State of cyber security: the Ugandan perspective.

1 Matovu Davis, 2 Mugeni Gilbert B , 3 Karume Simon, 4 Mutua Stephen, 5 Gilbert Gilibrays Ocen
1davismatovu@yahoo.com Busitema University- Uganda
2gbmugeni@gmail.com Masinde Muliro University of Science and Technology
3smkarume@gmail.com Communication Authority of Kenya
4stephen.makau@gmail.com Masinde Muliro University of Science and Technology
5gilbertocen@gmail.com Laikipia University

Abstract

The Internet of Things (IoT) is the network of physical objects accessed through the Internet that can identify themselves to other devices and use embedded technology to interact with internal states or external conditions. IoT systems or applications are used across various sectors of the economy such as energy, construction, infrastructure, manufacturing, health, agriculture, defence, and transport, as well as public sector and consumer applications, there will be few parts of society not affected by IoT. This massive adoption and usage of IoT systems or applications has seen cyber threats growing at an alarming rate. This paper assesses the state of Cyber Security threats and risks in Uganda through literature reviews and gathering stakeholders and Information Technology experts opinions. It has been revealed that the Cyber emerging security threats include Denial-of-service attacks, Data espionage, Natural threats,Sabotage,Computer,Frauds,Malicious attacks, Message falsification or injection,Vandalism,Copyright Violations. It is also envisaged that as the technologies advances, a resultant proliferation of cyber threats will be witnessed. Thus governments and Information Technology industries need to strategically plan and implement IoT technologies to help in combating cyber threats.

Keywords: Internet of Things, cyber security, cyber crime, ICT.

1.0 Introduction

The advances of information and communications technologies (ICTs) enable businesses and individuals to communicate and transact with other parties electronically, instantaneously and internationally Marco (2010). Among these developments has been the advent of the Internet of Things (IoT) phenomenon. IoT is an enabling technology that has the potential to fundamentally change society and business processes within and across sectors (Taylor et al,2018).

The evolution of IoT represents multiple categories of cyber-physical systems, integrating technologies related to smart grids, smart homes, intelligent transportation, manufacturing and supply chain and smart cities. Such new technologies come with new types of risks(Radanliev et al,2018).

In many countries the economic impact of cyber risk and cyber security importance is growing as the integration of IoT connected devices into smart manufacturing and supply, cities, intelligent transport systems, smart grids and more aspects of modern life, including banking, finance, autonomous cars and

personal medical devices increasingly scales up. Cyber-attacks are increasing in frequency and the increasingly target IoT devices (for example the Mirai botnet). Therefore the severity of future attacks could be much greater than what has been observed to date (Radanliev et al,2018).

According to Von Solms and Niekerk (2013),Cyber security has become a matter of global interest and importance. Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets (Von Solms and Niekerk,2013). Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment (Von Solms and Niekerk,2013).

Cyber security should be about protecting more than just the information, or information systems resources, of a person/organisation. Cyber security is also about the protection of the person(s) using resources in a cyber environment and any other assets, including those belonging to society in general, that have been exposed to risk as a result of vulnerabilities stemming from the use of ICT(von Solms and Niekerk,2013).

Ollie (2014) noted that the IoT phenomenon makes countries more susceptible to attacks and economic drain on society. Since cyber space or Internet as a whole is increasingly used as a tool and medium for transnational crime, cyber-crime prevention and security faces a number of challenges some of which are: the nature of cybercrime; the existence of "safe havens" for cybercriminals; content regulation; inter-agency cooperation and concurrent jurisdiction over the Internet; degree of regulatory intervention; and maintaining the separation of powers and regulatory independence(Marco (2010) ; Babate et al(2015)).

This rapid and unrelenting pace of changes and challenges in cyber security was the driving force that prompted an assessment for cyber security strategies in Uganda so as to improve on cybersecurity awareness, preparedness and resilience. This paper assesses the state of Cyber Security threats and risks in Uganda.

RELATED LITERATURE

2.0 The Security Risks and Challenges to IoT Devices

Currently, more things are connected to the Internet than people, according to an info graphic from Cisco. It goes on to say that 25 billion devices are expected to be connected by 2015 and 50 billion are slated to connect by 2020. In this quickly evolving world, all the things that connect to the Internet are exponentially expanding the attack surface for hackers and enemies (Baraja ,2014). A recent study by EY (2014) showed that 70 percent of IoT devices contain serious vulnerabilities.

According to Alsaadi & Tubaishat (2015) one of the challenges of Internet of Things cyber security has is DoS attacks in a distributed architecture approach, which can be used by blackmailers and activists to hijack unsecured network devices like sensors and routers and using them as bots to attack third parties. Other challenges are eavesdropping over the IoT network and node(Alsaadi&Tubaishat, 2015).

Baraja (2014) suggests that privacy is a serious concern not just in the IoT environment, but in all the applications, devices or systems where we share information. Even when users take precautions to secure their information, there are conditions that are beyond their control. Hackers can now craft attacks with unprecedented sophistication and correlate information not just from public networks, but also from different private sources, such as cars, smartphones, home automation systems and even refrigerators.

2.1 Internet of Things Cyber Security Risks

A number of cyber security Risks exist in the Internet of Things Phenomenon and according to (Mellisa, 2013),the IoT cyber security risks include Illegal access ,Data espionage ,Illegal Interception, Data interference, System Interference, Fraud and computer-related fraud , Illegal Content,Spam,Copyright Violations and Identity-Related Crimes.

2.2. Cyber risk assessment in the Internet of Things domain

According to Radanliev et al (2018), cyber risk assessment requires categorising into (1) risk identification assessment strategy ; (2) risk estimation strategy; and (3) risk prioritisation strategy. This because IoT capabilities create new types of cyber risk , which are neither anticipated nor considered in existing cyber risk assessment standards. Radanliev et al (2018) further argues that integrating IoT technology in the communications networks of critical infrastructure implies major ethical aspects that humans should be able to be aware of and comprehend, while also benefiting from maximum possible levels of trust and privacy. Integrating IoT technology in the communications networks also triggers question on data ownership, data privacy and economic lifespan of digital assets(Radanliev et al,2018).

3.0 Methodology

The study was carried out in Kampala district, Uganda. Using Krejcie and Morgan table, (1970), a sample of 127 respondents from 7 firms(The Ministry of ICT of Uganda, National Information Technology Authority of Uganda, Uganda Communication commission, Security Agencies of Uganda and Universities.) were conveniently selected basing on their accessibility and willingness to participate. It also gave each respondent an equal chance of being selected to participate in the study(Mugenda & Mugenda,1999).

Purposive sampling permits selecting key informants who are knowledgeable about the situation (Amin,2005). The study also used purposive sampling to select all Technical staff of the Cyber Security Unit and Emerging Technologies in each of these firms due to the need to target respondents who are knowledgeable on required information.

Primary data was collected using questionnaires and interview guides in focus groups. Secondary data was collected through documentary analysis. Secondary data sources include; previous researches and analyses of scholars; books, Journals, Conference proceedings, white papers and Government publications on cyber security that are related to the current trend of cyber emerging threats.

These mainly were composed of closed ended questionnaires to the respondents. The closed ended questionnaires form is advantageous in that it will be easy to fill out, saves time and keeps respondents on

subject and relatively objective. The questionnaire used a 5-point Likert scale ranging from 5 (strongly agree) to 1 (strongly disagree), in order to provide consistent responses. The questionnaire was designed to establish the extent of the respondents' agreement with the statements. The questionnaire was preferred because it's a quick way in data collection and it's easy to categorize, Quantify and generalize information.

Reliablity and validity of the instrument was tested.Reliability refers to the consistency of a test, survey, observation, or other measuring instruments and describes the extent to which instruments will produce consistent results in similar conditions over time (Holmström et al., 2009). Validity refers to the credibility and/or dependability of the research results (Salat&Dillman, 1994). In order to ensure validity, the researcher employed several methods including triangulation of data obtained via different research instruments and review, prolonged engagement with respondents. (Holmström et al., 2009).

Accordingly, a pilot study to pretest the questionnaire was conducted using 5 respondents randomly selected from the target respondents with similar characteristics as the target population but who were not to participate in the final survey. The instrument was also discussed with content experts suggested by the supervisors in the field of IoT cyber security. The experts were specifically requested to indicate whether the items in particular sections of the questionnaire adequately measured the respective constructs and whether the instrument was appropriate for this kind of study. The final instrument was developed upon incorporating all comments from the experts.

Assessment instruments must be both reliable and valid for study results to be credible. In the present study, reliability of the assessment tool was estimated using Cronbach alpha test of internal consistency. This test is frequently used to calculate the correlation values among the answers in the assessment tool. Cronbach alpha calculates correlation among all the variables, in every combination; a high reliability estimate should be as close to 1 as possible. The results are presented in Table 3.1.

Variable	*Number of items*	*Cronbach's Alpha value*
IoT threats exposure	9	.934
Risk determination of IoT	27	.968

Source: Primary Data

As shown in Table 1, all variables in the study a Cronbach alpha reliability coefficient above the acceptable minimum of 0.50 (Cronbach, 1951; Nunnally, 1978; Sekaran, 2000). This indicates that the instrument used to collect data in this study was acceptable.

Data obtained from close-ended responses was verified, processed and analyzed using the descriptive and inferential statistical analysis using SPSS version 16.0. The results are presented in the next section 4.

4.0 Results and Discussions

Description Statistics

The demographic characteristics of the respondents analyzed include gender, age, level of education and experience working at the job in Uganda. Results of demographic characteristics of the sample studied are presented using frequency tables.

Table 1.1: Descriptive characteristics of the respondents

Variable (N=127)	Description	Frequency	Percent
Gender	Male	74	58.3
	Female	53	41.7
Age	18-34yrs	40	31.5
	35-44yrs	42	33.1
	45-54yrs	32	25.2
	Above 55yrs	13	10.2
Education level	Diploma	19	15.0
	Degree	40	31.5
	Masters	68	53.5
Experience	<5yrs	39	30.7
	5-10 yrs	39	30.7
	10-15 yrs	30	23.6
	Above 15yrs	19	15.0

Source: Primary Data

Regarding the background characteristics of the respondents, table 1 indicates that the study was male dominated because, out of the 127 respondents constituting a percentage of (58.3%), 74 were males while 53 were females. It also revealed that most of the respondents (33.1%) were in the age bracket of 35-44yrs; followed by (31.5%) who were in the age bracket of 18-34yrs,this was followed by (25.2%) who were in the age bracket of 45-54yrs, and the least percentage (10.2%)were above 55 years.

Regarding the respondents' education level was such that the biggest percentage (68.0%) had above a master's degree, which implies that they could articulately read and understand the questions posed in that questionnaire, followed by degree holders (40%), and diploma holders (15.0%).

Regarding the respondents' experience, the study revealed that the majority of respondents (30.7%) had a work experience in the field of cyber security of 5 to 10yrs,this was followed by (30.7%) who had an experience of less than 5yrs. (23.6%) of the respondents had a work experience of 10 to 15 yrs and (15.0%) had a working experience of above 15yrs in the field of cyber security.

1.2 (IOT) Internet Of Things Cyber Threats Exposure In Uganda

Descriptive analysis was conducted on the items measuring IoT cyber threats Exposure to examine the level of IoT cyber threats Exposure in Uganda. On a scale of 1 = "No exposure" ,implying a low IoT cyber threats Exposure to 5 = "Extremely exposed", implying high IoT cyber threats Exposure. The results are presented in Table 4.2.

Table 4.2: Descriptive statistics of IoT cyber threats Exposure in Uganda

Measurement items	*N*	*Mean*	*S.D*

IoT cyber threats Exposure			
Denial-of-service attacks	127	1.61	1.027
Data espionage	127	1.90	.970
Natural threats	127	1.80	.988
Sabotage	127	1.90	1.050
Computer Frauds	127	1.90	1.113
Malicious attacks	127	1.91	1.088
Message falsification or injection	127	1.98	1.058
Vandalism	127	1.94	1.098
Copyright Violations	127	1.78	1.080

Source: Primary Data

1.3 To predict IoT risk determination and IoT threats exposure in Uganda

Multiple regression analysis was employed to predict values of IoT risk determination (the dependent variable) from the predictor variables (IoT threats exposure). The results are presented in Table 4.3.

Table 4.3. : Regression of IoT risk determination on IoT threats exposure

Predictor variables	*Unstandardized Coefficients*		*Standardized Coefficients*	*T*	*Sig.*
	B	Std. Error	Beta		
(Constant)	1.570	.198		7.943	.000
IoT threats exposure	.663	.096	.525	6.876	.000
Model statistics					
R	.525				
R^2	.276				
Adjusted R^2	.270				
F-statistic	47.282**				

Source: Primary Data

Regression analysis results in Table 4.3 show that IoT threats exposure (b = .525, t = 6.876, P-value < .05) was a significant predictor of IoT risk determination.

The model to predict IoT risk determination was adequate as the F-statistic (F = 47.282, P-value = .000) was significant at the 1% level (r< .01), indicating that the model was statistically significant. Also, an adjusted R2 (coefficient of determination) of .276 suggests that 27.6% of the variation in IoT risk determination is explained by variations in IoT threats exposure.

Thus, the regression model to predict values of IoT risk determination from the predictor variables was specified as: IoT risk determination = 1.570+ 0. 525 (IoT threats exposure).

A change in threat exposure would lead to an increase in risk determination on average by 0.525. The study shows that IoT threats exposure was found to have a positive significant effect on risks determination.(β=0.525,Sig=0.00).

1.4 Factors that determine the internet of things risks in the domain of readiness

Descriptive analysis was conducted on the items measuring Factors that determine the internet of things risks in the domain of readiness in Uganda. On a scale of 1 (strongly disagree) to 5 (strongly agree), mean values less than 2.50 were interpreted as depicting a high readiness. On the other hand, mean values of 2.50 or more depicted low readiness. The results are presented in Table 4.3.

Measurement items	*N*	*Mean*	*S.D*
POLICY (PO)			
There is an IoT Cyber Security Policy, and the policy achieves its intended purpose	127	2.40	1.393
There is existence of a functioning Cyber Security department in my Organization	127	2.57	1.551
There are systematic administrative procedures for gathering information regarding IoT risks	127	2.62	1.431
Mean		**2.53**	
HUMAN RESOURCE (HR)			
There is availability of cyber security trained technical personnel in my organization	127	2.85	1.633
There is documentation and monitoring of the privacy and security training activities for employees in the organisation.	127	2.86	1.361
The organization conducts employee IoT Security awareness and education campaigns.	127	3.01	1.354
Cyber security roles and responsibilities for all staff are established in my organisation.	127	2.96	1.461
Mean		**2.92**	
INFRASTRUCTURE (IN)- DEMAND SIDE INFRASTRUCTURE			
There is infrastructure for monitoring and detecting cyber security threats in my organization	127	2.94	1.388
My organisation has information risk and security management tools.	127	2.92	1.395
My organisation has an incident response plan in place in the event of a breach.	127	2.98	1.586
Mean		**2.94**	
INFRASTRUCTURE (IN)- SUPPLY SIDE INFRASTRUCTURE			
My organisation verifies that the IoT hardware and software acquired performs as expected and their overall security posture is as per the organisational standard.	127	3.17	1.473
The organisation IT security experts are always engaged in the IoT software and hardware preliminary tests with the suppliers before final delivery of the products.	127	3.31	1.417

Mean	**3.24**
Grand mean	**2.91**

Source: Primary Data

As shown in Table 4.3, the grand mean for factors that determine the internet of things risks in the domain of readiness in Uganda was 2.91 suggesting that; overall, the expatriates working in the firms surveyed perceived a high similarity between the readiness. A high similarity among readiness implies the existence of low readiness among the expatriates and local operating environment. This low readiness was attributable to a low policy (mean = 2.53) coupled with high human resources (mean = 2.92). However, there was a high level of infrastructure (in)- supply side infrastructure (mean = 3.24) in the organizations surveyed.

1.5 Factors that determine the internet of things risks in the domain of intensity

Descriptive analysis was conducted on the items measuring Factors that determine the internet of things risks in the domain of intensity in Uganda. On a scale of 1 (strongly disagree) to 5 (strongly agree), mean values less than 2.50 were interpreted as depicting a high intensity. On the other hand, mean values of 2.50 or more depicted low intensity. The results are presented in Table 4.4.

Measurement items	*N*	*Mean*	*S.D*
AWARENESS (AW)			
There is an IoT Cyber Security Policy, and the policy achieves its intended purpose	127	3.29	1.392
There is existence of a functioning Cyber Security department in my Organization	127	3.22	1.532
We regularly train staff to make them aware about IoT cyber security risks in the organisation.	127	3.54	1.557
Mean		**3.35**	
SEVERITY AND IMPACT(SI)			
I understand the need to safeguard personal information from un-lawful access	127	4.05	1.240
Any personal data online or on an IoT device is treated as confidential and cannot be disclosed without one's consent.	127	3.76	1.355
There is an accounting mechanism to determine the effect of IoT cyber crime	127	3.59	1.293
Mean		**3.80**	
Grand mean		**3.57**	

Source: Primary Data

As shown in Table 4.4, the factors that determine the internet of things risks in the domain of intensity surveyed in Uganda was high (Grand mean = 3.57). This high level of intensity was attributed by a severity and impact (mean = 3.80). On the other hand, the results indicate that awareness was modest (mean = 3.35).

1.6 Factors that determine the internet of things risks in the domain of adoption

Descriptive analysis was conducted on the items measuring Factors that determine the internet of things risks in the domain of adoption in Uganda. On a scale of 1 (strongly disagree) to 5 (strongly agree), mean values less than 2.50 were interpreted as depicting a high adoption. On the other hand, mean values of 2.50 or more depicted low adoption. The results are presented in Table 4.5.

Measurement items	*N*	*Mean*	*S.D*
PRIVACY AND SECURITY.(PS)			
I am satisfied with the inherent security built in commonly available IoT devices and networks	127	1.61	1.025
The effect and impact of IoT cyber crime rate is evaluated at my organization	127	1.89	.970
There is a department to manage the IoT cyber threats and risks at my organization	127	1.80	.987
Mean		**1.77**	
SELF EFFICACY (SE)			
I have the necessary skills to handle common IoT security risks	127	1.94	1.049
I have knowledge to identify and address potential IoT cyber security risks for users and providers than our competitors	127	1.90	1.112
I am aware of the fundamental standards that make it possible to create flexible strategies for the protection of organisational IoT devices and applications against IoT cyber security risks.	127	1.91	1.087
Mean		**1.92**	
FACILITATING CONDITIONS(FC)			
We have technological skills and competencies in the organization for increased protection and security against the IoT cyber security risks.	127	1.98	1.058
We have in-house expertise to help in adoption, of security controls and monitoring of IoT cyber security risks in the organisation.	127	1.94	1.097
The organization has financial resources to put in place the infrastructure needed to secure against IoT cyber security risks and threats	127	1.77	1.078
Mean		**1.89**	
Grand mean		**1.86**	

Source: Primary Data

As indicated in Table 4.5, the overall, the level of Factors that determine the internet of things risks in the domain of adoption surveyed in Uganda was low (Grand mean = 1.86). This level of performance is majorly attributed to low satisfaction with the inherent security built in commonly available IoT devices and networks (mean = 1.61, S.D = 1.025) and limited financial resources to put in place the infrastructure needed to secure against IoT cyber security risks and threats (mean = 1.77, S.D = 1.078). Others include

the effect and impact of IoT cyber crime rate is not being efficiently evaluated (mean = 1.89, S.D = .970) and absence of a department to manage the IoT cyber threats and risks at mean = 1.80, S.D = .987).

Conclusion

Cyber security is a new area of research that has rapidly attracted attention in the government, Technology industry and academia. The aim of this survey is to assess the state of Cyber security emerging threats. The results do reveal that there is low satisfaction with the inherent security built in commonly available IoT devices and networks, and limited financial resources to put in place the infrastructure needed to secure against IoT cyber security risks and threats. The study also revealed that there was a high level of intensity to determine the internet of things risks, the expatriates working in the firms surveyed perceived a high similarity between the readiness.

The study also revealed that Denial-of-service attacks, Data espionage, Natural threats,Sabotage,Computer,Frauds,Malicious attacks, Message falsification or injection,Vandalism,Copyright Violations are some of the major IoT cyber threats that the country is exposed to.

The paper argued that Cyber security is not necessarily only the protection of cyberspace itself, but also the protection of those that function in cyberspace and any of their assets that can be reached via cyberspace. It was predicted that Cybercriminals tactics in the near future is focused to be more complicated and difficult to prevent, detect and address compared to the current known ones (Babate et al,2015). This study therefore, recommends that governments and IT industry globaly should be wary of the growing danger of cybercrime in the near future and better improvise secure and efficient implementation of IoT technologies.

References

1. Treffyn L, K., Toni, R., Tuck W,L.(2013)Internet of Things: a review of literature and products.Conference Paper · ACM 978-1-4503-2525-7/13.DOI: 10.1145/2541016.2541048.

2. Krejcie, R.V., & Morgan, D. W (1970). Determining Sample Sizes for Research Activities, Educational and Psychological Measurements, 30,608.

3. Taylor, P., Allpress, S., Carr, M., Lupu, E., Norton, J., Smith, L.,Blackstock, J., Boyes, H., Hudson-Smith, A., Brass, I., Chizari, H.,Cooper, R., Coulton, P., Craggs, B.,Davies, N., De Roure, D.,Elsden, M., Huth, M., Lindley, J., Maple, C., Mittelstadt, B.,Nicolescu, R., Nurse, J., Procter, R., Radanliev, P., Rashid, A.,Sgandurra, D., Skatova, A., Taddeo, M., Tanczer, L., Vieira-Steiner, R.,Watson, J.D.M., Wachter, S., Wakenshaw, S., Carvalho, G., Thompson,R.J., Westbury, P.S., (2018). Internet of Things: realising the potential of a trusted smart world. Royal Academy of engineering: London.

4. Babate,A,I. Musa,M,A., Kida,A,M., Saidu,M,K(2015). State of Cyber Security: Emerging Threats Landscape. International Journal of Advanced Research in Computer Science & Technology

5. Von Solms,R, Niekerk,J.(2013)From information security to cyber security. computers & security38(2013) 97 e102. Elsevier Ltd

6. Ralstona, P.A.S., Grahamb, J.H., Hiebb, J.L.(2007)Cyber security risk assessment for SCADA and DCS networks. ISA Transactions 46 (2007) 583–594.

7. Hahn,A.,Ashok,A.,Sridhar,S.,Govindarasu,M.(2013).Cyber-Physical Security Testbeds: Architecture,Application, and Evaluation for Smart Grid. IEEE TRANSACTIONS ON SMART GRID, VOL. 4, NO. 2.

8. Salant, P.&Dillman, A. (1994). How to conduct your own survey. John Wiley & Sons,Inc 1994

9. Holmström, J., Ketokivi, M., &Hameri, A. (2009). Bridging Practice and Theory: A John Wiley & Sons, Inc (2009).Design Science Approach to bridging Practice and Theory

10. Amin, M.E. (2005). Social Science Research, Conception, Methodology Analysis. Kampala: Makerere University Printery.

11. Ollie white house (2015), An Implementer's Guide to Cyber-Security for Internet of Things Devices and Beyond.

12. Marco Gercke (2010) "The role of ICT regulation in addressing offenses in cyberspace" ITU GSR 2010 Discussion Paper,

13. Melissa Hathaway, (2013) "Cyber Readiness Index 1.0", Hathaway Global Strategies LLC.

14. Radanliev,P., Charles De Roure,D., Nicolescu,R., Huth,M., Mantilla Montalvo,R., Cannady, S., Burnap,P.(2018).Future developments in cyber risk assessment for the internet of things. Computers in Industry 102 (2018) 14–22

15. Radanliev, P., De Roure, C.., Cannady, S., Montalvo, R.M., Nicolescu, R., Huth, M., (2018). Economic impact of IoT cyber risk - analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance, in: Living in the Internet of Things: Cybersecurity of the IoT - 2018. Institution of Engineering and Technology, London.