Perceptions of Cybersecurity in Government Organizations: Case Study of Bhutan

Pema Choejey, David Murray, Chun Che Fung

Abstract**—**Bhutan is becoming increasingly dependent on Information and Communications Technologies (ICTs), especially the Internet for performing the daily activities of governments, businesses, and individuals. Consequently, information systems and networks are becoming more exposed and vulnerable to cybersecurity threats. This paper highlights the findings of the survey study carried out to understand the perceptions of cybersecurity implementation among government organizations in Bhutan. About 280 ICT personnel were surveyed about the effectiveness of cybersecurity implementation in their organizations. A questionnaire based on a 5 point Likert scale was used to assess the perceptions of respondents. The questions were asked on cybersecurity practices such as cybersecurity policies, awareness and training, and risk management. The survey results show that less than 50% of respondents believe that the cybersecurity implementation is effective: cybersecurity policy (40%), risk management (23%), training and awareness (28%), system development life cycle (34%); incident management (26%), and communications and operational management (40%). The findings suggest that many of the cybersecurity practices are inadequately implemented and therefore, there exist a gap in achieving a required cybersecurity posture. This study recommends government organizations to establish a comprehensive cybersecurity program with emphasis on cybersecurity policy, risk management, and awareness and training. In addition, the research study has practical implications to both government and private organizations for implementing and managing cybersecurity.

Keywords**—**Awareness and training, cybersecurity, cybersecurity policy, risk management, security risks.

I. Introduction

BHUTAN is a small, landlocked and developing country bordering India in the south and China in the north. The ICTs, particularly the Internet, is relatively a recent phenomenon. The Internet was first introduced in Bhutan only in June 1999. However, in more than a decade, Bhutan has seen progressive ICT development with government undertaking several initiatives to further the ICT growth, namely they are:

1) Establishment of the new Information and Communication Ministry in 2003 to spearhead ICT development in the country.
2) Formulation and adoption of Bhutan ICT Policy and Strategy Paper, 2004, which focuses on development of ICT Policies, Infrastructure, Human Capacity, Content and Applications [1].
3) Establishment of second international fibre connectivity to India to create reliable and redundant Internet connectivity.
4) Formulation and enactment of Bhutan's Information, Communications and Media Act [2].
5) Adoption of E-Government Master Plan, 2013, with a vision to create a knowledge based economy and information society [3].

These plans and policies of the government have facilitated many government organizations to create their own websites and develop internet facing information systems to improve work efficiency, deliver public services and to communicate electronically. More websites are being created as information portals to provide access to government services. Email is being used for official correspondence. Google Apps are being used for collaboration and event management. Data centers are being built for storage and backup of information systems and files [4]. Thus, all these tools and applications are changing the cyber environment while increasing organizational efficiency, improving work productivity, reducing cost, and increasing revenues. Consequently, government's dependency on ICT and the Internet has been increasing rapidly.

However, government information and information systems are becoming increasingly exposed to cyber risks. Many cyber criminals have found opportunities to exploit inherent vulnerabilities and weaknesses in information systems and human naivety. The recent cyber incident of online financial fraud that led the Bank of Bhutan to transfer 16 million (in Bhutanese currency) to three different accounts in India, Malaysia and Thailand based on a fake e-mail letter sent from the Royal Audit Authority, Bhutan is an indication that Bhutan is facing emerging cyber threats[5]. According to [6], common cybersecurity challenges facing Bhutan are hacking, malware, phishing, and denial of service.

These cyber threats are major causes of concern for the government and for the society as they are detrimental to the economy and security of the country. Information and information systems including networks need protection from cyber risks which cause unintended harm and disruptions to proper functioning of the organization. Among others, a notable government initiative to counter such cyber threats is the Bhutan Information Management Security Policy [7]. The ISMP is based on the ISO 27002 Standard Code of Practice for Information Security Management. The Standard provides guidance and best practices recommendations to be implemented based on the security requirements of individual

Pema Choejey is a Ph.D. student with the School of Engineering and IT, Murdoch University, 90 South St, WA 6150. (mobile: +61-452-509-677; e-mail: P.Choejey@murdoch.edu.au).

David Murray is the Senior Lecturer with the School of Engineering and IT, Murdoch University (e-mail: D.Murray@murdoch.edu.au).

Chun Chu Fung is the Emeritus Professor with the School of Engineering and IT, Murdoch University (e-mail: L.Fung@murdoch.edu.au).

organizations. However, there is no literature indicating how successfully the government agencies have implemented the policy.

To our best knowledge, this is the first cybersecurity perception survey being done to understand the effectiveness of cybersecurity practices. There is little understanding of how government organizations are managing cybersecurity issues being brought in with increasing use of ICT and its related technologies. Understanding the current state of cybersecurity is important to improve cybersecurity planning and its implementation to meet the security requirements of availability, integrity and confidentiality. Therefore, the main purpose of this study is to understand the effectiveness of cybersecurity implementation in various branches of the government.

The paper is organized as follows. In Section I, an overview of cybersecurity and related cyber concepts were discussed to define Cybersecurity and understand the current issues and challenges of Cybersecurity. Section II reviews the cybersecurity literature in the context of Bhutan and highlights the cybersecurity frameworks that can be used to implement and manage cybersecurity. Section III discusses the research method and materials. Section IV presents the data analysis and findings from the survey results. Section V then discusses the cybersecurity challenges facing Bhutan and recommends a managerial and technical approach to address the problems and challenges of cybersecurity in Bhutan. Section VI concludes the paper.

II. Literature Review

A. Studies Related to Cybersecurity in Bhutan

In 2003, an E-Readiness survey was conducted to gauge Bhutan's readiness to embrace the Internet and ICT related technologies [8] for digital transformation (e.g., e-government) and network economy (e.g., e-commerce). The study mainly assessed readiness in: i) network, ii) human, iii) infrastructure, and iv) legal capacity. However, the study has not studied readiness in the aspect of cybersecurity, which ideally would have been good if included. In addition, this study was the first and only readiness survey ever conducted in Bhutan.

In 2009, the International Telecommunication Union (ITU) conducted an assessment of Computer Incident Response Team (CIRT) covering India, Bhutan, Bangladesh and India [9]. The main purpose of the study was to understand and gain knowledge on how these countries are managing and responding to cyber incidents. The study's focus was on understanding cybersecurity challenges facing these countries and measures taken to respond to these challenges, especially establishment of CIRT to respond, coordinate and share information related to cyber incidents. While cybersecurity incident management forms one of the core domains of cybersecurity management, this study has not assessed other security domains such as cyber policy, organisational security and others.

A PKI (Public Key Infrastructure) based security framework for e-government platforms in Bhutan was proposed in [10]. The study performed SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis of the e-government situation from the security perspective and proposed the PKI solution derived from PKI solutions implemented in India, Korea and Taiwan largely taking the best practices of PKI implementation of these countries. Although, this study is related to aspects of information security for e-government platforms, the study is specific to the use of cryptography technologies as solution to the e-government security issues.

The most recent study on cybersecurity in Bhutan was an assessment of cybersecurity capability maturity jointly conducted by the Global Cyber Security Capacity Centre and the World Bank [11]. The study assessed maturity levels in five dimensions: i) policy and strategy, ii) culture and society, iii) education, training and skills, iv) law and regulation, and v) organisation, standards and technology. The study concluded that Bhutan is at the start-up level of maturity. It means that Bhutan neither has a capacity nor has undertaken concrete actions with respect to some factors in each dimension. While the study provides broad perspectives on cybersecurity from a national viewpoint, it does not provide insights and understanding of how government organizations have implemented cybersecurity activities and what people think and believe about the effectiveness of cybersecurity implementation. Further, their research method is based on group discussion and analysis of available documents.

B. Cybersecurity Categories Used in the Study

This study used 7 security categories, they are:

1) Security policy
2) Risk management
3) Access controls
4) Awareness and training
5) System development life cycle
6) Communications and operations management
7) Incident management

Selection of these cybersecurity categories are guided by the government's Information Management Security Policy [7], ISO 27001 Standard [12], and NIST's Guide for Assessing the Security of Controls in Federal Information Systems and Organizations [13]. These frameworks are implemented worldwide as security standards for cybersecurity management. The frameworks are divided into 10 to 20 functional areas sometimes called domains or control areas. They are based on risk management methodology and involves the use of security controls for protecting and preventing security risks. However, it should be noted that there is no one-to-one mapping between the categories used here and those found in the security frameworks.

Selection of categories are also based on our earlier studies [14, 15], and recent developments being undertaken by the government organizations in Bhutan.

III. Methods and Materials

A. Research Method and Instrument

A quantitative survey method was used for data collection. Questions were framed to elicit information and knowledge on: a) Cybersecurity Policy, b) Risk Management, c) Awareness and Training, d) Software Development, e) Incident Management, f) Access Control, and g) Operations and Communication Management. Each cybersecurity category has several items to measure cybersecurity effectiveness. A 5 point Likert scale, which was invented by Rensis Likert [16], was used to measure and assess the perceptions of respondents where 1 = strongly disagree, 2 = disagree, 3 = neutral (neither agree nor disagree), 4 = agree, and 5 = strongly agree. While there are no theoretical reasons to limit response options to 5 levels, however, empirical research study in [17] has found that 5 or 7-point scales produced slightly higher mean scores, difference was statistically significant at p=0.04, than 10-point format. The other problem with long scales beyond 5 or 7-point is the difficulty of labelling the response options as the "shades of agreement become as hard for survey designer to express as they are for respondent to distinguish" [18]. In addition, compared to random rating scales (e.g., rating from 1 to 20), 5-point scale use a neutral option to help avoid forcing respondents to expressing agreement or disagreement when they lack clear opinion or views.

B. Survey Sample

The survey population were ICT professionals working in various Bhutanese government organizations. ICT professionals were requested to participate in a survey questionnaire conducted online using Survey Monkey. Emails were sent to 280 ICT professionals (respondents). The contact list of potential respondents of ICT professionals was obtained from the Ministry of Information and Communications. Information about the purpose of the survey including the privacy and confidentiality information of the responses were included with the online survey questionnaire. Out of the 157 responses received, 109 respondents fully completed the questionnaire, which indicates that the response rate was 56.1% (157/280), and the completion rate of the responses were 69.4% (109/157). The demographic characteristics indicate that more than 60% of respondents were male with 66% falling in the 25-34 age group.

C. Survey Design Process

The survey questionnaire was designed to cover different aspects of cybersecurity categories discussed earlier. Questions were framed carefully to make them easy to understand and avoid biases of respondents. The design process also includes reviews by ICT experts from Bhutan and subsequent approval by the Murdoch University Human Research Ethics Committee (2014/148). Those design processes ensure that the questions meet the national and university quality and ethical standards, and that questions are well organized including the length of the survey. Furthermore, a pilot study consisting of 10 senior Bhutanese ICT professionals studying in Australia and Thailand was also conducted to ensure the reliability and validity of questionnaire. The questionnaire was found acceptable requiring no major alterations to the questions.

IV. Results

A. Key Findings

The study used descriptive statistics to analyse the survey results. A frequency distribution for each question item has been calculated and aggregated into various cybersecurity management practices as in Fig. 1. Some of the key findings from the survey results are:

1) Cybersecurity policy: 40% of respondents believe that cyber policy is effective while 32% think that cyber policy is ineffective.
2) Risk management: 41% of respondents also believe that cybersecurity risk management is ineffective.
3) Access controls: 63% of respondents believe that access controls are largely effective.
4) Awareness and training: 45% of respondents believe that cybersecurity training and awareness programs are ineffective.
5) System development life cycle: Only 34% of respondents think system development life cycle is effective.
6) Incident management: 34% of respondents think cybersecurity incident management is ineffective while 26% think otherwise.
7) Communications and operations management: 40% of respondents believe it to be effective while 24% disagree with the statements.

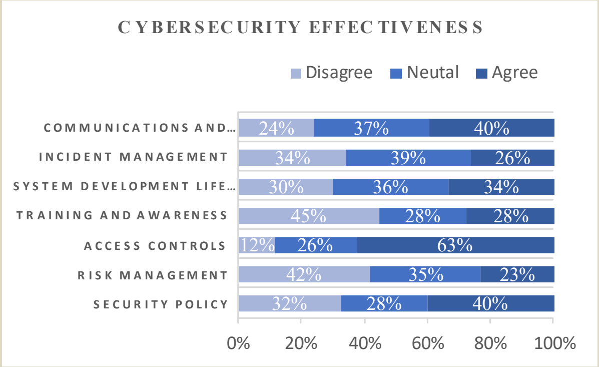

Fig.1 Aggregated perceptions of cybersecurity effectiveness

In summary, the results show slight favourable perceptions towards cybersecurity policy, system development, operation management and access controls. However, the proportion of respondents who believe cybersecurity implementation is effective is less than 50% in all categories. Similarly, the results indicate negative perceptions towards risk management, awareness and training, and incident management practices. Further, the results also show that there are respondents ranging from 26% to 39% who neither agree nor disagree with the questions, hence forming a neutral group. Since the overall weighted mean score of cybersecurity practices is just 3.04, in general, it may be concluded that cybersecurity implementation in government organisation is less effective.

The research findings suggest that cybersecurity implementation needs further improvement, particularly in areas where respondents' have rated very poorly. The study recommends to implement risk management, awareness and training, and incident management to improve cybersecurity. Without strong cybersecurity in place, government initiatives such as Government to Citizens (G2C) services, data center, multiple community tele-centers, and implementation of broadband infrastructure will not succeed. Cybersecurity will not only be critical to achieving organisational goals and objectives, but also for nation's economy, security, and critical infrastructure protection.

V. Discussions

Firstly, the survey results described earlier are based on the responses provided by the ICT professionals working in different government organisations. Hence, the findings fairly reflect the true state of cybersecurity situation in Bhutan. The study concludes that cybersecurity implementation is inadequate to meet the security requirements and objectives of the government organisations.

Secondly, it must be noted from the survey results that there are many respondents (ranging from 26% to 39%) who have neither agreed nor disagreed to the questions. Possible reasons for respondents not having any positive or negative feelings towards any cybersecurity practices may be due to: i) limited/insufficient knowledge of cybersecurity and ii) little organisational and personal experience of cybersecurity issues.

Finally, this survey was limited only to government organizations. Including survey participants from the corporate and private organizations may have led to different perspective and thinking. Furthermore, inclusion of survey participants of non-ICT people may result in different findings.

VI. Conclusions

This paper presents the survey results of cybersecurity perceptions among government organizations in Bhutan. The survey findings show that respondents have favourable perceptions towards cybersecurity policy, system development, operation management and access controls. On the other hand, they have reflected negatively towards risk management, awareness and training, and incident management. There are also respondents who were undecided – who neither agree nor disagree, which we believe may have changed the survey results had they expressed their opinions. Implementation of cybersecurity practices where respondents think and believe to be ineffective would help to improve cybersecurity. This study therefore recommends government organizations to establish a cybersecurity framework encompassing cyber policy, risk management, system development life cycle, incident management, access controls and cyber education.

This study is part of an ongoing research study and further results will be presented in the future.

Acknowledgement

The authors would like to thank Ms. Dechen Chhoeden, Department of IT and Telecom, Bhutan for her support in getting the approval and letter of support for this research study from the Ministry of Information and Communications and for subsequent support in providing the potential list of ICT professionals. The authors would also like to thank Mrs. Passang Dema, Office of Attorney General for her support for the conduction of the survey study.

References

[1] MoIC, "Information and Communications Technology (ICT) Policy for Bhutan: A White Paper ", M. o. I. a. Communications, Ed., ed. Thimphu: Royal Government of Bhutan, 2003.
[2] RGoB, "Bhutan Information Communications and Media Act," ed. Thimphu: Royal Government of Bhutan, 2006.
[3] MoIC, "Bhutan e-Government Master Plan," Ministry of Information and Communications, Ed., ed: Royal Government of Bhutan, 2013.
[4] GNHC, "Eleventh Five Year Plan Volume I: Main Document," G. N. H. Commission, Ed., ed. Thimphu: GNHC, 2013.
[5] N. Gyeltshen, "BoB transfers Nu 16M based on fake e-mail," in *BBS Online*, ed. Thimphu: Bhutan Broadcasting Service, 2016.
[6] P. Choejey, C. C. Fung, K. W. Wong, D. Murray, and D. Sonam, "Cybersecurity challenges for Bhutan," in *Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2015 12th International Conference on*, 2015, pp. 1-5.
[7] MoIC, "Information Management and Security Policy," M. o. I. a. Communications, Ed., ed: Royal Government of Bhutan, 2009.
[8] MoC, "Bhutan e-Readiness Assessment," T. D. o. I. Technology, Ed., ed: Ministry of Communications, 2003.
[9] ITU, "Cybersurity: Readiness Assessment for Establishing National CIRT," International Telecommunication Union2012.
[10] B. Nono, "Proposing a Government PKI in Bhutan: A Solution to e-Government Security Requirements " 2011.
[11] T. Roberts, "Building Cyber-Security Capacity in the Kingdom of Bhutan," G. C. S. C. Centre, Ed., ed: University of Oxford undated.
[12] ISO/IEC 27001, "Information technology – Security techniques – Information security management systems – Requirements," 2005.
[13] NIST, "SP 800-53: Recommended Security Controls for Federal Information Systems," *October,* vol. 31, p. 9, 2003.
[14] P. Choejey, C. C. Fung, K. W. Wong, D. Murray, and S. Dawa, "Cybersecurity Challenges for Bhutan," presented at the 12th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, Hua Hin, Thailand, 2015.
[15] P. Choejey, C. C. Fung, K. W. Wong, D. Murray, and H. Xie, "Cybersecurity Practices for E-Government: An Assessment in Bhutan," 2015.
[16] R. Likert, "A technique for the measurement of attitudes," *Archives of psychology,* 1932.
[17] J. G. Dawes, "Do data characteristics change according to the number of scale points used? An experiment using 5 point, 7 point and 10 point scales," *International journal of market research,* vol. 51, 2008.
[18] R. Johns, "Likert items and scales," *Survey Question Bank: Methods Fact Sheet,* vol. 1, 2010.