Information security threats encountered by Malaysian public sector data centers

Shammugam, Inthrani; Samy, Ganthan Narayana; Magalingam, Pritheega; Maarop, Nurazean; Perumal, Sundresan; Shanmugam, Bharanidharan

Published in:
Indonesian Journal of Electrical Engineering and Computer Science

DOI:
10.11591/ijeecs.v21.i3.pp1820-1829

Published: 01/03/2021

Document Version
Publisher's PDF, also known as Version of record

Indonesian Journal of Electrical Engineering and Computer Science
Vol. 21, No. 3, March 2021, pp. 1820~1829
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v21.i3.pp1820-1829

Information security threats encountered by Malaysian public sector data centers

Inthrani Shammugam[1], Ganthan Narayana Samy[2], Pritheega Magalingam[3], Nurazean Maarop[4], Sundresan Perumal[5], Bharanidharan Shanmugam[6]
[1,2,3,4]Razak Faculty of Technology and Informatics, UniversitiTeknologi Malaysia, Malaysia
[5]Faculty of Science and Technology, Universiti Sains Islam Malaysia, Malaysia
[6]College of Engineering, Information Technology and Environment, Charles Darwin University, Australia

Article Info

Article history:

Received Sep 3, 2020
Revised Dec 7, 2020
Accepted Dec 27, 2020

Keywords:

Data center security threats
ICT security threats
Viral websites threats

ABSTRACT

Data centers are primarily the main targets of cybercriminals and security threats as they host various critical information and communication technology (ICT) services. Identifying the threats and managing the risks associated with data centers have become a major challenge as this will enable organizations to optimize their resources to focus on the most hazardous threats to prevent the potential risks and damages. The objective of this paper is to identify major ICT security threats to data centers in the Malaysian public sector and their causes. The data for this study was collected through interview sessions. A total of 33 respondents from various government organizations were interviewed. The results revealed that the technical threats, spyware, phishing, bluesnarfing threats, social engineering and virus, trojan, malware, ransomware, viral websites threats are the major categories of threats often encountered by the malaysian public sector organizations. The causes for these threats are lack of budget, competent personnel, and manpower for security tasks, user awareness; lack of compliances and monitoring; insufficient security policies and procedures as well as deliberate cyber attacks. The outcome of this study will give a greater degree of awareness and understanding to the ICT security officers, who are entrusted with data center security.

Corresponding Author:

Ganthan Narayana Samy
Razak Faculty of Technology and Informatics
Level 7, Menara Razak, Universiti Teknologi Malaysia
Jalan Sultan Yahya Petra, 54100 Kuala Lumpur, Malaysia
Email: ganthan.kl@utm.my

1. INTRODUCTION

Technological advancements have broken the barriers between countries and the significance of time and place in communications has entirely transformed. The global cyber world connects countries, businesses and citizens completely in a new manner [1] and the information and communication technology (ICT) revolution has tremendously changed the way businesses and governments operate as well as the lifestyle of the citizens. The development of internet of things (IoT), which integrates computer technologies, communications technologies and various industry sectors too poses a big challenge and has created additional information security threats to the IoT applications [2]. In addition, with the change of human social interaction and adoption of emerging technologies, the number and range of information security threats are continuously growing although technological solutions have been improved considerably [3]. While the public sector, the economy, the business communities and citizens benefit from globally networked

services, the digital world has its own inherent vulnerabilities which may pose threats and cause security risks for everyone involved.

Data centers, in particular, have become the main target of cybercrimes and security threats as it hosts all the critical services such as applications, databases, websites, backups, and disaster recovery services. Organizations across the globe heavily dependent on data center infrastructure facilities, which serve as repositories for data storage with a variety of critical ICT assets [2]. As a result, identifying the threats and managing the risks associated with data centers has become a major challenge in the current cyber world. This study's focus is to identify the major threats that are frequently encountered by the data centers in the Malaysian public sector. It reports the results of an exploratory study conducted at various organizations in the Malaysian Public Sector.

As the current world is digitally connected and ICT security threats seem to be unceasing despite the continuous effort, it is imperative for organizations to take necessary steps to ensure their data centers are secure and reliable. Knapp *et al.*, [4] highlighted that the main security issues concerning modern data centers are particularly in regards to data center management, operations and physical security as well as disaster planning. According to [4-7] all disastrous threats that caused major business disruptions and damages to organizations, discussed by past researches were targeted at data centers. As a result, the security of data centers has become an utmost concern for both the government and the ICT industry with the increased societal reliance on internet-based cloud computing to provide secure and affordable storage. Thus, it is crucial for organizations to be able to predict the security risks and implement effective strategies to reduce them by implementing a systematic approach in managing information security [6-10] and the first step to ensure this is to identify the potential information security threats faced by the data centers effectively. This will enable organizations to apply right strategies and tactics to ensure successful information security management to protect organizational goal by curbing digital disruption [11].

According to [12], in Malaysia, cybercrimes and information security threats are expected to rise continuously and will become major concerns to public security and the economy of the country, which will pose dangerous threats if no effort is taken to curtail or prevent them. In 2017, it was reported that more than 150 countries worldwide, including Malaysia were affected by WannaCry with nearly 200,000 cases and the total actual number of attacks is unknown [13]. In 2019, the Malaysian computer emergency response team (MyCERT), a department under cyber security Malaysia, stated that over 400 defacement incidents occurred in Malaysia by 31st of August 2019, which included 19 government organizations [14]. Although the Malaysian government through various organizations have taken efforts to prevent cybercrimes and information security threats by introducing numerous cyber laws and regulations, control of such threats are still dependent on the people [12].

In view of the recurring and increasing ICT security threats in various forms and from various unknown sources targeting the data centers, it is vital for the Malaysian public sector organizations to identify all potential threats and associated risks proactively as well as systematically assess, control and monitor them to prevent any undesired incidents to safeguard the critical ICT assets from disastrous damages such as loss of sensitive and critical information; unavailability of critical systems and information; damages to hardware and software; and most importantly loss of clients' confidence and reputation. This has become even more paramount now as the expectations and demands of the citizens continue to increase, and the government of Malaysia is currently implementing many citizen-centric services through end-to-end ICT applications to increase its efficiency, ease of doing business and global competitiveness.

Critical assets with vulnerabilities can be exploited by threats [15, 16], hence, it is important to protect them from internal and external threats such as the network intrusions, thefts, vandalism, virus, power failures, adverse environmental conditions, and any other security breaches [17]. The ICT assets that are classified as critical for an organization by [9, 15, 16, 18, 19] are information, data, site or facility, software, hardware, personal and organization's structure. ICT infrastructures that are protected with sound and well-managed security program rarely encounter security breaches [20]. Therefore, it is crucial to identify the potential threats and mitigate the risks in time to protect the critical ICT assets, create a safe and secure ICT environment for business continuity.

Jouini *et al.*, [21] proposed a multi-dimensional threat classification model based on criteria such as security threat source or point of origin; security threat agents or cause; security threat motivation, either malicious or non-malicious and security threat intention or the damage. The human threats still remain as a critical and challenging in modern-day business organizations and concurred by many information security specialists [22]. Sarkar [23] stated that insider threat, which is subtle and fundamentally a people issue is a reality when motivated by money or revenge and some well-meaning staff can compromise the security due to their overzealousness in getting their job done. Firoozjaei *et al.*, [24] classified the security threats related to network into three categories, namely the security threats of network infrastructure such as denial of service, network congestion, flooding attacks, information leakage and misuse of shared resources by users;

security threats of network functions virtualization providers such as malware injection, eavesdropping, functional violation, confidentiality compromisation, traffic sniffing, and distributed denial of service attack; and security threats of users such as information leakage and service violation. Zhang *et al.*, [25] in their study, used the architecture of cyber-physical systems to classify the threats for the three layers, namely the perception-execution layer, which consists of physical equipment; the transport layer; and application-control layer.

Public administration, which adopted and operates on new technologies have become more sensitive to service disruption as it affects the reliability, efficiency and quality of their services [26]. Many countries and organizations have acknowledged the need to develop efficient solutions to increase the level of information security for permanent improvement in their delivery system to prevent any disruption and ensure service continuity [26]. Studies conducted previously on threats identification mainly were focused on specific areas such as insider threats, human threats, network front or general in nature. There were very few studies conducted on data center security [6] as only very few scholarly articles are available and none on the data centers in the Malaysian public sector.

2. RESEARCH METHOD

This study employed structured interview method for data collection. The interview questions were prepared based on a list of 86 potential information security threats that identified through systematic literature review, covering various aspects of the ICT operations, which can cause disruption and damage to an organization's business operations as in Table 1. Risk assessment should focus on risks that are most likely to occur and cause serious impacts on organization's operations [7, 27]. The list of threats was further divided into 8 categories based on their characteristics to better understand their impact on ICT assets. Categorization or classification of security threats helps organizations to identify and understand the threats that impact their assets and the effects better, hence, enable them to take the necessary preventive measures to protect their assets in a proactive manner [3, 21, 28].

A total of 33 respondents, representing various government organizations in the Malaysian public sector were selected for the interview. The respondents for this study were among the chief ICT security officers and officers in charge of the data center security. The interview questions were divided into 3 sections. Section 1 consisted of questions related to the demographic information of the respondent such as the name (optional), gender, current post, years of experience, as well as roles and responsibilities with regards to ICT security and data center. Section 2 focused on information on major ICT threats/risks faced in managing the data center. A list of 86 potential information security threats was identified and divided into 8 categories. The respondents were asked to rate them on a scale of 4-0 based on their experience (4=always, 3=often, 2=sometimes, 1=rarely and 0=never). This was followed by another question where the respondents were asked to rank the threat categories according to their frequencies on a scale of 1(most frequent) to 8 (least frequent). Next, they were asked to list down the possible causes for these ICT threats. Finally, Section 3 was queries on currently used guidelines/standards and best practices for risk assessment in managing ICT security risks in their organizations, namely the ISO 27005: information security risk management, ISO 27002: code of practice for information security controls, ISO 27001: information security management system and ISO 31000: risk management. Next, the respondents were also asked to state whether the Malaysian public sector should adopt a suitable Risk Assessment Framework/Methodology to manage the risks to ensure data center ICT security.

Table 1. Threats categories

Num.	Threats Categories Title	Threat ID	Threat Title
1	Virus, Trojan, Malware, Ransomware, Viral Websites Threats	T01	Introduction of virus, Trojan through unlicensed software / attempts
		T02	Malicious codes or Malware attacks / attempts
		T03	Viral Websites -Introduction of virus, Trojan and malware through illegal websites
		T04	Theft and Illegal usage/ misuse of personal information captured through Spyware.
2	Spyware, Phishing, SPAM, Bluesnarfing Threats	T05	Phishing:- Theft, disclosure and illegal use of sensitive financial or personal information through fraudulent email or instant messages.
		T06	Bluesnarfing:- Theft, disclosure of personal information through Bluetooth.
		T08	SPAM email
3	Social Engineering	T09	Attempts / Tricking computer users into revealing computer security or private information such as passwords, email addresses, etc.

(Table continued)

Num.	Threats Categories Title	Threat ID	Threat Title
		T10	Network (LAN/ WAN/ WiFi) service failure/ unavailability
		T11	Network congestion
		T12	Eavesdropping (network function virtualization)
		T13	Traffic sniffing
		T14	Confidentiality compromisation (network function virtualization)
4	Unsecured Wireless Access Points (WAP) / Network Service	T15	High volume of packet transmission or flooding attacks
		T16	Control network denial of service attacks
		T17	Aggregation node or nodes attacks
		T18	Black hole / Packet drop attacks
		T20	Wormhole attacks
		T21	Trap doors Sybil attacks
		T22	Earthquakes/ Tremor
		T23	Flash Flood
5	Natural Disaster / Environmental	T24	Fire
		T25	Tsunami
		T26	Haze drought
		T27	Portal / Service disruption/ unavailability
		T28	Application Systems failure/ Cannot be accessed
		T29	Hardware malfunction (Server, Load balancer, Storage, Printer, etc)
		T30	Software malfunction (OS, web service, etc)
		T31	Failure/ faulty of network equipment (switches, routers, Netapp controller, etc)
		T32	Failure/ faulty of security hardware & software (IPS, Firewall, Antivirus, etc)
		T33	Faulty communication lines
		T34	Electromagnetic leakages/ interferences
		T35	Power surge/ trip/ failure
6	Technical Threats	T36	Unpatched vulnerabilities of software (not known to the users until something occurs)
		T37	Backup failure, Faulty/ defective storage media (tapes, hard disk, cartridges)
		T38	Failure of database caused by technical faulty in hardware/ software error.
		T39	External power supply failures.
		T40	Internal power supply disruption/ failure (rack / fuse, etc)
		T41	Air conditioning / Ventilation disruption / High temperature.
		T42	Chiller system down/ faulty.
		T43	UPS failure or related hardware faulty (battery & other parts).
		T44	Accidental destruction / corruption of part of or whole database.
		T45	Accidental Deletion of customer data.
		T46	Accidentally Deleting proprietary software.
		T47	Accidentally Deleting backups.
		T48	Accidentally Deleting proprietary designs.
		T49	Incompetency of internal staff.
7	Human Error (Accidental)	T50	Incompetency of External Vendors in outsourced project (misconfiguration of hardware or software).
		T51	Incompetency of Temporary / Contract staff.
		T52	Hazards posed by janitors or cleaners (vacuum, sweep, wipe, empty thrash).
		T53	Mishandling of critical ICT assets and other equipment.
		T54	Misleading SOP and Procedures.
		T55	Accidentally shutting down of hardware (servers, console, etc).
		T56	Accidentally shutting down software (application, software, database, etc).
		T57	Deliberate destruction / corruption of part of or whole database.
		T58	Elevation of privilege.
		T59	Unauthorised modification or deletion of customer data.
		T60	Planting logic bombs in application systems.
		T61	Deleting proprietary software or designs.
		T62	Deleting backups.
		T63	Denial of services / legitimate access.
		T64	Denial of information usage / unavailability of data.
8	Deliberate Human Threats	T65	Service violation attacks.
		T66	Distributed denial of service attack.
		T67	Physical attacks.
		T68	Pandemics.
		T69	Riots.
		T70	Wars.
		T71	Terrorist attacks.
		T72	Unauthorised Access to data center facility/ restricted area (illegal entry).
		T73	Vandalism /theft / loss of hardware/ software.
		T74	Website Defacement / Compromised.
		T75	Unauthorised access to servers / critical systems.
		T76	Sabotage by Internal staff (integrity).
		T77	Sabotage by External Vendors in outsourced project (integrity).

(Table continued)

	T78	Sabotage by Temporary / Contract staff (integrity).
	T79	Attempts to hack IP/ intrusion/ invasion of network threats.
	T80	SQL injection.
	T81	Cross site scripting.
	T82	Data breach / information Leakage.
	T83	Privacy in data mining.
	T84	Control command forged attacks.
	T85	Shutting down of hardware (servers, console, etc).
	T86	Shutting down software (application, software, database, etc).

3. RESULTS AND DISCUSSION

3.1. Respondents and experiences

About 33 government organizations were selected for the interview and the respondents consist of 15 (45%) females and 18(55%) males. The analysis also revealed that 4(12%) respondents have more than 15 years of experience, 7(21%) have 11-15 years of experience, 9(27%) have 5-10 years of experience and 13(40%) have less than 5 years of experience in managing data centers.

3.2. Threats frequencies

The analysis of the data obtained for the frequency of the threats shows that the top three threats rated **4 (always)** were the technical threat (13), social engineering (12) and deliberate human threats (10). This was followed by the spyware, phishing and bluesnarfing threats (8), virus, trojan, malware, ransomware, viral websites threats and deliberate human threats (5), accidental human error (4) and unsecured wireless access points (WAP)/network threats (2). No respondent selected the natural disaster/environmental threats under this category. Figure 1 illustrates the analysis results of the frequencies of the major ICT security threats encountered by data centers in the Malaysian Public Sector.

It was also discovered that the top three threats rated **3 (often)** were spyware, phishing, bluesnarfing threats (13), technical threats (12) and social engineering (10). This was followed by deliberate human threats (9), unsecured wireless access points (WAP)/network (7), virus, trojan, malware, ransomware, viral websites threats (6), and accidental human error (5). There was no response for the natural disaster/environmental threats under this category. The top three threats rated **2 (sometimes)** were the accidental human error (13), unsecured wireless access points (WAP)/network (13), and spyware, phishing, bluesnarfing threats (11). This is followed by the virus, trojan, malware, ransomware, viral websites threats (10), deliberate human threats (8), technical threats (7), social engineering (6), and natural disaster/environmental threats (1). The three threats categories rated **1 (rarely)** were the virus, trojan, malware, ransomware, viral websites threats (12), the accidental human error (11), and unsecured wireless access points (WAP)/network (11). This was followed by deliberate human threats (6), natural disaster/environmental threats (6), social engineering (5), technical threats (1), and spyware, phishing, bluesnarfing threats (1). The only threats category that fell under the **0 (never)** rating was the natural disaster/environmental threats with 26 responses.

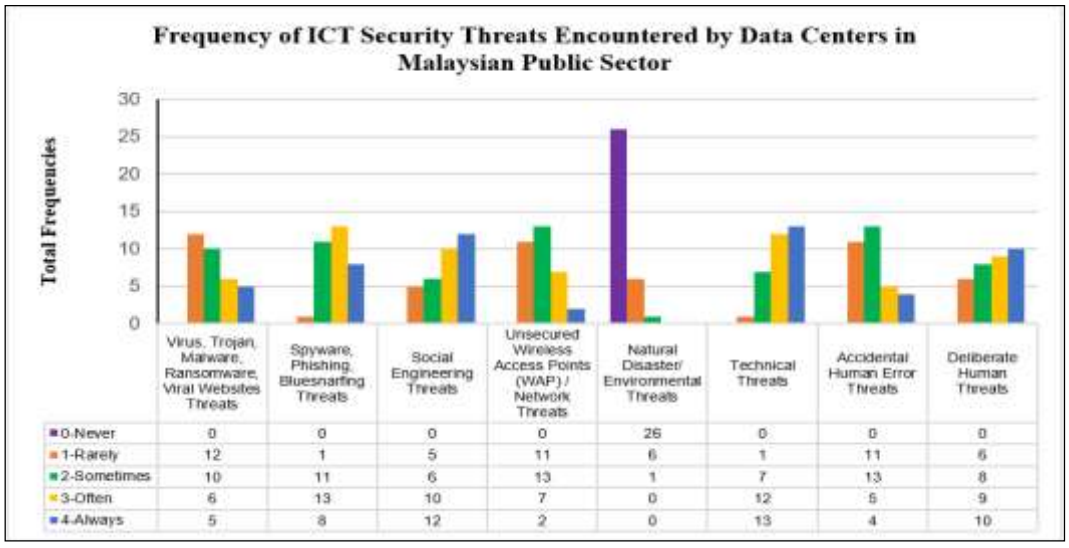

Figure 1. Frequencies of ICT security threats encountered by data centers in the Malaysian public sector

3.3. Threats ranking

Figure 2 depicts the ranking analysis of the threat categories based on their frequencies on a scale of 1(most frequent) to 8(least frequent). The results show that the most frequent threats (highest to lowest based on the total for 1-Most to 4 only) are the Technical threats (28), Spyware, Phishing, Bluesnarfing Threats (24), Social Engineering (24), Virus, Trojan, Malware, Ransomware, Viral Websites Threats (22), Deliberate Human Threats (17), Unsecured Wireless Access Points (WAP)/Network (10), Accidental Human Error (7) and the Natural Disaster/Environmental (0). These ranking results closely match the results for the previous question and indicates the consistency of the respondents in their answers.

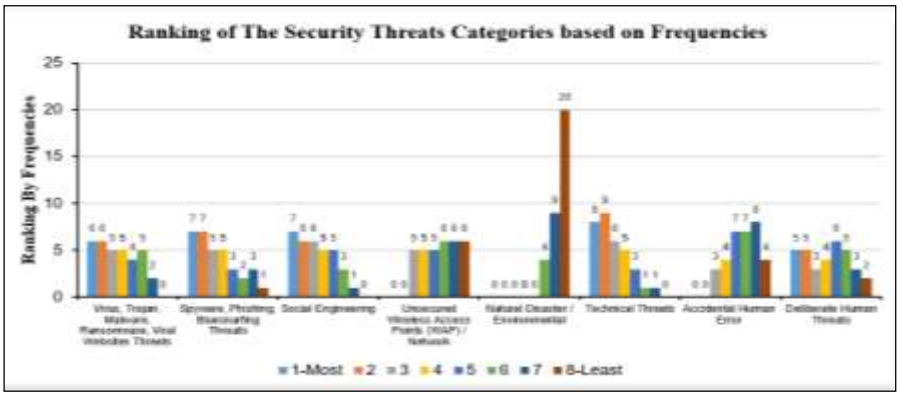

Figure 2. Ranking of the threat categories by frequencies

3.4. Causes of the threats

The Table 2 shows the causes of the threats cited by the respondents.

Table 2. Causes of threats

Num	Threats Categories	Causes
1	Virus, Trojan, Malware, Ransomware, Viral Websites Threats.	Vulnerabilities in hardware/software, Unpatched/un-updated software, Lack of security awareness/ education, Unintentionally downloading free software/email attachments from unknown source, Clicking on false advertisement, Accessing malicious websites/ software, Inadequate or weak security policies/procedures, Failure to follow or violating policies/procedures & Lack of monitoring.
2	Spyware, Phishing, Bluesnarfing Threats.	Lack of security awareness/ education, Too many phishing emails/ attachments/ links to viral websites that confuse the users, Clicking on false advertisement, Inadequate or weak security policies/procedures, Failure to follow or violating policies/procedures, Too many spyware and malware at network layer & Lack of monitoring.
3	Social Engineering.	Too many SPAM emails, SPAM emails come with new email addresses even after being blocked & Lack of security awareness/ education.
4	Unsecured Wireless Access Points (WAP) / Network	Lack of competency in handling critical hardware/ software, Obsolete hardware/ software and products that have reached end of life, Old hardware specifications that do not meet the current requirements, Vulnerabilities in network hardware/ software, Unsupported hardware/ software & Unpatched/ Un-updated hardware/ software.
5	Natural Disaster / Environmental	Lack of competency in identifying the right location & Flood due to failure to identify right location for data center.
6	Technical Threats	Lack of budget to replace obsolete hardware/software and products that has reached end of life, High cost of maintenance, Lack of dedicated staff to focus on ICT security tasks, Lack of competent personnel, Legacy application systems, Old hardware specifications that do not meet the current requirements, Vulnerabilities in old hardware/ software and legacy application systems, Unsupported hardware/software, Unpatched/Un-updated software, Inadequate standard operating procedure (SOP)/ service level agreement (SLA) & Lapse of contract.
7	Accidental Human Threats	Lack of competency in handling critical hardware/ software, Inadequate standard operating procedure (SOP)/ service level agreement (SLA), User negligence & Lack of monitoring.
8	Deliberate Human Threats	Common attacks by outsider/hackers, Information leakage and theft, Web defacement and malicious code injection, Distributed denial of service attacks, Inadequate or weak security policies/procedures, Lack of compliances and monitoring, Inadequate standard operating procedure (SOP)/ service level agreement (SLA), Lack of preventive measures, Weak access control and poor access management, Failure in implementing risk assessment on ICT assets & Lack of enforcement on ICT security compliance and audit.

3.5. Technical threats

The analysis results revealed that these are the most frequent and highest ranked threats by the data centers in the Malaysian public sector. The main cause of these threats are the constraints or lack of resources in terms of budget and manpower. Many have no choice but to continue using obsolete hardware/software. This hardware/software are not supported in terms of maintenance by the suppliers and the latest patches are not being updated. As a result, these hardware and software are very vulnerable and always/often breakdown or experience other technical issues. Another factor that contributes to the technical issues is the lack of experienced, skilled personnel and dedicated personnel to manage ICT security related tasks. The results also show that 40% of the respondents have only less than 5 years of experience in managing ICT security and data centers. This lack of experience leads to mishandling of critical hardware and software as well as negligence.

3.6. Spyware, phishing, bluesnarfing threats, social engineering threats and virus, trojan, malware, ransomware, viral websites threats

These are the next highly encountered and ranked threats categories. Many reasons were mentioned in Table 2. However, the main contributing factor was the lack of awareness and education of the users, which in turn contributed to other factors such as being manipulated clicking on false advertisements and attachments from unknown sources and websites. In addition, factors such as the vulnerabilities of obsolete and outdated hardware/software, lack of strong ICT security policies and failure to adhere to them have also contributed to these threats.

3.7. Deliberate human threats

This category has become a critical challenge which has been continuously faced by the whole world. This is also one of the frequently encountered threats by the data centers in Malaysia as reported by [13, 14]. Some of the reasons cited for these threats were the weak and inadequate ICT security policies/procedures, lack of preventive measures, failure in implementing risk assessment on ICT assets and lack of enforcement on ICT security compliances and audits. These create vulnerabilities in the access system and ICT assets and provide opportunity for deliberate human threats.

3.8. Unsecured wireless access points/network and accidental human error threats

The next 2 categories were the “Unsecured Wireless Access Points/Network” and the “Accidental Human Error Threats”. The reasons cited for these threats were the lack of resources and incompetent personnel. Lack of competency in handling critical hardware/software coupled with negligence also contributed to these threats. This is evident from the results which revealed that 40% of personal managing the ICT security and data centers have less than 5 years of experience. Besides that, the usage of obsolete/unlicensed/unsupported network equipment were also a source of threats.

3.9. Natural disaster/environmental

This threat is something that was rarely encountered by the data centers in Malaysia. This category falls at the bottom of the ranking list and only one respondent responded to this threat. The respondent stated that the cause was due to a failure in identifying the right locate/on for the data center. It must be noted that Malaysia faced a major flood which was described as the worst flood in decades in 2014 [29]. Some government agencies with data centers located in east coast states were affected by this major flood.

3.10. Risk assessment methods and guidelines currently in use

For this, the respondents cited a few methods or guidelines, 15 respondents mentioned that they use the Malaysian risk assessment method (MyRAM) and Malaysian public sector information security high-level risk assessment (HiLRA). 5 respondents stated that they refer to the public sector ICT security policy or Agency’s ICT Security Policy. 2 respondents cited the ISO/IEC27001. 11 (33%) respondents didn’t state anything. The responses also revealed that there was a lack of adherence and monitoring on the agency’s side in ensuring risk assessment is done on their critical ICT assets.

3.11. Should the Malaysian public sector adopt a suitable risk assessment framework/methodology to effectively prevent, mitigate and manage the risks and challenges in ensuring data center ict security?

For this, 31 respondents (94%) indicated that they need a suitable risk assessment methodology whilst 2 (6%) stated that it was not required. This feedback shows that majority of the personnel in charge of ICT security or data center security believe that there is a need for a suitable risk methodology to effectively manage the risks and other security related challenges in their organizations.

The results have revealed the frequent information security threats encountered by the data centers in the Malaysian Public Sector and the causes. This will enable the organizations to optimize their limited resources, adopt right strategies to curb these threats, ensure service continuity and curtail damages to safeguard their reputation.

4. CONCLUSION

This paper discussed an exploratory study of the major ICT security threats to data centers of 33 government organizations. The are 8 categories of common threats that occur in data centers in Malaysian Public Sector were used in this study to identify their frequencies and to determine their ranking as well as to identify their causes. It was discovered that the technical threats, spyware, phishing, bluesnarfing threats, social engineering and virus, trojan, malware, ransomware, viral websites threats are the major threats often encountered by the organizations. The main causes for these threats are the lack of resources in terms of budget and competent personnel, lack of manpower to focus on security tasks, lack of user awareness and education, weak or insufficient security policies and procedures, lack of compliances and monitoring, and deliberate attacks by hackers. Although the data collected from the respondents was relatively consistent with very little variation, the frequencies of the threats and ranking may be different for other organizations. This is because agencies with strong ICT security policies, continuous awareness or education programs, sufficient ICT budget allocation, adherence to compliances and close monitoring may not have high frequencies in the categories of threats identified. A resilient, well maintained and monitored security system with continuous support from all interested parties will better prevent any undesired security breaches. In conclusion, this study has successfully identified major ICT security threats that frequently encountered by data centers in the Malaysian public sector. The outcome of the study will give a greater degree of awareness and understanding to the ICT security officers, who are entrusted with data center security. This will also enable them to optimize their limited resources, focus on the most frequent threats and implement the necessary controls to thwart the potential risks and curb damages to safeguard organization's reputation, customer confidence and image of the Malaysian public sector.

REFERENCES

[1] M. Lehto, "Cyber Security Education and Research in the Finland's Universities and Universities of Applied Sciences," *International Journal of Cyber Warfare and Terrorism*, vol. 6, no. 2, pp. 15-31, 2016.

[2] D. Bagay, "Information security of Internet things," *Procedia Computer Science*, vol. 169, pp. 179-182, 2020.

[3] R. Andrade and S. Yoo, "Cognitive security: A comprehensive study of cognitive science in cybersecurity," *Journal of Information Security and Applications*, vol. 48, pp. 102352, 2019.

[4] K. Knapp, *et al.*, "Key issues in data center security: An investigation of government audit reports," *Government Information Quarterly*, vol. 28, no. 4, pp. 533-541, 2011.

[5] F. Munodawafa and A. Awad, "Security risk assessment within hybrid data centers: A case study of delay sensitive applications," *Journal of Information Security and Applications*, vol. 43, pp. 61-72, 2018.

[6] A. de Gusmão, *et al.*, "Information security risk analysis model using fuzzy decision theory," *International Journal of Information Management*, vol. 36, no. 1, pp. 25-34, 2016.

[7] S. Snedaker and C. Rima, *Business continuity and disaster recovery planning for IT professionals*. Waltham, Mass: Elsevier, Syngress, 2014.

[8] M. Silva, *et al.*, "A multidimensional approach to information security risk management using FMEA and fuzzy theory," *International Journal of Information Management*, vol. 34, no. 6, pp. 733-740, 2014.

[9] A. Shameli-Sendi, *et al.*, "Taxonomy of information security risk assessment (ISRA)," *Computers & Security*, vol. 57, pp. 14-30, 2016.

[10] J. Srinivas, *et al.*, "Government regulations in cyber security: Framework, standards and recommendations," *Future Generation Computer Systems*, vol. 92, pp. 178-188, 2019.

[11] M. Burdon and L. Coles-Kemp, "The significance of securing as a critical component of information security: An Australian narrative," *Computers & Security*, vol. 87, pp. 101601, 2019.

[12] D. Mohamed, "Combating the threats of cybercrimes in Malaysia: The efforts, the cyberlaws and the traditional laws," *Computer Law & Security Review*, vol. 29, no. 1, pp. 66-76, 2013.

[13] D. Jack Stubbs, "Cyber attack sweeps globe, researchers see 'WannaCry' link," *U.K.*, 2020. [Online] Available: https://uk.reuters.com/article/uk-cyber-attack-idUKKBN19I1TF (accessed Sept. 20, 2020).

[14] Q. Tariq, "CyberSecurity Malaysia: Watch out for cyberattacks ahead of Malaysia Day," *The Star Online*, 2020. [Online] Available: https://www.thestar.com.my/tech/tech-news/2019/09/13/cybersecurity-malaysia-watch-out-for-cyberattacks-ahead-of-malaysia-day (accessed Sept. 20, 2020).

[15] J. Bhattacharjee, *et al.*, "A formal methodology for enterprise information security risk assessment," *in 2013 International Conference on Risks and Security of Internet and Systems (CRiSIS)*, 2013, pp. 1-9.

[16] P. Shamala, *et al.*, "A conceptual framework of info structure for information security risk assessment (ISRA)," *Journal of Information Security and Applications*, vol. 18, no. 1, pp. 45-52, 2013.

[17] J. Andress, *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Waltham, MA: Syngress, 2014.
[18] G.M. Heng. *Analyzing & Reviewing the Risks for Business Continuity Planning*. GMH Continuity Architects. Singapore: GMH Pte, 2008.
[19] ISO/IEC 27005:2018, *ISO*, 2020. [Online] Available: https://www.iso.org/standard/75281.html (accessed Sept. 20, 2020).
[20] J. Ryan, *et al.*, "Quantifying information security risks using expert judgment elicitation," *Computers & Operations Research*, vol. 39, no. 4, pp. 774-784, 2012.
[21] M. Jouini, *et al.*, "Classification of Security Threats in Information Systems," *Procedia Computer Science*, vol. 32, pp. 489-496, 2014.
[22] W. Kearney and H. Kruger, "Can perceptual differences account for enigmatic information security behaviour in an organisation?," *Computers & Security*, vol. 61, pp. 46-58, 2016.
[23] K. Roy Sarkar, "Assessing insider threats to information security using technical, behavioural and organisational measures," *Information Security Technical Report*, vol. 15, no. 3, pp. 112-133, 2010.
[24] M. Daghmehchi Firoozjaei, *et al.*, "Security challenges with network functions virtualization," *Future Generation Computer Systems*, vol. 67, pp. 315-324, 2017.
[25] L. Zhang, *et al.*, "Security threats and measures for the cyber-physical systems," *The Journal of China Universities of Posts and Telecommunications*, vol. 20, pp. 25-29, 2013.
[26] E. Szczepaniuk, *et al.*, "Information security assessment in public administration," *Computers & Security*, vol. 90, pp. 101709, 2020.
[27] P. Shamala, *et al.*, "Integrating information quality dimensions into information security risk management (ISRM)," *Journal of Information Security and Applications*, vol. 36, pp. 1-10, 2017.
[28] M. Jouini, *et al.*, "A Multidimensional Approach towards a Quantitative Assessment of Security Threats," *Procedia Computer Science*, vol. 52, pp. 507-514, 2015.
[29] 2014–15 Malaysia floods, *En.wikipedia.org*, 2020. [Online]. Available: https://en.wikipedia.org/wiki/2014–15_Malaysia_floods (accessed Sept. 20, 2020).

BIOGRAPHIES OF AUTHORS

Inthrani Shammugam received her B.Sc. (Computer Science) Degree from University of Science Malaysia and her M.Sc. (Information Technology) Degree in 2000 from University of New South Wales, Australia. She has vast experience in handling many government ICT projects and now is a ICT Consultant for Project Management at the Malaysian Administrative Modernisation and Management Planning Unit, Prime Minister Department. Her areas of expertise include Project Management, Informatin Security Risk Management, Disaster Recovery and Business Continuity Management. She is an active member in ISO/IEC JTC1 SC27 for working WG1 and WG5 since 2015. Email: inthra63@gmail.com

Ganthan Narayana Samy is currently a Senior Lecturer at the Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia (UTM). He received his Master degree in IT from University of Malaya, and a Master degree in Economics from National University of Malaysia. He obtained his Ph.D degree in Computer Science from UTM in 2012. Currently, he is the Head of MPROTEC Research Group. He has published more than 80 research papers with more than 40 research papers are indexed publication. His research interests include Information Security Risk Management, Healthcare Information System Security and Cloud Computing. He is also on the Scientific and Technical Committee & Editorial Review Board on Humanities and Social Sciences for World Academy of Science, Engineering and Technology (WASET), since 2018. Email: ganthan.kl@utm.my

Pritheega Magalingam received her B.Sc. (Computer) Degree in Software Engineering and M.Sc. (Information Security) Degree from UTM. She has completed her PhD at Royal Melbourne Institute of Technology, Australia in July 2015. She is now a senior lecturer at Razak Faculty of Technology and Informatics, UTM. Her area of expertise is Digital Forensics Analysis and Validation, Data Analytics, Information Security Risk Management and Applications of Complex Network Analysis. She became a member of the Information Theory Society and Computer Society, IEEE in 2016 and a member of the Information Systems Audit and Control Association**,** ISACA in 2017. Email: mpritheega.kl@utm.my

Nurazean Maarop is currently a Senior Lecturer with UTM. She received the BSc degree in Computer Science and MSc Computer Science UTM. She obtained the Ph.D degree from University of Wollongong, Australia. Apart from lecturing, she also contributed her service as Program Coordinator and Head of Research Group.She has published more than 130 research papers with more than 50 are indexed publication. Her research interests include Success Model of Information Systems, Diffusion and Adoption of Technology, Information Security Related Issues, Health Informatics, Government Informatics, Enterprise Architecture, and Digital Transformation. She is in the Editorial Board member of Open International Journal of Informatics, since 2018. Email: nurazean.kl@utm.my

Sundresan Perumal is a senior lecturer, computer forensic investigator, network security consultant and noted authority on electronic evidence. He provides industry-leading secure information services, computer forensic, incident response and technology consulting services to law firms, corporations and government agencies. He conducts computer forensic investigations and provides insightful solutions and acumen to solve a wide array of matters involving electronically stored information (ESI). He is currently heading the Innovation and Commercialization Unit in University Science Islam Malaysia. His research specialization is in Digital Forensic, Advanced Persistent Threat, Internet of Things Forensic, and Internet of Medical Things. Email: sundresan.p@usim.edu.my

Bharanidharan Shanmugam received his Ph.D from UTM in 2010 specialising cyber security. He is currently a Lecturer at Charles Darwin University and part of cyber research group. His current research interests include Intrusion Detection System, cyber security, IoT threats, Malware analysis and Cyber Risk Management. Dr. Bharani is also part of Australia Information Security Association Darwin chapter focusing on enriching cyber digital skills for next generation and elders. Email: bharanidharan.shanmugan@cdu.edu