Cybersecurity Practices for E-Government: An Assessment in Bhutan

Pema Choejey, Chun Che Fung, Kok Wai Wong, David Murray and Hong Xie
School of Engineering and IT, Murdoch University, Murdoch, Western Australia
mail2pemac@gmail.com, [L.Fung | K.Wong | D.Murray | H.Xie]@murdoch.edu.au

Abstract— **The main goal of e-government implementation is to improve the effectiveness, efficiency and quality of public service delivery using Information and Communication Technologies (ICT). However, its success is dependent on the provision of information security goals such as confidentiality, integrity, availability and trust. Therefore, cybersecurity is vital for the successful adoption of e-government systems. This paper presents an assessment of cybersecurity practices, cyber threats and other factors affecting effective implementation of cybersecurity program in government organizations in Bhutan. Selected cybersecurity practices included in the study were cyber policy, risk management, training and awareness, and access controls for protection of network including mobile computing devices. Out of 280 potential respondents, 157 respondents completed the survey. The results show that, in many organizations, there is very limited use of or a lack of formal cybersecurity policy, risk management, awareness, or incident management practices. The results also indicate that many organizations have either suffered from, or been affected by, cybersecurity threats such as malware, hacking and phishing scams. The study recommends both managerial and technological practices to improve cybersecurity posture of government organizations and to improve people's level of trust and confidence in e-government services.**

Keywords—cybersecurity; cybersecurity policy; risk management; awareness and training; cyber threats; e-government;

I. INTRODUCTION

E-Government refers to 'the use of or application of information technologies' such as Wide Area Network (WAN), Internet and the World Wide Web (WWW) by the government to 'transform relations with or to reach out to citizens, business and other arms of government' [1, 2]. E-government implementation goals, among others, is to improve the effectiveness and efficiency of public service delivery. The benefits of e-government adoption are many [1]:

- Facilitate faster delivery of services to citizens;
- Improve interactions between government, citizens, business and industry;
- Empower citizens through access to knowledge and information; and
- Make government operations and functions more efficient and effective.

Many countries have therefore started implementing e-government initiatives as it has been proven to be useful in providing efficient and quality services to citizens and businesses. Bhutan as one of the developing countries, has embraced e-government development.

According to the E-Government Masterplan, Bhutan's ICT vision is to become "*An ICT-Enabled, Knowledge-based Society as a Foundation for Gross National Happiness*" [3]. Underlying the vision are the three main goals: ICT for Bhutanese Information Society, ICT as a key enabler for sustainable economic growth and ICT for Good Governance, see Figure 1. Each of these goals has several strategic action plans and activities, which when combined and implemented successfully can help to achieve the vision.

While there are many important initiatives undertaken by the Bhutanese government, one of the most notable forms of e-government initiative implemented so far is the Government-to-Citizens (G2C) services (see e-government classification categories in [4]). The main objective for implementing the G2C applications is to improve the efficiency and quality of service delivery to citizens (e.g., online tax filing and birth registration) by improving accessibility, optimising human resources and reducing service delivery time [5].

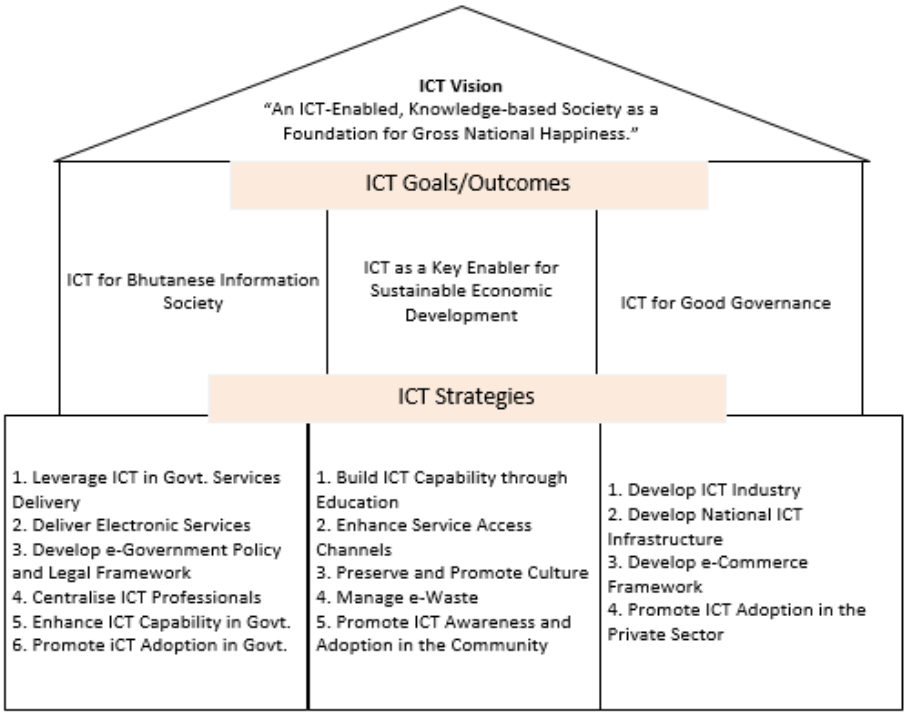


Fig. 1: ICT Vision, Outcomes and Strategies, adapted from [3]

Notwithstanding the fact that the Internet and Television was introduced only in 1999, and despite Bhutan being a least developed country constrained by limited resources and lack of qualified ICT professionals, Bhutan's e-government development growth so far has been commendable among similar countries. For example, according to the UN E-Government Survey [6] conducted in 2014, Bhutan was ranked 143 out of 193 member states in the E-Government Development Index (EGDI). This was an increase of 9 points compared to EGDI ranking of 152 in 2012. Similarly, in a study conducted to assess the G2C and G2B aspects of key ministry e-governance websites of South Asian Association for Regional Cooperation (SAARC) countries, Bhutan and Bangladesh have scored the highest [7].

However, e-government implementation is not without obstacles and challenges. Several studies on e-government have pointed out that cybersecurity being, besides political, economic and cultural factors, one of the key concerns for many government organizations [4, 8]. ISO/IEC defines cybersecurity as "the preservation of confidentiality, integrity and availability of information in the Cyberspace." [9]. Cybersecurity is essential for e-government implementation because the underlying infrastructure constituting e-government applications consist of computing devices, hardware and software, networks and information systems, which are inherently insecure by design or have system vulnerabilities. In the context of Bhutan, cybersecurity threats such as malware, hacking, denial of service and phishing have been on the rise ever since the Internet was introduced in Bhutan [10]. Therefore, ensuring confidentiality, integrity and availability of information and networks are vital for successful adoption of e-government [11]. The protection of e-government services and information from cyber threats has become even more crucial for government organizations in Bhutan as they consolidate their efforts to make government services accessible from anywhere, anytime.

Thus this paper presents an empirical assessment of cybersecurity practices of government organizations in Bhutan. This assessment aims to provide an: a) understanding of existing security measures implemented by government to protect their information assets, b) understanding of established cyber policies and procedures that form the cornerstone of effective cybersecurity program implementation, c) understanding of level of awareness and training, and d) understanding of incident handling and

response capability to deal with cybersecurity incidents. Based on the gap analysis of the current state of cybersecurity, a set of technological and managerial practices are recommended to improve the cybersecurity posture. To the best of our knowledge, this study is the first of its kind to be conducted in Bhutan related to cybersecurity.

The paper is organized into the following sections. Section I provides an overview of e-government and its potential benefits to government, citizens and businesses. Section II presents the related works in the context of developing countries. Section III describes the research methods and materials. Section IV presents the analysis and results. Section V proposes relevant recommendations based on the survey findings to improve the cybersecurity posture, and finally, Section VI presents the conclusion summarizing the purpose and findings of the study.

II. RELATED WORKS

While there are many studies related to information security for e-government, this section provides some of the findings carried out in the context of developing nations.

A. Cybersecurity Policy, Awareness and Threats

AlGarni [12] investigated the issue of information security policy for e-government in Saudi Arabia. The study examined the effectiveness, vulnerabilities and threats of the system. Based on study findings, AlGarni reported that common cybersecurity challenges and threats facing e-government adoption in Saudi Arabia were hacktivists, software errors and terrorists. Saudi Arabia also faces challenges of lack of awareness, inadequate training of the employees dealing with e-services and low trust in the e-government applications. In a study conducted in Nigeria regarding e-government implementation benefits, risks and barriers [13] found information security, particularly the threat to personal identity and privacy of information, to be a risk to successful implementation of e-government. Although not directly linked to information security, the study also found lack of knowledge, awareness, and implementation policy as barriers for realisation of e-government aspirations.

B. Conceptual Frameworks and Maturity Models

A managerial conceptual framework was proposed in [14] for e-government security management within the context of developing nations. The framework can be used as an analytical tool for investigation and clarification of security culture, infrastructure and managerial roles affecting the effectiveness of e-government security programs. In other words, effectiveness of e-government security is likely to be influenced by variables such as organisational culture, management commitment, security mechanism, to mention a few. An information security maturity model for secure e-government services [15] was proposed based on socio-technical approach. The model was evaluated by conducting a survey study in six organizations in Tanzania. The model can be used for revealing and understanding issues concerning both technical and non-technical security services.

C. International Guidance and Cybersecurity Strategy

Tagert [16] argues that the common approaches and frameworks proposed by the developed nations and international organizations such as ITU's cybersecurity framework [17] for building cybersecurity are not suitable for developing nations, as they are designed and developed based on the perspectives, experiences, cultural settings and ICT maturity levels of the developed nations. Targert use the guidance for establishment of the Computer Security Incident Response Team (CSIRT) model as a case in point to argue why the model is not suitable for developing nations, as many countries have differing cultural context, ICT maturity levels and socio-economic conditions. Newmeyer [18] conducted a qualitative case study to examine the perceptions of cybersecurity readiness of the government and private sector in Jamaica, especially the current policy development process to respond to cyber threats. While Jamaica has started the process of developing a cybersecurity strategy, the author found a lack of formal cyber policy that may inhibit the coordination of cyber response against the potential cyber incidents. The author also found a lack of awareness and education program, which is vital to inform consumers about the risks of using mobile devices and applications.

Some of the security challenges facing developing nations suggested by literature are:

- Cybersecurity policy;
- Awareness and training;
- Incident handling and response capabilities;
- Technical and managerial controls to secure information;
- Social and cultural differences and context;

As no specific study on Bhutan has been done so far, the above security issues provide the basis to assess cybersecurity practices among government organizations in Bhutan.

III. METHODS AND MATERIALS

A quantitative survey method was used for data collection. The survey questionnaire was designed and developed based on ISO/IEC and NIST frameworks [19-21] best practices and also issues highlighted in related studies on developing countries. Questions were framed to elicit information and knowledge on: a) common cybersecurity practices being carried out by the organizations, b) cybersecurity policies, plans and standards, c) prevalent cybersecurity threats and their countermeasures. Questions were also developed to elicit information, knowledge and perceptions about factors that are detrimental to effective implementation of cybersecurity program and factors that would help to improve cybersecurity posture.

The survey questionnaire were thoroughly reviewed by ICT experts from Bhutan and further vetted by the Research Ethics Committee of Murdoch University to 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. A pilot study consisting of 10 senior ICT professionals was also conducted to ensure the reliability and validity of questionnaire. The questionnaire were found acceptable requiring no major alterations to the questions.

An online survey using SurveyMonkey was conducted by emailing 280 randomly selected ICT professionals (respondents) working in various Bhutanese government organizations. The potential respondents contact list of ICT professionals was provided by the Ministry of Information and Communications. Information about the purpose of the survey, consent to participate and clauses regarding the privacy and confidentiality of the responses were included with the online survey questionnaire. Of 280 potential respondents contacted via email, 157 responses were received. However, only 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).

IV. Assessment Results

The survey results were processed to ensure that respondents have answered all the questions. Questions which were partially completed were removed from the survey.

A. Demongraphic Information

Table I provides an overview of the demographic information of the respondents in terms of gender, age, qualification, job function and their work experience. The general population of the survey respondents may be characterized as young and the majority are in age range from 25 to 34 (66%). In terms of qualifications, work experience and current job function: approximately 49% have bachelor degree with Information Technology being their specialization; 24% of the respondents are responsible for network and system administration followed by 19% of them being responsible for network and systems security and management; 53% of respondents have work experience between 5-10 years.

B. The Key Findings from the Survey Results are:

1) Limited cybersecurity policies and risk management plans in most of the organizations

Policy sets the direction of security management, defines organizational structure, roles and responsibilities of security professionals and how policy should be communicated and internalized among stakeholders and computer users. Most respondents said that their organizations have no cybersecurity policy in place. In addition, respondents also indicated that in most organizations, there is lack of risk management plan established for effective security implementation, see Figure 2 and Figure 3 for detail information.

TABLE I. DEMOGRAPHIC CHARACTERISTICS

Variable		**Frequency**	**Response (%)**
Gender	Male	75	68.81
	Female	34	31.19
Age	45 and over	4	3.67
	35-44	26	23.85
	25-34	72	66.06
	24 and under	7	6.42
Qualification	Certificate	3	2.75
	Diploma	30	27.52
	Bachelor	53	48.62
	Master	23	21.10
	PhD	0	0.00
Specialisation	Computer Science	30	27.52
	Information Technology	53	48.62
	Computer Applications	22	20.18
	Computer Engineering	2	1.83
	Electronics and Communications	1	0.92
	Electrical Engineering	1	0.92
Job Function	Network/System Administrator	26	23.85
	Application/Database Administrator	15	13.76
	IT/Network/Information Systems Security	21	19.27
	IT/MIS/Technical Management	21	19.27
	Web Master/Manager	4	3.67
	Software Programmer/Designer/Developer	11	10.09
	Desktop/Technical Support	11	10.09
Work Experience	Less than 5	29	26.61
	Between 5 and 10	53	48.62
	More than 10	27	24.77

2) Risk management

Risk management is crucial for risk evaluation to prioritize which information assets need higher protection. It also helps to determine how risk should be managed to ensure that desired security protection is achieved with appropriate security control implementation.

- In most of the government organizations, there is a lack of cybersecurity policy. About 66% of respondents indicated that they do not have a security policy in place while 77% respondents said they have no IT risk management plan.

3) Lack of training and awareness

Effectiveness of security is dependent on the behavior of the people. In fact, "People are arguably the weakest element in the security formula that is used to secure systems and networks. The people factor, not technology, is a critical factor that is often overlooked in the security equation" [22]. In most government organizations, there is a lack of training and awareness among the employees and computer users.

Fig. 2. Distribution of cybersecurity policy responses

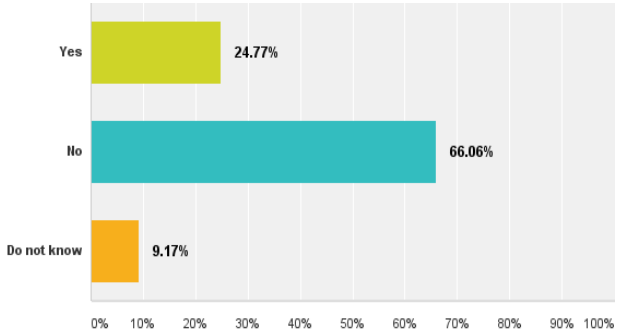
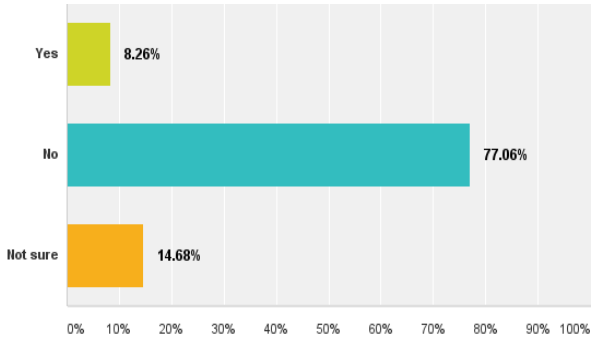


Fig. 3. Distribution of risk management plan responses



- 68% of respondents said no specific trainings or awareness have been provided, but they learn on their own while 25% said that they learn by attending conferences and seminars.
- 47% of respondents said that they are not aware of any international security standards or best practices. 41% of respondents have said they are not aware of Information Security Management Policy (IMSP), which the Ministry of Information and Communications (MoIC) have endorsed as the Security Policy for government organizations. The IMSP is adapted based on ISO 27000 standards.

4) Lack of security incident handling and response capability

In most organizations, there is no incidents handling response capability team.

- 73% of respondents said that their organizations do not have any incident handling and response team.
- 50% of respondents said that their organizations do not know how to handle and response to cyber incidents and attacks
- 56% of respondents also indicated that they do not have resources and processes to respond to cybersecurity incidents.

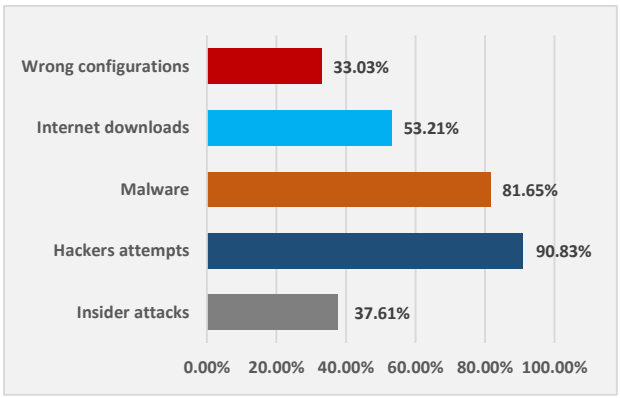
5) Common security risks and incidents

When asked about the most prevalent security risks to their organizations and the security incidents they suffered during the past year, most respondents considered hacking attempts, malware and internet downloads are the most prevalent security risks, see Figure 4.

- About 91% of respondents consider hacker attempts as the most prevalent security risk followed by malware threats (82%) and internet downloads (53%).

Similarly, when asked about what cyber incidents have occurred in their organizations during the past 12 months, most respondents said that virus attacks (85%), malware (68%) and hacking of websites (46%) are the most common cyber incidents.

Fig. 4. Distribution of cybersecurity risk responses



6) Information security management issues

When asked to rank the selected information security issuess [23] in their organizations, the respondents have indicated that users awareness and training, top management support, and vulnerability and risk management are the top three issues that they see as factors affecting the effectiveness of cybersecurity in their organizations. See Table II for top ten issuess. This results are comparable with that of information security issues found in [23].

V. IMPLICATIONS FROM RESEARCH

As seen from the study findings, the current state of cybersecurity in most government organizations at Bhutan is very limited and therefore, by extension, the security program implementation may not be able to provide required security requirements for the e-government initiatives. Some of the priority strategies government organizations need to implement in order to improve cybersecurity for establishment of secure e-government initiatives are:

A. Cybersecurity Policy

Policy is a blue-print that sets the direction of security management, defines organization structure, roles and responsibilities of security professionals and how policy should be communicated and internalized among stakeholders and computer users. Establishing cybersecurity policy would help government organizations to improve cybersecurity by:

- Ensuring that organisational strucuture is established to led cybersecurity;
- Roles and responsibilities of the security professionals including Chief Information Officer is well defined;
- That top executive management commits their support to cybersecurity;
- That policies and procedures are well communicated to users and stakeholders;

B. Risk Management

Risk management is crucial for risk evaluation to prioritize which information assets need higher protection. Not all information assets are equally important. Prioritizing information assets for risk assessment is necessary to ensure that limited resources are used where it is needed. Risk management also helps to determine how risk should be managed to ensure that security is achieved with appropriate security control implementation. Instituting risk planning, therefore, would help government organizations to improve cybersecurity.

C. Awareness and Training

Human are often debated as the weakest link in the security chain. Whatever efforts and however strong security controls might be, security is ultimately dependent on the behavior of the people both concerned with security implementation and affected by the security aspects. Therefore, raising awareness on cybersecurity and imparting training to raise the skills and knowledge of users is very important to enhance cybersecurity in organizations. Awareness and training among users in government organizations would help in ensuring that security is treated as something that is crucial to organizational success.

D. Cyber Incident Reponse Team

There is no 100% security. Given the sophistication and complexity of the information systems and networks, and also with increasing complexity in cyber threats, cyber incidents are inevitable. Incident handling and response actions need to be well organized, coordinated, structured and communicated among the players involved. Cyber incidents information need to be shared as quickly as possible to contain the negative effects arising from those incidents thereby minimizing impact and losses to the organizational reputation, trust and work productivity. Establishing cyber incident handling and response team, therefore, is important for government organizations.

TABLE II: TOP INFORMAITON SECURITY ISSUES

Security Issues	**Average Score**	**Rank**
User Awareness Training & Education	7.67	1
Top Management Support	7.50	2
Vulnerability & Risk Management	6.21	3
Malware	6.06	4
Policy Related Issues	5.63	5
Patch Management	5.00	6
Access Control & Identity Management	4.94	7
Organization Culture	4.48	8
Internal Threats	4.31	9
Business Continuity & Disaster Preparation	3.19	10

E. Technical Controls

As most government organizations are constantly under attack from malware, viruses, hacking and other security threats including unwarranted software downloads, technical measures such as access controls – both physical and logical, technical control measures such as content filtering, firewall configurations, patch management, and installation of host and network security tools such as anti-virus software, intrusion detection system, unified threat management system would help to prevent security risks and protect information systems and networks from cyber-attacks.

While the above mentioned cyber initiatives provide a broad framework for cybersecurity improvement for secure e-government, its effectiveness will depend on the need of individual organization as security requirements are dependent not only on the level of country's ICT development, and sophistication of the systems and networks, but also on the organizational culture and the level

of cyber literacy of the users. Therefore, any approach to improve cybersecurity posture may have to be adapted based on the context and the specific security needs of the organizations.

VI. Discussions and Limitations

Relevant literature related to cybersecurity in developing countries was reviewed and identified cybersecurity practices such as policy, awareness and training, incident response capability, etc., as important security issues to be considered. The survey study was designed based on these factors. The study was carried out to understand the gaps in cybersecurity for e-government initiatives in Bhutan's government organizations. Security requirements is one of the factors determining the success or failure of the e-government services. Information confidentiality, integrity and availability are core objectives of cybersecurity, which are essential for e-government success. The study results indicate that cybersecurity implementation in most government organizations is very limited. In most organizations, there is complete lack of or inadequate cyber policy and risk management plans. In addition, they also have minimal cybersecurity awareness and training, and incident handling response capability. The weakness in the current cybersecurity posture may be alluded to:

- Government's focus into ICT infrastructure development and acquisition of IT systems and hardware for e-government than securing the information systems and networks supporting e-government services;
- General lack of understanding and awareness of cybersecurity and its importance to e-government among policy makers, government executives, users and customers;
- Low level of ICT development and literacy;
- Low level of systems sophistication and complexity, for example, the current e-government services do not have provision for online transaction. Hence, need for security has not been felt;
- Lack of investment and budget for cybersecurity technologies;

As this study is limited to only government agencies, the findings may not be applicable to corporate and private sector. The cybersecurity situation may be better off especially in banking and financial institutions as they deal with financial services and frequently interact with customers. They also have financial resources and funding capability to invest in security needs. A holistic view of cybersecurity may be obtained by extending this study to include corporate and private sector in future.

VII. Conclusion

This paper presents an assessment of cybersecurity practices in government organizations in Bhutan. One of the key government information assets that needs to be protected from cyber incidents and intrusions is the e-government services. Protection of information availability, integrity and confidentiality of e-services is important in order to avoid data loss, disruption to services and loss of privacy. The survey results show that in most government organizations, there is inadequate cybersecurity policy, which is crucial for setting the direction in how organization conduct security and security implementation to meet its business objectives. There is also no risk management process to identify which information assets need to be protected, prioritized and evaluated to ensure effective security controls. In addition, lack of awareness and training among government employees and users, indeed, affects the effectiveness of cybersecurity. Furthermore, complete lack of cyber security incident handling and response team, which coordinate, investigate and contain security incidents inhibit the cybersecurity posture. Therefore, based on the survey findings, this study recommends to establish:

a) Cybersecurity policy and risk management plan,

b) Awareness and training program to raise the skills and knowledge, and

c) Cyber incident handling and response team for security incident coordination, information disseminations, issuance of security alerts and warnings, and for responding to security breaches.

As the level of ICT development varies from organization to organization, any approach to cybersecurity including the security initiatives recommended in this study need to be adapted and tailored to the context, culture and specific security needs of the organizations.

Acknowledgement

The authors would like to extend our sincere thanks to Dechen Chhoeden, ICT Management Division, Department of IT and Telecom (DITT), Ministry of Information and Communications (MoIC) for providing us with the ICT Professional contact list and Passang Dema, Office of Attorney General, Bhutan for giving us free access to SurveyMonkey account for this survey study.

References

[1] S. Bhatnagar, "Enabling e-government in developing countries: From vision to implementation," 2000.
[2] infoDev/World Bank. (2009). *e-Government Primer*.
[3] MoIC, "Bhutan e-Government Master Plan," Ministry of Information and Communications, Ed., ed: Royal Government of Bhutan, 2013.
[4] M.-S. Hwang, C.-T. Li, J.-J. Shen, and Y.-P. Chu, "Challenges in e-government and security of information," *Information & Security*, vol. 15, pp. 9-20, 2004.
[5] G2C, "G2C: Service Delivery Initiative," ed. Thimphu: Royal Government of Bhutan, n.d.
[6] UPAN, "UN e-Government Survey 2014: E-Government for the Future We Want," ed. New York: UPAN, 2014.
[7] S. V. Anandkumar, R. Bojjagani, and J. Saravanan, "e-Governance in South Asia: An assessment of G2C and G2B

Aspects of Key Ministry Websites of SAARC Countries," *A Biannual Journal of South Asian Studies*, p. 51.

[8] S. Singh and D. S. Karaulia, "E-Governance: Information Security Issues," in *International Conference on Computer Science and Information Technology (ICCSIT'2011) Pattaya*, 2011, pp. 120-124.

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

[10] 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.

[11] E. Khanyako and G. Maiga, "An information security model for e-government services adoption in Uganda," in *IST-Africa Conference and Exhibition (IST-Africa), 2013*, 2013, pp. 1-11.

[12] K. AlGarni, "Information Security Policy for E-government in Saudi Arabia: Effectiveness, Vulnerabilities and Threats," 2015.

[13] O. R. Ashaye and Z. Irani, "e-Government Implementation Benefits, Risks and Barriers in Developing Countries: Evidence from Nigeria," *International Journal of Information Technology & Computer Science (IJITCS)*, pp. 92-105.

[14] S. Alfawaz, L. J. May, and K. Mohannak, "E-government security in developing countries: A managerial conceptual framework," 2008.

[15] G. Karokola, S. Kowalski, and L. Yngström, "Towards an information security maturity model for secure e-government services: a stakeholders view," in *Proceedings of the 5th HAISA2011 Conference, London, UK*, 2011, pp. 58-73.

[16] A. C. Tagert, "Cybersecurity challenges in developing nations," 3445893 Ph.D., Carnegie Mellon University, Ann Arbor, 2010.

[17] F. Wamala, "ITU national cybersecurity strategy guide," *International Telecommunications Union*, vol. 11, 2011.

[18] K. P. Newmeyer, "Cybersecurity Strategy in Developing Nations: A Jamaica Case Study," 3616630 Ph.D., Walden University, Ann Arbor, 2014.

[19] ISO/IEC 27001, "Information technology – Security techniques – Information security management systems – Requirements," 2005.

[20] S. P. NIST, "800-12: An Introduction to Computer Security–The NIST Handbook," ed: October, 1995.

[21] N. I. o. Standards, Technology, and U. S. o. America, "Framework for Improving Critical Infrastructure Cybersecurity," 2014.

[22] P. Bowen, J. Hash, and M. Wilson, *Information security handbook: a guide for managers*: US Department of Commerce, Technology Administration, National Institute of Standards and Technology, 2006.

[23] K. J. Knapp, T. E. Marshall, R. K. Rainer, Jr., and D. W. Morrow, "THE TOP INFORMATION SECURITY ISSUES FACING ORGANIZATIONS: WHAT CAN GOVERNMENT DO TO HELP?*," *EDPACS*, vol. 34, pp. 1-10, Oct 2006 2006.