Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2017 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

Summer 7-19-2017

Cyber Security Violation in I0T-Enabled Bright Society: A Proposed Framework

Magiswary Dorasamy
Multimedia University, magiswary.dorasamy@mmu.edu.my

Su-Cheng Haw
Multimedia University, sucheng@mmu.edu.my

Thesigaruphani Vigian
Multimedia University, thesigarhupani@mmu.edu.my

Cyber Security Violation in IoT-Enabled Bright Society: A Proposed Framework

Research-in-Progress

Magiswary Dorasamy
Multimedia University
Persiaran Multimedia, 63100
Cyberjaya, Selangor
magiswary.dorasamy@mmu.edu.my

Su-Cheng Haw
Multimedia University
Persiaran Multimedia, 63100
Cyberjaya, Selangor
sucheng@mmu.edu.my

Thesigaruphani a/p Vigian
Multimedia University
Persiaran Multimedia, 63100 Cyberjaya, Selangor
thesigarhupani@mmu.edu.my

Abstract

The undesirable consequences of ICT proliferation remains a big concern. The rise in Internet of Things (IoT) have further exacerbated security and information privacy challenges. One main reason is organizations and individuals constantly violate regulations and rules. While cybersecurity and privacy scholars accentuate on the likelihood of rule violations at the individual and organizational levels, the evidence for and discussion of this concept is still scant. This study proposes an empirical response to the Bright ICT initiative of the Association of Information System. This initiative aims to drastically eliminate adverse effect of Internet of Things (IoT). However, a robust privacy and cybersecurity model is needed. This study draws on the selective organizational information privacy and security violation model and delineate it at individual level. Specifically, attitude towards behaviour and subjective norms, contextual conditions, rule and regulatory conditions, perceived risk of violating a privacy or security rule, economic and non-economic strain constructs are hypothesized to determine the likelihood of a privacy and cybersecurity rule violation. In this context, pertinent cybersecurity literatures for IoT-enabled environment were examined to suggest solutions to reduce the dark side of IoT-enabled bright society. This paper presents the proposed model.

Keywords: Cybersecurity, piracy, IoT, bright society, ICT

Introduction

Despite impressive progress in cybersecurity measures, the undesirable consequences of ICT proliferation remain a big concern. The rise in Internet of Things (IoT) have further exacerbated security and information privacy challenges. One main reason is organizations and individuals constantly violate regulations and rules. While cybersecurity and privacy scholars accentuate on the likelihood of rule violations at the individual and organizational levels, the evidence for and discussion of this concept is still scant. This study proposes an empirical response to the Bright ICT initiative of the Association of Information System. This initiative aims to drastically eliminate adverse effect of Internet of Things (IoT). However, a robust privacy and cybersecurity model is needed. This study draws on the selective organizational information privacy and security violation model and delineate it at individual level. Specifically, attitude towards behaviour and subjective norms, contextual conditions, rule and regulatory conditions, perceived risk of violating a privacy or security rule constructs are hypothesized to determine the likelihood of a privacy and cybersecurity rule violation. In this context, pertinent cybersecurity literatures for IoT-enabled environment were examined to suggest solutions to reduce the dark side of IoT-enabled bright society. Driven by a positivistic

research philosophy, this study focuses on testing the research model driven by three anchor theories: Merton's strain theory, privacy and security violation model and theory of reasoned action. The hypothesized model will be tested with data to be collected from the survey of high-risk group youths in Malaysia. SEM will be applied to test the hypotheses. Outcome of this study will give light to reduction of violation likelihood and promoting cybercrime awareness for better prevention aimed at high-risk group. Hence, the benevolent intention of the IoT-enabled Bright Society initiative will lay foundation for a new and safer Internet platform for Malaysians. This paper aims to present the proposed theoretical framework.

The Problems

ICT has changed our life to better life. Such changes have driven growth and innovation in the business world. However, the dark side of ICT proliferation is increasing incidents of cybercrimes. Cyberspace has become a goldmine of violations, crime and terrors. A recent Semantec's Internet Security Threat Report 2015 indicated that attackers are moving fast compared to defenses (Semantec, 2015). Risks to IoT-enabled society are increasing due to heavy usage of smartphones and wearable devices. Based on Symantec report, health apps are among the high risk wearable devices with 52 percent of them do not have clear privacy policy (Semantec, 2015). 68 percent of the users declared that they did not realize that they agreed to give access while downloading a free app (Semantec, 2015). It is shocking that at least 1 million malicious apps exist at present. The attacks are on the IoT-enabled society who uses wearable devices and the Internet. Semantec confirms that most devices that forms the IoT infrastructure are already under attack (Semantec, 2015). IoT is extremely exposed to various attacks. The reasons for the vulnerability is firstly, its components are often unattended and remotely located (Ashraf & Habaebi, 2015). Hence, cyber intruders are able to launch physical attacks as there is lack of security measures. As IoT systems become very sophisticated, interoperability and maintenance issues are also added to the existing security problem. Most of IoT objects are smart and therefore, human intervention to manage security is even harder. Secondly, wireless technology is commonly used by IoT for communication. Wireless transmissions is known for its vulnerability for information to be compromised. Scholars in cybersecurity and privacy research accentuate that violation of rules and regulations in contextual conditions be it formal or informal and rule is has possible influence on perceived risk of violating a privacy or security rule. Another prominent condition is rule and regulation conditions that includes enforceability, goal clarity of rules and rule connectedness that possibly influence the violation. However, these constructs have not been empirically tested to give light to the question whether an organization or an individual can be effectively protected from privacy or cybersecurity rules violation. This research will examine the impact of these two conditions with a new condition that focuses on individual psychological context to extend the current privacy and security violation model. Given the problems in IoT-enabled society, this research seeks to show that the likelihood of violating a privacy and security rule at individual level might be deeply rooted on the individual psychological factors (Wall et al., 2015).

Given the problem, the research questions for this research are: 1.Why attacks on IoT devices are more serious than ever? 2. How externally communication structures and governed policy influence the likelihood of privacy and security violation? 3. How attitude towards behaviour and subjective norms influence the likelihood of privacy and security rule violation? Objectives of this study are: 1. To investigate the vulnerability of IoT-enabled society towards privacy violation and cybercriminals. 2. To investigate the influence of formal and information communication structures towards perceived risk of violating a privacy or security rule, at individual level. 3. To investigate the influence of attitude towards behaviour and subjective norms towards the likelihood of privacy and security rule violation. 4. To formulate an enhanced privacy and cybersecurity violation model for IoT-enabled bright society to create awareness on cybercrime among high-risk group youth in Malaysia. Youth is chosen the focus group as they are the future generation that will thrive in a digital economy. Microsoft survey 2017 revealed that Malaysian youth expects IoT to have biggest impact on their future (Chua, 2017). Youth have ranked IoT as top technology for that will contribute to their growth (Chua, 2017). According to the survey, 35% of the youth of Malaysia has security and privacy as their top concern in regards to IoT (Chua, 2017). This reflects how important it is to establish trust on IoT in order to leverage the technology for their future improvement. Hence, this study aims to study on youth in order to make bigger impact to the future generation and digital economy.

Background

Recent report on cybersecurity by Semantec revealed that 378 million global users were recorded as victims of cybercrimes in 2013. Specifically, 38% of mobile users have experienced mobile cybercrimes (Semantec, 2013). Distributed denial of service (DDos) attacked almost 60% of companies in North America. In Malaysia, 38 incidents of DOS has been recorded in year 2015 (MyCert, 2015). Besides this, Semantec reported that cybercrime cost US$113 billion to consumers in year 2013. The growing volume of attacks in the Internet, specifically through Internet of Things (IoT) enabled applications is alarming. According to Gartner, the spending on information security has increased significantly since 20014 as organizations are becoming more aware of the threats (Moore, 2015). Therefore, the need to study on the likelihood of information privacy and security violation is inevitable. One of the initiative to solve this problem was proposed by the Council of the Association for Information Systems (AIS). The Council has adopted a grand vision of an ICT-Enabled Bright Society (in short, the Bright ICT Initiative). This initiative is a bottom-up approach to prevent security issues. This study will also support this Bright ICT initiative. The expected outcome is to create an IoT-enabled bright society that is able to leverage the ICT proliferation without any interference from cyber-attacks.

Malaysian Scenario

Malaysia is ranked at 3rd in the world for Global Cybersecurity Index by International Telecommunication Union (ITU) 2015 (ITU, 2015). This ranking was evaluated based on countries readiness on commitment and preparedness of a country. Malaysia Computer Emergency Response Team (MyCERT) which was formed in 1997 is the main agency of Cybersecurity Malaysia. GCERT MAMPU was founded in 2001 by the Government ICT Security Policy Framework (PA 3/2000) MyCERT and GCERT aim to ensure continuity of government ICT arrangements. GCERT has collaboration with 55 other CERT agencies. In addition, Malaysia has established the following frameworks, directives and policies for cybersecurity (ITU, 2015): 1. National Cybersecurity Frameworks, 2. National Cyber Security Policy (NCSP), 3. Arahan 24 (NSC Directives No. 24), 4. The Cabinet's Decision in 2010, 5. Arahan Keselamatan under Chief Government Security Office (CGSO), 6. NCSP – Policy Thrust 3: Cybersecurity Technology Framework, Specifically for cybersecurity, three more instruments are enacted: 1. Communications and Multimedia Act 1998, 2. Financial Services Act 2013 and 3. Digital Signature Act 1997.

Despite this impressive cybersecurity ranking, control and measures, the country still faces continuous stream of attacks and Internet vulnerabilities. In year 2015 alone, about 9915 cyber threats and attacks were report (MyCert, 2015). This attacks includes content related attacks, cyber harassments, denial of service, fraud, intrusion, intrusion attempt, malicious code, spam, and vulnerabilities report as show in Figure 1. In addition, RMK11 has highlighted crime prevention as one of the main focus. Through the Safe City Programme cybercrime prevention will be intensified in terms of omnipresence, and volunteerism programmes. This programme targets to reduce the crime rate by 5% annually. In addition, it also aims to increase the perception of feeling safe from 39% in 2014 to 60% in 2020 (RMK11, 2015). Hence, this study is timely to identify individual level information privacy and cyber security violation likelihood among youth in Malaysia.

The Internet of Things

The Internet of Things (IoT) refers to all computing devices that has Internet connectivity. This includes a wide range of wearable devices such as smartwatch, fitness trackers, calculator watch, smart shoes, e-textiles, heart monitors and other Internet-enabled devices such as smart tvs, vehicle control, networks, and smart home appliances. The diverse threats are reflected by the diverse devices (Gomes, 2015, Ashraf and Habaebi, 2015).

Theoretical Framework

This study advances understanding on the prevention of information privacy and cyber security violations to create IoT-enabled bright society. Thus, the literatures in violations to privacy and security research identified that individual violations of privacy and cyber security rules are dynamic and volatile (Wall et al., 2015). The selective organizational information privacy and security violations model (SOIPSVM) model is explains the behavior of organizations. This model was originated from Merton's strain theory (1938), which is leveraged to suggest that organizations that cannot achieve socially desirable goals through legitimate means might seek to do so through deviant

behavior. In the context of society, societal goals that are general accepted influences an individual to conform to achieve the goal, failing which leads to their involvement in a deviant culture. According to Merton, "societies that placed a lot of emphasis on monetary success and accumulated wealth and a low emphasis on the norms and rules for attaining these goals have higher crime rates." (Cote, pg. 97). In this study, we believe that this theory can explain the reason for individuals involving in cyber security violations. Second theory that underlies our proposed model is Theory of Reasoned Action (TRA). TRA posits that "individual behavior is driven by behavioral intentions where behavioural intentions are a function of an individual's attitude toward the behaviour and subjective norms surrounding the performance of the behavior" (www.istheorizeit.org). Individual's attitude towards positive and negative feelings and subjective norms are evaluated for desirability of an action. We believe that this theory can explain individual's change of behavior towards deviant culture. We combined all these 3 theories/models to explain the problem addressed in this study. This study will extend the model by adding individual level behavior towards rule violations. To this end, net impact of likelihood of rule violations mediated by perceived risk by individuals is considered to vary across youths who are considered high-risk group in cyberspace. We believe that investigating the implications of individual behavioral variables will give light to broader understanding of the role of privacy and security rule violation models towards creating an IoT-enabled bright society.

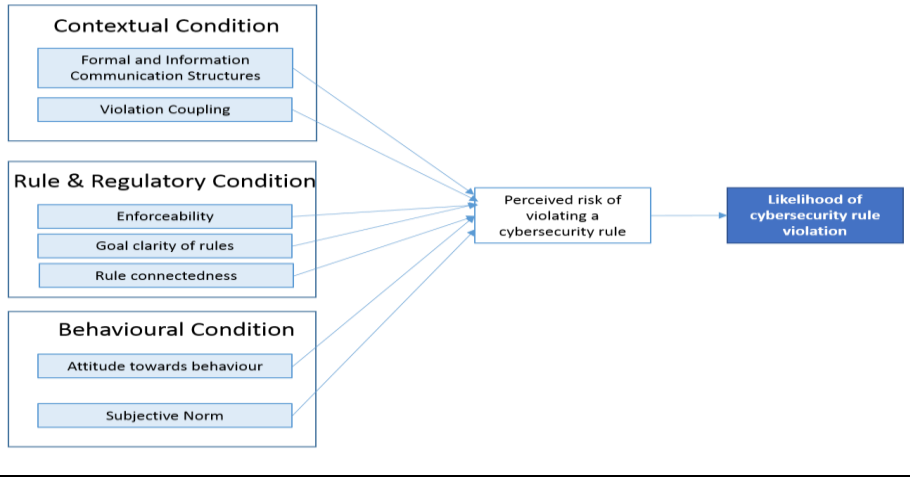

Figure 2. The Individual Cybersecurity Violations Model for IoT-Enabled Bright Society

	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Content Related	2	3	3	3	0	4	6	3	1	3	4	1	33
Cyber Harassment	30	40	32	51	30	45	42	32	24	43	43	30	442
Denial of Service	1	2	2	5	3	3	5	7	2	3	2	3	38
Fraud	276	235	232	313	303	388	253	252	247	230	231	297	3257
Intrusion	88	508	29	63	21	20	85	233	206	215	178	68	1714
Intrusion Attempt	28	22	21	21	10	6	13	8	13	42	84	35	303
Malicious Code	21	30	26	26	35	51	43	39	220	31	26	19	567
Spam	389	430	455	434	348	850	338	88	58	63	47	39	3539
Vulnerabilities Report	1	1	2	2	4	0	1	3	2	1	2	3	22
TOTAL	836	1271	802	918	754	1367	786	665	773	631	617	495	9915

Figure 1. MyCert Reported Incidents based on General Incident Classification Statistics 2015 (MyCert, 2015)

The definitions of the constructs presented in the above model are:

Table 1: Definitions of Constructs		
Constructs	**Definition**	**Sources**
Formal and Information communication structures	"the way that patterns of information, organizational structures, processes, and transactions, and the structure of regulatory relations systematically undermine the attempt to know and interpret situations in organizations".	Vaughan, 1996, p. 238
Violation coupling	"the perceived likelihood that… violations will lead to known outcomes – either positive, such as a performance improvement, or negative, such as regulatory penalties"	Lehman & Ramanujam, 2009, pp. 648
Enforceability	"the extent to which organizations view regulatory agencies as able and likely to monitor compliance with a rule and seek justice for violations"	Fuller, Edelman, & Matusik, 2000
Goal clarity of rules	"the extent to which a rule designates objectives that minimize the potential for alternative interpretation and provides information about how to achieve the objectives"	Tziner, Kopelman, & Livneh (1993). Wall et al., (2015) pp. 35
Rule connectedness	"the amount of interdependence or the number of functional links a rule has with other rules"	March et al., 2000, Wall et al., (2015)
Attitude towards behaviour	"as the individual's positive or negative feelings about performing a behaviour. It is determined through an assessment of one's beliefs regarding the consequences arising from a behavior and an evaluation of the desirability of these consequences"	IS Theoriseit.com
Subjective norm	"as an individual's perception of whether people important to the individual think the behavior should be performed."	IS Theoriseit.com
Perceived risk of violating cybersecurity rule	"the extent to which a rule violation will be perceived as having negative outcomes that are certain, severe, and uncontrollable" in the context of cybersecurity	March & Shapira, 1987, Wall et al., (2015)
Likelihood of rule violation	"to the degree to which systemic factors within an organization and regulatory environment may prompt an organization to violate an externally governed rule established to protect the privacy and security of confidential information"	Wall et al., (2015), pp. 22-23

Table 1: Definitions of Constructs

Given the problem, background and related theories, we hypothesize that:

H1: Perceived risk of violating a privacy or cybersecurity rule has negative influence with the likelihood of a privacy or security rule violation for IoT-enabled society
H2: Formal and informal communication structures that favour rule compliance will increase individual perception of risk of violating rule
H3: Violation coupled to negative outcomes will increase individual perceptions of risk association with rule violation
H4: Enforceability of rule and regulation will positively influence individual perception of risk of violating rule
H5: Goal clarity of rules will positively influence individual perception of risk of violating rule
H6: Connectedness will positively influence individual perception of risk of violating rule
H7: Attitude towards behaviour will positively influence individual perception of risk of violating rule
H8: Subjective norms will positively individual perception of risk of violating rule

Method

This study will adopt quantitative survey in investigating the cybersecurity rule violation on IoT enabled services, based on the hypothesized relationships mediated by perceived risk construct. Another important issue in research design is the specification of the unit of analysis, which is the level of investigation. This study's main unit of analysis is the individuals who are in the category of youth of Malaysia (age between 16 – 30), the high-risk category of users who are inclined to violate rules of cybersecurity. Specifically, the subject measures for each variable will be assessed using Likert Five-point interval scales. The primary level of analysis is the individual; therefore, in order to ensure respondents' heterogeneity, the purposive sampling method will be used in the selection of respondents. The survey is expected to target 500 individuals, citizens of Malaysia. While, the proposed study's subgroup (or strata) will be the based on the demographic categories and location

clusters. At the initial stage, the Statistical Package for the Social Sciences (SPSS) will be used in order to screen the data and obtain the univariate statistical analysis. The second stage will make use of SEM for confirmatory test. This will involve the evaluation of the hypothesized relationships among the constructs and associated dimensions, as earlier explicated. Considering the multiple nature of relationships among the variables, SEM has been selected for its support in conducting multiple regression analyses simultaneously, with the incorporation of the measurement error in the estimation process.

Conclusion

This study aims to contribute to the Bright ICT initiative of the Association of Information System. The project is at the stage of finalizing instruments for data collection. Upon completion of this study, the proposed framework is expected to provide a robust cybersecurity model for IoT-related usage.

Acknowledgements

We thank the Ministry of Higher Education of Malaysia for funding this project under Fundamental Research Grant Scheme (FRGS) 2016–2018. The project ongoing and currently is at a preliminary state.

References

Ashraf, Q.M. & Habaebi, M.H. 2015. "Autonomic Schemes for Threat Mitigation in Internet of Things," *Journal of Network and Computer Applications*, (49:2015), pp. 112-127.

Cote, S. 2002. Criminological Theories: Bridging the Past to the Future, USA: Sage Publications.

Chua, J. 2017. Microsoft Survey: Malaysia Youth Expect Internet of Things To Have Biggest Impact On Their Future.

Fuller, S. R., Edelman, L. B., and Matusik, S. F. 2000. "Legal Readings: Employee Interpretation and Mobilization of Law," *Academy of Management Review*, (25:1), pp. 200-216.

Gomes, J.F. 2015. Futures Business Models of An Internet of Things (IoT) Enabled Healthcare Sector. Master's Thesis, Department of Management & International Business, Autumn 2015, University of Oulu.

International Telecommunication Union (ITU). 2015. Global Cybersecurity Index & Cyber Wellness Profiles Report.

Lee, J.K. 2015. Research Framework for AIS Grand Vision of the Bright ICT Initiative, Guest Editorial, Association of Information Systems.

Lehman, D. W. and Ramanujam, R. 2009. "Selectivity in Organizational Rule Violations," *Academy of Management Review*, (34:4), pp. 643-657.

March, J. G., Schulz, M., and Zhou, X. 2000. The Dynamics of Rules: Change in Written Organizational Codes, Palo Alto, CA: Stanford University Press.

March, J. G. and Shapira, Z. 1987. "Managerial Perspectives on Risk and Risk Taking," *Management Science*, (33:11), pp. 1404-1418.

Moore, S. 2014. Gartner Report 2014. Ava

MyCert (Malaysian Computer Emergency Response Team). Reported Incidents based on General Incidents Classification Statistics 2015.

RMK 11. (2015). Eleventh Malaysia Plan 2016-2020 Anchoring growth on people, Malaysia.

Semantec Report, ISTR20 Internet Security Threat Report. Vol. 18, USA, 2013, pp. 1-58.

Semantec Report. ISTR20 Internet Security Threat Report. USA, Vol. 20, April 2015, pp. 1-119.

Theorizeit. Theory of Reasoned Action. Accessed on 29 April 2017 from https://is.theorizeit.org/wiki/Theory_of_reasoned_action.

Tziner, A., Kopelman, R. E., and Livneh, N. 1993. "Effects of Performance Appraisal Format on Perceived Goal Characteristics, Appraisal Process Satisfaction, and Changes in Rated Job Performance: A Field Experiment," *Journal of Psychology*, (127:3), pp. 281-291.

Vaughan, D. 1996. The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA. Chicago, IL: University of Chicago Press.

Wall, J., Lowry, P.B., and Barlow, J. 2015. "Organizational Violations of Externally Governed Privacy and Security Rules: Explaining and Predicting Selective Violations under Conditions of Strain and Excess," *Journal of the Association for Information Systems*, (17:1), pp. 39–76.