EXPLORING CRITICAL SUCCESS FACTORS FOR CYBERSECURITY IN BHUTAN'S GOVERNMENT ORGANIZATIONS

Pema Choejey, David Murray and Chun Che Fung

School of Engineering and IT, Murdoch University, Perth City, Australia
P.Choejey|D.Murray|L.Fung@murdoch.edu.au

ABSTRACT

This paper presents the results of open-ended survey exploring the critical success factors for cybersecurity implementation in government organisations in Bhutan. Successful implementation of cybersecurity depends on a thorough understanding of cyber threats and challenges to the organisational information assets. It also depends on identification of a responsible, dedicated personnel to lead and direct cybersecurity initiatives. Furthermore, it is important to know the critical areas of cybersecurity activities for management to target, prioritise and execute. Understanding of what key things need to be done right by the responsible agency and its leader, at a particular time and in particular context, can lead to better decision making and resource optimisation including skills and knowledge. The survey findings indicate that, among other factors, awareness and training, policy and standards, and adequate financing and budgetary commitment to cybersecurity projects are three most important success factors. Channelling an organisation's limited resources to these few factors is expected to enhance cybersecurity posture and its management. The research outcome has implications to both government and private organizations in Bhutan.

KEYWORDS

Cybersecurity, Critical Success Factors, Top Management, Awareness and Training

1. INTRODUCTION

Cybersecurity is a global issue that affects both developed and developing countries. Bhutan, which introduced the Internet only in 1999, is facing its own sets of cyber problems. The recent online financial scam, based on the fake email letter that was supposedly sent from the Royal Audit Authority, caused the Bank of Bhutan to transfer 16 million (in Bhutanese currency) to three different accounts in India, Malaysia and Thailand [1]. This cyber incident clearly shows that Bhutan is not immune to cyber threats. Private and government websites have been defaced [2-4] and networks and systems were made inaccessible due to rampant malware and physical disruptions [5].

In just over a decade, the Internet subscriber rate of Bhutan increased from less than 1% in 2004 to 34.3% in 2013. Similarly, the mobile subscriber rate increased from 37% in 2004 to 74.3% in 2013. The Internet and mobile services are now accessible in all 20 *dzongkhags* (or Districts) and 205 *Geogs* (or Village blocks) [6] By 2014, there were more than 80,000 Facebook and Social Networking sites users, which is 10% of the country's 750,000 people [7]

According to the 11th Five Year Plan of 2013, Bhutan's main ICT focus areas are to: i) implement Government-to-Citizens (G2C) services to improve the efficiency and quality of service delivery

Natarajan Meghanathan et al. (Eds) : NETCOM, NCS, WiMoNe, GRAPH-HOC, SPM, CSEIT - 2016
pp. 49– 61, 2016. © CS & IT-CSCP 2016 DOI : 10.5121/csit.2016.61505

to citizens (e.g., online tax filing and birth registration) by improving accessibility, optimizing human resources and reducing service delivery time, ii) establish a government data centre to improve systems reliability, accessibility and resiliency, and iii) consolidate and integrate the wide area network in the capital, which connects all central ministries, and local area networks in the regions for smooth functioning of many services offered online. In addition, the government intends to explore the potential of mobile technology services including implementation of financial payment systems [8-10].

As described earlier, government ICT agenda suggests that Bhutan's dependency on ICT and the Internet is growing and becoming more sophisticated. In other words, it means that its cyber landscape is constantly changing and becoming unpredictable as more people, government, devices, systems and networks become interconnected.

However, aside from the studies in [11, 12], there is no indication of how the government in Bhutan will manage cybersecurity. Clearly, there is a gap of knowledge and understanding of what cyber threats Bhutan is currently facing, who is responsible to lead cybersecurity initiatives and what are the critical success factors that government need to focus upon to make their cyber program a success.

Considering that Bhutan is a developing country, hugely dependent on foreign aid from development partners and international organizations, utilization of limited resources for the wrong strategic goals and objectives may become complete waste of national efforts. Therefore, it is important for the government, policy makers and practitioners to understand and realize what critical things need to done in a specific situation, at a particular time, to make implementation of every national program a success. An understanding of the success factors for cybersecurity is crucial for Bhutan's government, as it has neither material capacity nor human resources to tackle the emerging cybersecurity challenges.

One of the approaches to identity the critical success factors for the organizations is to use the Critical Success Factors (CSFs) method. According to [13, 14], CSFs are defined as *"the limited number of areas in which satisfactory results will ensure successful competitive performance for the individual, department or organisation. CSFs are the few key areas where "things must go right" for the business to flourish and for the manager's goals to be attained. CSFs are the particular areas of major importance to a particular manager, in a particular division, at a particular point in time."*

The key areas are the activities [15]:

- *in which favourable results are necessary to achieve goals.*
- *where things must go right for the organisation to flourish.*
- *that should receive constant attention from management.*

Unlike other approaches, the central idea to CSF method is to focus on "individual managers", by extension to organisations and individuals, and to identify their "information needs". CSF is also unique as it takes into consideration the fact that "information needs vary from manager to manager and that these needs change with time" [13] and by extension with change in environment (e.g., technology). Thus, CSF method is a flexible and dynamic tool that can be used to assess and identify the key areas of activities that are necessary for ensuring the success and performance of a company or an organisation.

While the standard approach of CSFs is to conduct a face-to-face interviews or group discussions with key people in the organisation, this study uses open-ended survey questions to gauge what respondents think and believe would be the critical success factors for implementing cybersecurity in government organisations. The survey approach provides an advantage of having more respondents, anonymity and openness to respond to survey questions.

In the survey, the study asked four open-ended questions to the participants:

- *Please list three of the greatest threats to information resources in your organisation?*
- *Who do you perceive as being responsible for information security in your organisation?*
- *Please list issues that you think are inhibiting cybersecurity effectiveness in your organisation?*
- *Please list things that you think would be critical success factors for implementation of cybersecurity?*

Complete understanding of current cybersecurity situation and context is important. Therefore, the purpose of the study is soliciting knowledge and information on what challenges government organisations are currently facing, who respondents think should be make responsible for cybersecurity and what critical areas the management and its leaders should focus upon to achieve organisational cybersecurity objectives. However, this paper describes only the analysis and findings of the survey responses related to critical success factors for effective cybersecurity implementation.

The paper is organized as follows. Section I introduces Bhutan's cybersecurity situation and the purpose of the study; Section II describes cybersecurity related studies done in Bhutan, Section III presents the research methods and materials; Section IV describes the data analysis and results; Section V provides brief description of study limitations followed by conclusion in Section VI.

2. LITERATURE REVIEW

Because the Internet in general and cybersecurity in particular are fairly new concepts or phenomena, cybersecurity related studies done in Bhutan is far and few.

An E-Readiness study [16] was conducted in 2003 to assess Bhutan's readiness to embrace and participate in the network economy and information society. The purpose of the study was to assess maturity levels in network, human, infrastructure and legal capacity. Country's maturity level below certain threshold in any of these elements is considered as not ready. Knowing the state of ICT development also provide directions where government need to focus and prioritize its national efforts to improve the level of readiness. However, readiness in cybersecurity nor challenges facing Bhutan has been studied.

One of the common mechanisms to counter cybersecurity challenges, especially cyber incidents, is to establish the Computer Incident Response Team (CIRT) [17]. In order to understand how developing countries are managing and responding to cyber incidents, the International Telecommunication Union (ITU) conducted assessment of CIRT covering India, Bhutan, Bangladesh and India [18]. The main objective of the study was to understand cybersecurity challenges facing these countries, to document measures taken to respond to these challenges and to assess their capabilities to coordinate, respond and share information related to cyber incidents. However, this study was limited to cyber incident management capabilities. It has not assessed other security domains such cyber policy, organizational security and personnel security. Nor it has assessed which of security factors developing countries should implement to achieve maximal security benefits.

Another study assessing Bhutan's cybersecurity capability and maturity was conducted by the Global Cyber Security Capacity Centre and the World Bank [19]. The study measured maturity levels in five dimensions: i) policy and strategy, ii) culture and society, iii) education, training and skills, iv) law and regulation, and v) organization, standards and technology. The maturity levels in each dimension were assessed based on five stages: start-up, formative, established, strategic and dynamic. The study findings suggest that Bhutan is at the start-up level of maturity, meaning that Bhutan neither has a capacity nor has undertaken concrete actions with respect to some factors in each dimension. While the study provides an understanding of cybersecurity in Bhutan from the national perspectives, it does not, however, provide specific insights and understanding of how government organizations have implemented cybersecurity activities. Further, their research method is based on group discussion and analysis of available documents.

In [20], a PKI based security framework was proposed for e-government platforms in Bhutan. The framework was derived from PKI solutions and best practices implemented in India, Korea and Taiwan. Even though this study addresses security gaps for e-government platforms, the study is specific to the use of cryptography technologies as solution to the e-government security issues. Moreover, they study used SWOT (Strengths, Weaknesses, Opportunities and Threats) method along with analysis of relevant policy documents.

Recently, an overview of cybersecurity challenges facing Bhutan was presented in [11]. Based on the analysis of available government reports and printed media, common cyber threats and challenges (e.g., hacking and phishing) facing Bhutan were identified and documented. This study was based on a desk audit research method and content analysis, which largely involves reviewing, collation and synthesis of information from secondary sources.

Another recent study related to cybersecurity management was the assessment of cybersecurity practices in the context of e-government implementation [12]. The study surveyed 280 potential respondents to assess the implementation of cybersecurity practices such as cyber policy, risk management, and training and awareness. The study suggests that in most government organizations there is very limited and/or complete lack of cybersecurity policy, risk management, awareness and incident management implementation. It also indicates that many organizations have either suffered from or been affected by cybersecurity threats such as hacking, malware and phishing scams. While the study recommends implementation of both managerial and technological solutions, it does not say which are the few key things government should decide and take action to achieve maximum benefits from security investments.

3. METHODS AND MATERIALS

3.1. Sample and Procedure

A formal approval was sought from the Secretary of the Ministry of Information and Communications (MoIC), Bhutan to provide the contact list of ICT professionals working in various government organisations. Contact addresses of ICT professionals were, then, obtained from the Department of IT and Telecom under the ministry. Emails with a link to the survey were sent to the 280 potential respondents. A follow-up e-mail was sent after one month to improve the survey response rate.

3.2. Instrument

An online survey questionnaire was used to collect data for this study. Survey Monkey was used to design and develop the survey questionnaire. Information related to objectives, confidentiality and consent to participate were included in the survey. The survey also has the option for withdrawal in the case that respondents changed their mind midway through the survey. The survey involved 280 participants. They were asked an open-ended question to list at least 3 critical success factors for cybersecurity program in government organisations. Prior to the actual survey, the questionnaire was pre-tested with 10 senior ICT professionals who were studying abroad in different countries. Further, the survey instrument was reviewed and approved by the Murdoch Ethics Committee to ensure its appropriateness to the research and that the risk factors to the participants were duly considered, especially their privacy and confidentiality.

4. RESULTS

4.1. Response Rate

Electronic mail invitations were sent to potential survey participants to participate in the online survey study. Of 280 respondents, 157 of them responded to the survey. That means that the response rate was about 56% (157/280). However, not all participants who responded to the survey answered all the survey questions. There were only 109 respondents who fully completed the questionnaire. Therefore, the completion rate of the responses was about 69% (109/157).

4.2. Demographic Characteristics

The demographic data is shown in Table 1. Survey participants can be characterised as mostly young with their age ranging from 25 to 34. Most of the participants have a bachelor degree closely followed by diploma and master degree. Their expertise and speciality is mostly in the field of Information Technology, Computer Science and Computer Applications. In terms of gender, more than 68% of participants were male while female participants constituted about 31% of survey responses.

Table 1. Demographic characteristics of survey respondents

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

4.3. Analysis

4.3.1 Data Pre-processing

The responses to open-ended questions were analysed using NVivo software. Prior to importing the data into the NVivo program, responses were pre-processed to ensure that non-response items or partially completed responses were removed. Responses were also processed to ensure that words and phrases were correctly spelled and formatted. For example, budget top management is separated as budget and top management or budget, top management. This process improved the quality and accuracy of the data. In addition, responses were categorized into codable texts and classifiable texts. Coding can be performed only on codable texts while classifiable texts can be used for answering multiple questions or to perform demographic comparisons as male versus female.

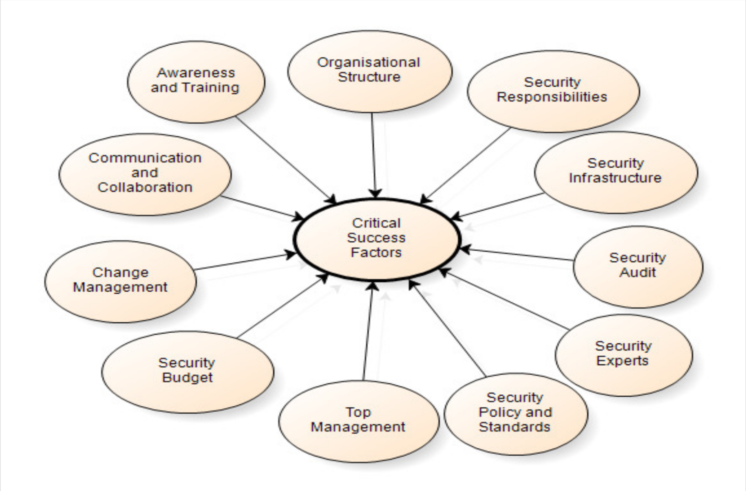


Figure 1. Themes coded from qualitative data

4.3.2. Coding Themes

The coding of qualitative data was performed using the In Vivo Coding method [21]. This method is used to code themes emerging from the codable texts of responses. In other words, it allows texts to be coded using words and phrases found in the qualitative data. For example, as question 4 is related to success factors for cybersecurity implementation in Bhutan, this question is broadly coded as Critical Success Factors under which further sub-themes are categorized. Within this broad category, sub-themes such as awareness and training, security policy and standards, and top management can be categorized. Within the sub-category, for example, training and awareness, there are sub-sub-themes such as seminars, workshops, advocacy, training, etc. These sub-sub-themes constitute or aggregate into abstract concept of training and awareness, which further can be abstracted as one to critical success factors for effective cybersecurity implementation. The resulting coded themes from the qualitative data is shown in Figure 1.

Table 2. Critical success factors for cybersecurity.

Critical Success Factors	*Frequency*	*Percentage* (n=109)*
Awareness and Training	56	51%
Security Policy and Standards	30	28%
Security Budget	23	21%
Top Management	22	20%
Security Infrastructure	15	14%
Security Audit	11	10%
Security Responsibilities	9	8%
Organizational Structure	8	7%
Security Experts	3	3%
Change Management	3	3%
Communication and Collaboration	1	1%

**rounded to nearest percent*

4.4. Key Findings

As different countries face different cybersecurity challenges, the idea was to solicit and understand the prerequisites to cybersecurity implementation success. Therefore, respondents were asked to list at least three critical success factors for cybersecurity in their organisation. The survey results show, see Table 2, that the top five cybersecurity success factors for government organisations are:

- Awareness, training and education.
- Security policy, standards and procedures.
- Cybersecurity financing and resources.
- Top management support for cybersecurity.
- Cybersecurity audit and compliance.

Nearly, 51% (56/109) of respondents believe that government organizations should focus on awareness and training to make cybersecurity a success. Another 27% (30/109) of respondents believe that management should establish policy and standards while 21% (23/109) of respondents think that sufficient budgetary commitment to cybersecurity initiatives will help government organizations to achieve their organizational security objectives. Respondents also identified top management (20%) and security infrastructure (14%) as the fourth and the fifth critical success factors for cybersecurity implementation.

4.5. Recommendations

4.5.1. Awareness and Training

In [22], Fadi argues that educating and training users is must to combat IT security threats. He believes improving the security awareness among the normal users can prevent them becoming the *weakest link* in any organization or becoming an easy and soft target for the cyber criminals [22]. Awareness and training is also important for the legitimate users because people with authorized privilege and access rights bypassed rules to trade-off security against usability, people sometimes make biased decision, so that they gain maximum benefits for the cost of action or decision [23]. Close to 51% of survey respondents believe that awareness and training is the topmost critical success factor that can help government organizations to improve cybersecurity to achieve its business goals and objectives.

4.5.2. Cybersecurity Policy

According to [24], policy in general refers to “a plan or a course of action” that “influence and determine decisions, actions and other matters” of government, organization and business. In the context of cybersecurity, it is a formal statement of “set of rules that dictate acceptable and unacceptable behaviour within an organization”. In other words, the security policy is the foundation for planning, management and maintenance of cybersecurity. Policy drives the implementation of standards which further drives the implementation of practices, procedures and guidelines. Further, policy is a living document that has to be flexible, adaptable and constantly reviewed to reflect the change in environment. The survey results show that nearly 28% of respondents believe that cybersecurity policy is the second most important critical factor to ensure the success of cybersecurity implementation.

4.5.3. Security Budget

Budget underlies any policy initiatives to be undertaken by any government. Without budget and financial resources, it would be impossible to initiate any development activities and implement them successfully. The survey finding suggests that security budget (21%) is the third most important factor that the Bhutanese government should consider while implementing cybersecurity. Budget is central to other priority areas such as training and awareness, security policy and security infrastructure. Without budgetary commitment and resources, none of these critical factors can be implemented successfully.

4.5.4. Top Management Support

The success of cybersecurity efforts depends to a large extent on the commitment and support of the top management [25, 26]. Managerial issues are regarded as the most important security issues and requires management involvement to solve. In a worldwide survey conducted by Knapp et al, [27] found that ‘top management support’ to be the highest ranked issue among a list of 25 information security issues. Top management’s support and commitment is not only significant to planning, executing and governing of security decisions, but also important to demonstrate to security communities and stakeholders that their investment into security benefits them. Therefore, it is important for any organization to have competent and abled security managers to lead the security governance. Nearly, 20% of survey respondents identified management support as of one the critical success factors that government organization should consider for cybersecurity.

4.5.5. Security Infrastructure

Security infrastructure such as hardware and software (e.g., firewalls and intrusion detection systems) are equally important to meet organization's security requirements and implementation of access controls. Cybersecurity is often considered to be technical issue more than management issue. As a result, security mechanisms such as firewalls and antivirus solutions are widely implemented to protect information resources from security breaches. The survey results show that 14% of respondents view security infrastructure as the success factor for cybersecurity.

The study, therefore, recommends government organization to consider and adopt these critical success factors as priority areas to improve cybersecurity in Bhutan.

5. DISCUSSIONS

Cybersecurity may be global in nature but is highly localised to specific organisation in a particular country. No two countries have the same cybersecurity context and the level of maturity [28, 29]. Developing countries such as Bhutan, as described in the literature review, are at a different level of cyber maturity.

The survey results provide a broad perspective of cybersecurity and in particular the direction in which government in Bhutan needs to proceed in cybersecurity implementation. The critical success factors described in the survey findings are identified by the ICT professionals engaged in ICT activities in Bhutan. Therefore, it reflects the practical cyber challenges and the requirements to improve cybersecurity. The top two priorities identified in the survey were awareness and training, and security policy and standards. This suggests that most ICT professionals believe that the majority or most serious issues may be solved within the surveyed group. While there are some who believed that internal or external factors such as security budget, top management and security infrastructure were important, it is promising that the majority of staff were not externalising the problem.

Success factors in information security implementation in government organisations in Oman was explored based on information security experts view [30]. The five success factors identified in the study were: 1) Awareness and Training, ii) Management Support, iii) Budget, iv) Information Security Policy Enforcement and Adaptation, and v) Organisation's Mission. Another study carried out in Iran's Municipal Organisations based on the view of experts in the studied organisations suggests that top management support, information security policy and awareness and training programs are the most important success factors in implementing information security management systems. Furthermore, an empirical study [27] based on the survey of 874 certified information systems security professionals (CISSPs) suggest that top management, security budget and security awareness are among top ten information security issues. Another exploratory research of Yanus and Shin [31] suggests that security technologies, top management support and information awareness and training are factors critical for successful implementation of information awareness program.

The findings of this study in Bhutan shares many similarities and commonalities of success factors that are critical for successful implementation of cybersecurity and security related programs.

This survey was limited only to government organisations. Including survey participants from the corporate and private organisations may have led to different perspective and thinking. Furthermore, inclusion of survey participants of non ICT personnel may result in different findings. However, the survey results provide a list of conceptual areas which may be further investigated to validate their importance to cybersecurity effectiveness. Future work may include other organisations and groups to confirm the applicability of the reported success factors.

6. CONCLUSIONS

This paper presents the results of open-ended survey exploring critical success factors for cybersecurity implementation. This study has surveyed 159 Bhutanese ICT professionals about the key factors for Cyber security success. The results suggest that the top five priorities, in order of reported importance, are:

a) awareness, training and education – ICT professionals who are responsible for cybersecurity and ICT users affected by security issues must be made aware of their security responsibilities and trained in cybersecurity technologies,

b) policy, standards and procedures – policy is the cornerstone for planning and executing cybersecurity initiatives, while standards and procedures are necessary to achieve policy objectives and organisational vision,

c) Cybersecurity budget – budgetary commitment is essential not only for investment in cybersecurity technologies and infrastructure, but also for policy implementation and conduction of cybersecurity training and awareness,

d) top management support – competent leadership drives the success of the organisation. Top management support is essential to get the stakeholders support and secure budget for cybersecurity,

e) security infrastructure – effective cybersecurity needs security controls and tools (e.g., firewalls and antivirus) to mitigate cyber risk and prevent security breaches, and

f) cybersecurity audit process – compliance to cyber rules, policies and data standards are equally important. Cybersecurity audit process ensures that organisations meet the security requirements and remain up to date with changing environment.

The outcome of this research will have significant impact to both governmental organization and non-governmental organizations in terms of understanding the limited number of areas in which satisfactory results will ensure successful competitive performance for the individual, department or organisation. If implemented successfully, these factors would not only improve cybersecurity by reducing security breaches, but also meet organisational goals. However, the identified factors need to be further validated using different tools and techniques.

ACKNOWLEDGEMENTS

The authors would like to thank Miss Dechen Chhoeden, Department of IT and Telecom for her kind support for providing us with the contact list of ICT professionals.

REFERENCES

[1] N. Gyeltshen, "BoB transfers Nu 16M based on fake e-mail," in BBS Online, ed. Thimphu: Bhutan Broadcasting Service, 2016.

[2] 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.

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

[4] 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.

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

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

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

[8] GNHC, "Eleventh Five Year Plan Volume I: Main Document," G. N. H. Commission, Ed., ed. Thimphu: GNHC, 2013.

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

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

[11] 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.

[12] P. Choejey, C. C. Fung, K. W. Wong, D. Murray, and H. Xie, "Cybersecurity Practices for E-Government: An Assessment in Bhutan," presented at the The 10th International Conference on e-Business, Bangkok, Thailand, 2015.

[13] J. F. Rockart, "Chief executives define their own data needs," Harvard business review, vol. 57, pp. 81-93, 1978.

[14] C. V. Bullen and J. F. Rockart, "A primer on critical success factors," 1981.

[15] R. A. Caralli and W. R. Wilson, "Applying Critical Success Factors to Information Security Planning," DTIC Document2004.

[16] MoC, "Bhutan e-Readiness Assessment," T. D. o. I. Technology, Ed., ed: Ministry of Communications, 2003.

[17] J. Haller, S. A. Merrell, M. J. Butkovic, and B. J. Willke, "Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability," DTIC Document2010.

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

[19] T. Roberts, "Building Cyber-Security Capacity in the Kingdom of Bhutan," G. C. S. C. Centre, Ed., ed: University of Oxford undated.

[20] B. Nono, "Proposing a Government PKI in Bhutan: A Solution to e-Government Security Requirements " 2011.

[21] J. Saldaña, The coding manual for qualitative researchers: Sage, 2009.

[22] F. A. Aloul, "The Need for Effective Information Security Awareness," Journal of Advances in Information Technology, vol. 3, 2012.

[23] D. Besnard and B. Arief, "Computer security impaired by legitimate users," Computers & Security, vol. 23, pp. 253-264, 5// 2004.

[24] M. E. Whitman and H. J. Mattord, Management of information security: Nelson Education, 2013.

[25] J. M. Torres, J. M. Sarriegi, and J. Santos, "Critical Success Factors and Indicators to Improve Information Systems Security Management Actions," Handbook of Research on Information Security and Assurance, vol. 160000, p. 140000, 2009.

[26] S. Posthumus and R. von Solms, "A framework for the governance of information security," Computers & Security, vol. 23, pp. 638-646, 2004.

[27] 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.

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

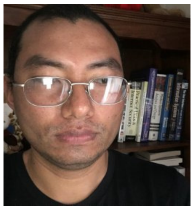
[29] K. P. Newmeyer, "Cybersecurity Strategy in Developing Nations: A Jamaica Case Study," 3616630 Ph.D., Walden University, Ann Arbor, 2014.

[30] M. Al-Awadi and K. Renaud, "Success factors in information security implementation in organizations," in IADIS International Conference e-Society, 2007.

[31] R. Yanus and N. Shin, "Critical Success Factors for Managing an Information Security Awareness Program," in Proceedings of the sixth Annual ISOneWorld Conference, 2007.

AUTHORS

PEMA CHOEJEY



Pema Choejey is currently studying Doctor of Philosophy (Ph.D) in Information Technology, School of Engineering and IT at Murdoch University, Australia. He has bachelor degree in Electronics and Communications Engineering from PSG College of Technology, Bharathiar University, India and master of science in Information Technology from King Mongkut's University of Technology, Thailand. Prior to becoming a Ph.D student, he worked as the Chief ICT Officer and Head of Research Division for the Department of Information Technology and Telecom under the Ministry of Information and Communications, Bhutan.

CHUN CHE FUNG

Chun Che Fung received his B.Sc.(Hon.) and M.Eng. degrees from the University of Wales in 1981 and 1982 respectively. He was awarded a Ph.D degree from the University of Western Australia in 1994. Currently, he is Professor Emeritus at the School of Engineering and Information Technology, Murdoch University. Prior to his present position, he worked as Associate Professor and Associate Dean of Research at Murdoch University (2003-2015), Senior Lecturer at the School of Electrical and Computer Engineering, Curtin University (1988 to 2002), and the Department of Electronic and Communication Engineering, Singapore Polytechnic (1982 to 1988). His research interests are computational intelligence techniques and intelligent systems applications for practical problems.

DAVID MURRAY

David Murray received his Ph.D degree from Murdoch University. Currently, he is Senior Lecturer at the School of Engineering and Information Technology at Murdoch University. His research interests are in wireless networks, data communications and security. He has published in the areas of TCP Performance Enhancing Proxies, Wi-Fi performance, fast roaming, network measurement, routing protocols and security.