The Relationship between Security Motivations and Security Safeguard Usage

Assoc. Prof. Dr Sureerut Inmor[1]

Information System Department[1]
Rajamangala University of Technology Thanyaburi
Thailand
sureerut_i@rmutt.ac.th*

***Abstract*— Research on Computer Security Safeguard within the workplace in Thailand is aim to survey the computer security safeguard in the workplace and also the motivation of user on the implementation of them. The first hypothesis states that the demographic difference (gender, age, educational level, job type, and working experience), affecting on the level of usage for security safeguard. The second hypothesis is the security motivation (The severity of the damage, Protection Capabilities, System risk, Benefits of system protection) has a relationship with level of usage for security safeguard. The sample group consisted of 385 respondents by simple random sampling of the employee who works on computer related job in Thailand which calculated by Taro Yamane' formula and confidence level at 95 percent. The tools used to collect data were a questionnaire with a reliability level of .98. The statistics used for data analysis are Descriptive statistics and inferential statistics (Independent t-test, One-way ANOVA, and Pearson's chi-squared) at a significant level of .05.. The study found that the different in job type have significant effects on the level of usage for security safeguard. The supporting and training group has the lowest significant level of security usage when compare with other job types. The organization should create security awareness into this group as a first priority before they begin their training jobs. This group will contribute these awareness and security knowledge through other user in general. The result from the study showed that the system risk is the most motivator that has a high relationship with the usage of security safeguard. The training in security should emphasize on the system risk and the damage from the security threat. The organization could use this result to plan for their security training and create security awareness among computer system users.**

Keywords— Workplace Training, Security Safeguard, Security Motivation, Organizational Learning, Security Policy

I. INTRODUCTION

Security threats to computer system are the problem of every organization and government sector nowadays. Several method of security safeguards range from the simple one as password protection, virus defense technology, access control to the complicated one as data encryptions and firewall technology are available to use. [1] The lost from security damage could consume much monetary fund from the organization. There are so many evident that the best way to protect computer resource (hardware, software, database, and network) from such a security damage is to create user awareness and to establish the security policy on how to implement these safeguard more effectively.

Prior to develop the security policy and create user awareness, it is important for the organization to learn from the security motivation. [2] The motivation factor will explain why the user utilizes the security safeguard. This research aims to find the user security motivation toward the way they implement several method of security safeguard in their works.[3] Besides that the study will analyze the difference in demographic background of user in whether they will make a vary decision in using safeguard. The result could be used for organization as a basic knowledge in planning for the security training course both policy and educational priority. They also use this information to create user awareness toward security protection.

In this study, the motivation that could have a possible relationship with the usage of security safeguards are the severity of the damage, protection capabilities, system risk, and benefits of system protection.

II. LITERATURE REVIEW

Computer users in any environment especially online system are experienced security threat those are virus/malware, identity thief, hardware and software damage, information loss, and phishing. The perception of those threats could come from their own experiences, working community, personal use, news, social media, and training course including the security related material. Usually in the organization environment, they are equipped with the tools and technology to provide security to the system such as firewall, physical protection, data encryption during communication, but the user still has to face the security threat problem. This is acceptable in all computer community that beside effective tools and equipment; the human factor is also

importance to the success of security protection. Based on the security baseline composition which consist of 4 aspects as business system basic configuration, state management, and security vulnerabilities, the motivation to response to vulnerability is very important. [4, 5]

Protection Motivation Theory (PMT) created based on the theory of reasoned action. When used PMT in computer security, the theory will explain how and why users decide to implement protective behaviors. The theory classifies motivation of protective behaviors by threat and coping appraisals. There are many researches on this area. The proposed technology threat avoidance theory (TTAT) to identify factors that predict technology threat avoidance behavior found that both threat and coping appraisals were prediction of behavior to avoid threat [6]. Another study by [7] suggests of confidence in security behavior and subjective norms (other opinions) will have an effect on how to avoid security threat.

The subjective norms were also a key factor in several studies [8,9,10]. The subjective norms in computer security mean that how individuals concern about other person who are important to them might think what they should behave. They tend to act according to other people expectation [11]. They considered subjective norm or social norm as important factor to the user behavior on how to implement security safeguard [12,13,14,15,16,17]. There are the studies on factors affecting security protection in home computers and found that there are different factors that affect the protective behavior [18,19]. They found that hazards experience, responsibility, security support, and habit strength are important factors.

The researcher had suggested about the security training program that should be continuous, cover the relevant topics, right after the major incident, and make sure that all the officers understood the whole procedures [20]. They also recommended from the [21] that an officers handling important information should sign a code of conduct. The security policy should follow the organization policy and the law. They also have to attend the security training course as well.

Research from [22] on protection motivation theory (PMT) has investigated motivation factors that predicted security intentions of internet users. They found that habit strength response efficacy, and personal responsibility was the strongest predictor. The research that has conducted a survey on Internet of Things security and suggested the threat to the internet user such as confidentiality, viruses, encryption, and identity theft [23]. They also give the security safeguard to those threats. The research on the principle of security safeguards with the objective to create a set of guideline for protecting personal information with adequacy level of security protection [20]. The result shows the recommended guideline to protect privacy of information. The study recommended encryption technique for the followings information: Legal, Finance, and Customer Information.

Access Right [23]: based on the principle that the data should be secure and accessible to only the authorized user. The system will specify access right to resource that are those important information and peripherals. Password is the simplest way to provide security of computer system. The system administrator will establish user name and verify the password, this process is sometimes called the authentication. The password could be something user has, knows, and is or any combination of these. Beside pre-setting password, the system might use the challenge/response mechanism which is only the challenger (system) and responder (user) knows the shared words [20].

III. METHODOLOGY

A. Purpose of the Study

The research objective is to study the security motivation of IT workers toward the usage of security safeguard. The benefit of the study is to use the information from research as the basic knowledge on how to design security training policy and create user awareness.

B. Conceptual Framework and Hypotheses

The conceptual framework for the research is as follow:

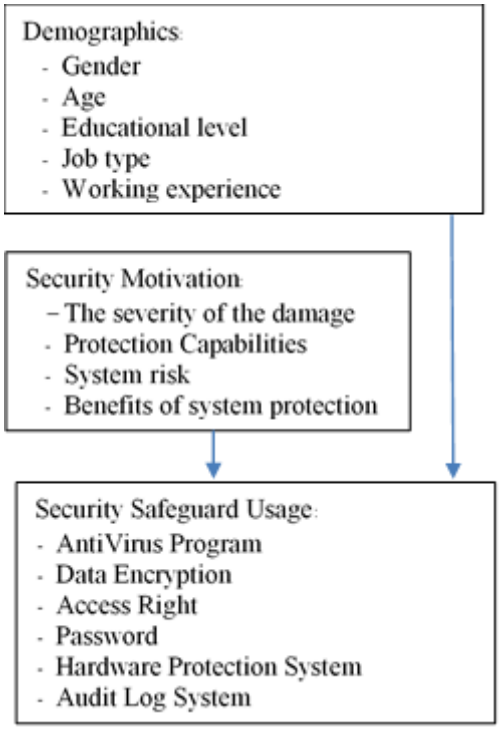

Figure 1. Research Framework.

Hypothesis:

1. The demographic difference affecting on the level of usage for security safeguard.
2. The security motivation has a relationship with level of usage for security safeguard.

C. Scope of Study

The sample group consisted of 385 respondents from the employee who works on computer related job in Thailand. The statistics used for data analysis are Descriptive statistics and inferential statistics (Independent t-test, One-way ANOVA, and Pearson's chi-squared). The target population is 385 IT

workers in Thailand. Questionnaires were used to collect basic data from October 2018 to September 2019.The statistics used for data analysis were descriptive statistics and Pearson correlation.

IV. FINDINGS

The population are mostly Female (63.38), age between 18-25 yrs. (60.86), educational background in Bachelor degree (65.91), with the status of student (55.81%), and the monthly income less than 15,000.00 Thai Baht (69.95%). This is in line with the basic information that social commerce that used by the majority of the younger generation. Analysis of data according to each category using descriptive statistics (frequency, percentage, mean, and standard deviation) displays in Table I.

TABLE I. SHOWS NUMBER (FREQUENCY) AND PERCENTAGE OF DEMOGRAPHIC DIFFERENCES

Demographic Category	Number (frequency)	%
Gender		
Male	238	61.8
Female	147	38.2
Age		
Less than 25 yrs.	99	25.7
25 yrs. – 40 yrs.	244	63.4
More than 40 yrs.	42	10.9
Educational Background		
Less than Bachelor	60	15.6
Bachelor	289	75.1
Master	33	8.6
Higher than Master	3	0.8
Job type		
System Dev.	55	14.3
System Design	42	10.9
System Tester	35	9.1
Customer Support	174	45.2
Other	79	20.5
Working experience		
Less than 3 yrs.	146	37.9
3 yrs. – 6 yrs.	145	37.7
6 yrs. – 10 yrs.	54	14.0
More than 10 yrs.	40	10.4

Most of the respondents are male, age between 25-40 years, bachelor degree background, work as the customer support and have less than 3 years' experience. Due to the emerging of programming package and the outsourcing environment, the customer support and training are getting larger in organization and play important role in the success of security safeguard. The descriptive statistics is used to explain the analysis of relationship of community characteristics and purchasing intention as in Table II.

TABLE II. SHOWS MEANS AND STANDARD DEVIATION FOR THE SECURITY MOTIVATION

Security Motivation	Level of Importance			
	$\bar{x}$	S.D.	Meaning	Order
1. The severity of the damage	2.21	0.587	Moderate	4
2. Protection capabilities	2.48	0.418	Most	2
3. System risk	2.26	0.570	Moderate	3
4. Benefits of system protection	2.60	0.402	Most	1

From the survey, the respondents give the most important to the motivation for benefits of system protection. This should be the main topic in the training course. The user should understand the benefit of each security safeguard on what they can do to the computer system.

TABLE III. DISPLAY MEANS AND STANDARD DEVIATION FOR THE LEVEL OF USAGE FOR SECURITY SAFEGUARD.

Security Safeguard	Level of Usage			
	$\bar{x}$	S.D.	Meaning	Order
1. Antivirus Program	2.48	0.448	Most	1
2. Data Encryption	2.43	0.444	Most	3
3. Access Right	2.45	0.430	Most	2
4. Password	2.33	0.517	Moderate	4
5. Hardware Protection System	2.09	0.489	Moderate	5
6. Audit Log System	2.43	0.475	Most	3

The antivirus program is the security safeguard that is most used in organization. This is the simplest way to implement the safeguard because the user can find the program with less cost and less technical difficulty than other methods. Next section, the hypothesis from the research will be tested.

Hypothesis 1: The demographic difference affecting on the level of usage for security safeguard.

The analysis found that some of the demographic difference has significant effect on the security safeguard usage as follows:

Hypothesis 1.1 The different in job type affect the usage level for security safeguard.

TABLE IV. DISPLAY DIFFERENT DEMOGRAPHIC TESTING DATA AFFECTS THE USAGE LEVEL OF SECURITY SAFEGUARD, CLASSIFIED BY JOB TYPE

Security Safeguard	F	Sig.
1. Antivirus Program	2.702	**0.030***
2. Data Encryption	1.667	0.157
3. Access Right	3.086	**0.016***
4. Password	3.870	**0.004***
5. Hardware Protection System	3.010	**0.018***
6. Audit Log System	2.865	**0.023***

* Significant at the statistical level 0.05

The analysis found that difference in job type affect significantly for the security safeguard in all type except in data encryption. Since this method is implemented by most technical knowledge and somehow done by the system without user acknowledgement, the respondents might not aware of this safeguard.

Next section will be discussed the comparison of significant difference between each job type and each category of security safeguard.

TABLE V. POST HOC TEST (LSD) BETWEEN EACH JOB TYPE FOR THE USAGE LEVEL OF SECURITY SAFEGUARD (ANTIVIRUS PROGRAM).

Job type		Develop.	Design	Tester	Support	Other
		2.67	2.69	2.51	2.46	2.58
Development	2.67		-0.02	0.16	0.21	0.10
			0.873	0.178	**0.012***	0.344
Design	2.69			0.18	0.23	0.11
				0.157	**0.014***	0.298
Tester	2.51				0.06	-0.07
					0.589	0.538

Support	2.46					-0.12
						0.097
Other	2.58					

* Significant at the statistical level 0.05

The analysis found that the support and training group has implemented antivirus program less than development and design group at a significant level.

TABLE VI. POST HOC TEST (LSD) BETWEEN EACH JOB TYPE FOR THE USAGE LEVEL OF SECURITY SAFEGUARD (ACCESS RIGHT).

Job type		Develop.	Design	Tester	Support	Other
		2.75	2.62	2.60	2.47	2.49
Develop.	2.75		0.13	0.15	0.27	0.25
			0.260	0.220	**0.001***	**0.009***
Design	2.62			0.02	0.13	0.11
				0.879	0.205	0.339
Tester	2.60				0.13	0.11
					0.205	0.399
Support	2.47					-0.02
						0.763
Other	2.49					

* Significant at the statistical level 0.05

For the implementation of access right control, the support and training group has used this safeguard less than development group at a significant level.

TABLE VII. POST HOC TEST (LSD) BETWEEN EACH JOB TYPE FOR THE USAGE LEVEL OF SECURITY SAFEGUARD (PASSWOR).

Job type		Development	Design	Tester	Support	Other
		2.55	2.69	2.37	2.29	2.34
Development	2.55		-0.15	0.17	0.25	0.20
			0.292	0.230	**0.015***	0.084
Design	2.69			0.32	0.40	0.35
				0.038*	**0.001***	**0.007***
Tester	2.37				0.08	0.03
					0.528	0.828
Support	2.29					-0.05
						0.593
Other	2.34					

* Significant at the statistical level 0.05

The testing of password protection found that tester and supporting group has utilized this method less than designer group at a significant level.

TABLE VIII. POST HOC TEST (LSD) BETWEEN EACH JOB TYPE FOR THE USAGE LEVEL OF SECURITY SAFEGUARD (HARDWARE PROTECTION SYSTEM).

Job type		Development	Design	Tester	Support	Other
		2.33	2.07	2.29	2.10	1.97
Development	2.33		0.26	0.42	0.22	0.35
			0.057	0.769	**0.027***	**0.002***
Design	2.07			-0.21	-0.03	0.10
				0.153	0.776	0.438
Tester	2.29				0.18	0.13
					0.133	**0.020***
Support	2.10					0.13
						0.147
Other	1.97					

* Significant at the statistical level 0.05

With the hardware protection system, the supporting group still implemented less than the development group at a significant level.

TABLE IX. POST HOC TEST (LSD) BETWEEN EACH JOB TYPE FOR THE USAGE LEVEL OF SECURITY SAFEGUARD (AUDIT LOG SYSTEM).

Job type		Develop.	Design	Tester	Support	Other
		2.45	2.71	2.74	2.49	2.47
Develop.	2.45		-0.26	-0.29	-003	-0.01
			0.031	**0.023**	0.708	0.893
Design	2.71			-0.03	0.23	0.25
				0.831	**0.025***	**0.028**
Tester	2.74				0.25	0.28
					0.019*	**0.021**
Support	2.49					0.20
						0.800
Other	2.47					

* Significant at the statistical level 0.05

The designer group has implemented audit log system more than supporting group at a significant level. The group of job type that most utilized this security safeguard are the designer and tester group because of the nature of their job and difficulty in technical aspect of the safeguard.

The analysis found that difference in job type affect significantly for the security safeguard in all type except in data encryption. Since this method is implemented by most technical knowledge and somehow done by the system without user acknowledgement, the respondents might not aware of this safeguard.

Next section tested the second hypothesis by using Pearson's chi-squared statistics.

Hypothesis 2: The security motivation has a relationship with level of usage for security safeguard.

Hypothesis 2.1: The security motivation (System Risk) has a relationship with level of usage for security safeguard.

The following tables display the result from Pearson's chi-squared statistic.

TABLE X. DEMONSTRATE THE RELATIONSHIP BETWEEN SYSTEM RISK MOTIVATION AND ANTIVIRUS PROGRAM USAGE.

System Risk Motivation	AntiVirus Program Usage		
	Least	Moderate	Most
Least	10	51	0
Moderate	0	95	57
Most	0	9	163
Statistics			
$\chi 2$	Cramer's V	Sig.	
2.404	0.559	**0.000***	

* Significant at the statistical level 0.05

From the analysis found that motivation in system risk has a relationship with the usage of AntiVirus program at significant level 0.05 (Sig.= 0.000) with the redundant relationship (Cramer's V=0.559). The two variables are probably measuring the same concept.

TABLE XI. DEMONSTRATE THE RELATIONSHIP BETWEEN SYSTEM RISK MOTIVATION AND DATA ENCRYPTION USAGE.

System Risk Motivation	Data Encryption Usage		
	Least	Moderate	Most
Least	6	23	32
Moderate	9	67	76
Most	1	50	121
Statistics			
$\chi 2$	Cramer's V	Sig.	
22.416	0.171	**0.000***	

* Significant at the statistical level 0.05

From the analysis found that motivation in system risk has a relationship with the usage of Data Encryption at significant level 0.05 (Sig.= 0.000) with the weak relationship (Cramer's V=0.171). The two variables are minimally acceptable.

TABLE XII. DEMONSTRATE THE RELATIONSHIP BETWEEN SYSTEM RISK MOTIVATION AND ACCESS RIGHT.

System Risk Motivation	Access Right Usage		
	Least	Moderate	Most
Least	5	31	25
Moderate	4	75	73
Most	2	48	122
Statistics			
$\chi 2$	Cramer's V	Sig.	
29.952	0.197	**0.000***	

* Significant at the statistical level 0.05

From the analysis found that motivation in system risk has a relationship with the usage of Access Right at significant level 0.05 (Sig.= 0.000) with the weak relationship (Cramer's V=0.197). The two variables are minimally acceptable.

TABLE XIII. DEMONSTRATE THE RELATIONSHIP BETWEEN SYSTEM RISK MOTIVATION AND PASSWORD.

System Risk Motivation	Password Usage		
	Least	Moderate	Most
Least	16	21	24
Moderate	17	77	58
Most	10	51	111
Statistics			
$\chi 2$	Cramer's V	Sig.	
9.228	0.226	**0.000***	

* Significant at the statistical level 0.05

From the analysis found that motivation in system risk has a relationship with the usage of Password at significant level 0.05 (Sig.= 0.000) with the moderate relationship (Cramer's V=0.226). The two variables are acceptable.

TABLE XIV. DEMONSTRATE THE RELATIONSHIP BETWEEN SYSTEM RISK MOTIVATION AND HARDWARE PROTECTION SYSTEM.

System Risk Motivation	Hardware Protection System Usage		
	Least	Moderate	Most
Least	15	31	15
Moderate	28	89	35
Most	20	92	60
Statistics			
$\chi 2$	Cramer's V	Sig.	
10.259	0.115	**0.036***	

* Significant at the statistical level 0.05

From the analysis found that motivation in system risk has a relationship with the usage of Hardware Protection System at significant level 0.05 (Sig.= 0.036) with the very weak relationship (Cramer's V=0.115). The two variables are not generally acceptable.

TABLE XV. DEMONSTRATE THE RELATIONSHIP BETWEEN SYSTEM RISK MOTIVATION AND AUDIT LOG SYSTEM.

System Risk Motivation	Audit Log System Usage		
	Least	Moderate	Most
Least	8	17	36
Moderate	8	69	75
Most	3	58	111
Statistics			
$\chi 2$	Cramer's V	Sig.	
19.806	0.160	**0.001***	

* Significant at the statistical level 0.05

From the analysis found that motivation in system risk has a relationship with the usage of Hardware Protection System at significant level 0.05 (Sig.= 0.001) with the weak relationship (Cramer's V=0.160). The two variables are minimally acceptable.

V. CONCLUSION/RECOMMENDATION

For the usage of computer safeguard, it is not the whole responsibility of security officers. In several cases, we have to accept that it was the duty of users to follow the security instruction [24]. The duty of security management team is to ascertain that the users have enough knowledge and awareness on the security aspects. The contribution from research will use in designing of security training course that suitable for the specific groups of user. The promotion of user awareness and motivation in protecting their computer system is another area that could gain benefit from this knowledge. We found that the supporting and training group has the lowest significant level of security usage when compare with other job types. The organization should create security awareness into this group as a first priority before they begin their training jobs. This group will contribute these awareness and security knowledge through other user in general. For the user motivation toward the usage of security safeguard, the training course should emphasize on the system risk and the damage from the security threat. This is the result from the study that the system risk is the most motivator that has a high relationship with the usage of security safeguard.

ACKNOWLEDGMENT

This research was supported by Faculty of Business Administrator, Rajamangala University of Technology Thanyaburi. The researcher would like to express great appreciation to all parties that provided us with very valuable information.

REFERENCES

[1] Min Xiao, Mei Guo, Computer Network Security and Preventive Measures in the Age of Big Data: Procedia Computer Science 166 (2020), pp. 438-442.

[2] Sadaf Hina et al., Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world: Computers & Security Volume 87, November 2019, 101594.

[3] Obi Ogbanufe, Enhancing End-User Roles in Information Security: Exploring the Setting, Situation, and Identity: Computers & Security Volume 108, September 2021, 102340.

[4] Yanqing Ding et al., Research and appl ication of secur ity ba seline in bus ine ssinf or mation system: Procedia Computer Science 183 (2021), pp. 630-635.

[5] Ma Li, Zhu Guobang, Lu Lei. Interpretation of the "Basic Requirements for Network Security GradeProtection" (GB / T 22239-2019) [J].Information Network Security,2019(02): pp. 77-84.

[6] Liand H., Xue Y., Understanding security behaviors in personal computer usage: a threat avoidance perspective. J Assoc Int Syst 2010; 11(7):394-413.

[7] Anderson CL., Agarwal R. Practicing safe computing : a multimedia empirical examination of home computer user security behavior intentions. MIS Q 2010;34(3):63-43.

[8] Herath , Rao Hr. Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur J Inf Syst 2009;18(2):106-25.

[9] Ifinedo P. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Comput Secur 2012;31(1):83-95.

[10] Lee Y, Larsen KR. Threat or coping appraisal: determinants of SMB executives; decision to adopt anti-malware software. Eur J Inf Syst 2009;18920:177-87.

[11] Conner M, Armitage CJ. Extending the theory of planned behavior: a review and avenues for further research. J Appl Soc Psychol 1998;28:1429-64.

[12] A.C. Johnston, M. Warkentin.,Fear appeals and information security behaviors: an empirical study. MIS Q, 34 (3) (2010), pp. 549–566.

[13] M.J. Culnan, C.C. Williams.,How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches.MIS Q, 33 (2009), pp. 673–687.

[14] Q. Hu, T. Dinev, P. Hart, D. Cooke., Managing employee compliance with information security policies: the critical role of top management and organizational culture. Decision Sciences, 43 (4) (2012), pp. 615–660.

[15] P.B. Lowry, G.D. Moody., Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organizational information security policies. Information Systems Journal, 25 (5) (2015), pp. 433–463 https://doi.org/10.1111/isj.12043

[16] C. Posey, T. Roberts, P.B. Lowry, B. Bennett, J. Courtney., Insiders' protection of organizational information assets: development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. MIS Q, 37 (4) (2013), pp. 1189–1210.

[17] A. Vance, M. Siponen, S. Pahnila., Motivating IS security compliance: insights from habit and protection motivation theory. Information & Management, 49 (3) (2012), pp. 190–198 https://doi.org/10.1016/j.im.2012.04.002

[18] D. Dang-Pham, S. Pittayachawan., Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: a protection motivation theory approach. Comput Secur, 48 (2015), pp. 281–297 https://doi.org/10.1016/j.cose.2014.11.002

[19] Y. Li, M.T. Siponen., A call for research on home users' information security behavior. PACIS (2011), p. 112.

[20] Rasika D., The principle of security safeguards: Unauthorized activities., Computer Law and Security Review 25 (2009) 165-172.

[21] PIPEDA 226. Company's collection of medical information., unnecessary; safeguards are inappropriate. Available from:http://www.privcom.gc.ca/cf-dc/2003/cf-dc_031031_e.asp;2003.

[22] Hsin-yi, S.T., Mengtian, J., Saleem, A., Robert, L., Nora, J. R., Shelia R. C., 1. Understanding online safety behaviors: A protection motivation theory perspective, Computers & Security Volume 59, June 2016, Pages 138–150 https://doi.org/10.1016/j.cose.2016.02.009

[23] Fadele, A.A., Mazliza, O., Ibrahim, A.T.H., Faiz, A. Internet of Things security: A survey. Journal of Network and Computer Applications 88(2017);10-28.

[24] PIPEDA 315. Web-centred company's safeguards and handling of access request and privacy complaint questioned. Available from: http://www.privcom.gc.ca/cf-dc/2005/315_20050809_03_e.asp; 2003.