample opportunity for Bhutan to begin security on a clean slate and to avoid thinking security as an after-thought, which could lead to mistakes and pitfalls that have occurred in the developed countries.

V. CONCLUSION

This paper presents an overview of cybersecurity challenges in Bhutan. From the viewpoint of Bhutan's cyberspace, cases of specific cybersecurity incidents have been reviewed and documented. Common cyber threats facing government organisations, business and individuals are phishing, hacking, viruses, spam and pornography. However, these incidents of cyber-attacks and cybercrimes are mostly anecdotal stories reported in print and social media. Therefore, it is proposed to conduct an empirical study to investigate cybersecurity management and practices in government organisations. The research findings from this study will result in creating a knowledge-base and understanding of how small developing nations like Bhutan addresses the concept of cybersecurity and in particular, the cybersecurity management and practices, in order to achieve cybersecurity goals of confidentiality, availability and integrity. In addition, the outcome from this research study will have implications to similar developing nations whereby they may learn from the proposed security frameworks and models for adaptation in order to avoid likely security pitfalls.

REFERENCES

[1] International Telecommunication Union, *The World in 2014: ICT Facts and Figures*: ITU, 2011.

[2] Internet Society, *Global Internet Report*: Internet Society, 2014.

[3] ISO/IEC, "Information technology — Security techniques — Guidelines for cybersecurity," ed. Switzerland: ISO/IEC, 2012.

[4] D. Lee, "Flame: Massive cyber-attack discovered, researchers say," in *BBC News*, ed: BBC, 2012.

[5] T. Sandle. (2012, December 14). *Shamoon virus attacks Saudi oil company*. Available: http://www.digitaljournal.com/article/331033

[6] BBC, "Iran says it has 'controlled' Duqu malware attack," in *BBC News*, ed: BBC, 2011.

[7] BBC, "Security firms uncover 'sophisticated' Regin spyware," in *BBC News*, ed: BBC, 2014.

[8] NSB, "Bhutan at a Glance," National Statisitcs Bureau, Ed., ed. Thimphu: Royal Government of Bhutan, 2013.

[9] R. Gruys. (2000) Information Technology in Bhutan – Propelling a Himalayan Kingdom into the Information Age. *Tashi Delek, Druk Air In-Flight Magazine*. Available: http://www.bluepeak.net/bhutan/IT/it-in-bhutan.pdf

[10] GNHC, "8th Five Year Plan," Gross National Happiness Commission, Ed., ed. Thimphu: Royal Goverment of Bhutan, 1997

[11] "Internet World Stats: Usage and Population Statistics," 2014, n.d.

[12] MoIC, "Annual InfoComm and Transport Statistical Bulletin," Ministry of Information and Communications, Ed., 5 ed. Thimphu: Royal Governemtn of Bhutan, 2014.

[13] MoIC, "Bhutan e-Government Master Plan," Ministry of Information and Communications, Ed., ed: Royal Government of Bhutan, 2013.

[14] G2C, "G2C: Service Delivery Initiative," ed. Thimphu: Royal Government of Bhutan, n.d.

[15] B. Shmueli, "RCSC, BoB, RGoB Portal among tens of hacked websites," in *ThimphuTech.com: Technology, food and happiness in Bhutan* vol. 2014, ed: ThimphuTech.com, 2012.

[16] B. Shmueli, "Bhutan's domain registration website hacked," in *ThimphuTech.com: Technology, food and happiness in Bhutan* vol. 2014, ed: ThimphuTech.com, 2014.

[17] ITU, "Cybersurity: Readiness Assessment for Establishing National CIRT," International Telecommunication Union2012.

[18] BoB. (2013, 14/01/2015). *New Phishing Targets BOBL Customers: Botnet Phishing Scam*. Available: http://www.bob.bt/2013/03/new-phishing-targets-bobcustomers/

[19] B. Shmueli, "DrukNet Servers Still Under Attack," in *ThimphuTech.com: Technology, food and happiness in Bhutan* vol. 2014, ed: ThimphuTech.com, 2012.

[20] B. Shmueli, "Hackers enjoy a free ride using RGoB, OAG, TCC, and other Bhutanese websites," in *ThimphuTech.com: Technology, food and happiness in Bhutan* vol. 2014, ed: ThimphuTech.com, 2012.

[21] G. Dorji. (2012). *Hackers run amuck in Bhutanese cyberspace*. Available: http://www.kuenselonline.com/hackers-run-amuck-inbhutanese-cyberspace/

[22] Kuensel. (2009, 01/12/2014). *Too Good to be True*. Available: http://www.kuenselonline.com/editorial-toogood-to-be-true/#.VHyV6OlxnVI

[23] C. Tshering. (2003, December 1). *Spam Mail.* Available: http://www.kuenselonline.com/spam-mail/#.Us0NC_QW2So

[24] BBS. (2011, November 04). Investigation into internet scam launched. Available: http://www.bbs.bt/news/?p=6113

[25] T. Palden. (2014, November 04). *A cyber fraud victim seeks justice* Available: http://www.kuenselonline.com/a-cyberfraud-victim-seeks-justice/#.VFiJ_-lxnIU

[26] B. Schmueli, "Are Viruses Clogging Bhutan's Information Highways?," in *ThimphuTech.com: Technology, food and happiness in Bhutan*, ed: ThimphuTech.com, 2010.

[27] BBS. (2014, 20/12/2014). *Cybercrime: Private affairs going public.* Available: http://www.bbs.bt/news/?p=42097