Journal of ENVIRONMENTAL Treatment Techniques

J. Environ. Treat. Tech.
ISSN: 2309-1185

Journal web link: http://www.jett.dormaj.com

Physical Security Problems in Local Governments: A Survey

Poon Ai Phin*, Hafiza Abbas, Norshaliza Kamaruddin

Advanced Informatics Department, Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Jalan Sultan Yahya Petra, 54100, Kuala Lumpur, Malaysia
Corresponding author: aiphin@graduate.utm.my

Received: 26/10/2019 Accepted: 26/03/2020 Published: 20/05/2020

Abstract

Physical security refers to the control of access into organizations, buildings, rooms, and information technology (IT) peripherals. However, physical security may be overlooked by organizations because they are more concerned about information security; this is because the organization assumes that those granted access can be trusted. The physical security is not a new issue in a local government environment; however, in most cases, hackers are to blame, while the actual culprits may be the employee(s) of the local government itself. This paper is a survey done to investigate the problems faced by a local government and the measures needed to be taken to keep their physical access secure. The subject of the research is chosen from among municipal councils in Malaysia since they hold various private information about the residents of the area, where physical security awareness is still low among the members of the organization. As a case study, the Kota Bharu Municipal Council (KBMC) was selected and its security problems were identified through a research comprising a mixed method of quantitative (questionnaire and observation) and qualitative (interview) techniques. The respondents of the research were eight employees of the IT Department, while the solution to their security problems was derived through interviewing its IT Officer. The researchers also discuss if KBMC is able to apply other local government's solutions to their own security problems. The discussion reveals that the security awareness program is the most suitable solution to the KBMC's security problems since it enhances security awareness of top management officers and enables the employees to be aware of their responsibilities in their daily work routine.

Keywords: Physical security, Physical access, Local government, Security awareness, SETA, Sustainable security culture

1 Introduction

In information technology (IT), security refers to the safeguarding of digital information and IT assets against internal/external, malicious, and accidental threats (1). This includes detection, prevention, and taking actions against a threat with the use of security policies, software tools, and IT services. Security can be divided into physical security and information security, where physical security refers to the control of access into organizations, buildings, rooms, and IT peripherals, while information security controls access to computer networks, system files, and data (2). However, physical security is often overlooked because most organizations focus on information security (3) because the organization's main aim is to prevent outsider threat, but they neglect the issue of insider threat as the organization assumes that those granted access can be trusted (4). Physical security is not a new issue in a local government environment; however, in most cases, hackers are to blame, while the actual culprit is the employee of the local government itself.

2 Physical Security Problems in Local Governments

According to (5), local government refers to the authority that manages the administration of a town, city, country, and district in a state. Local government provides vital services for people and businesses in their authorized area; it normally provides services such as social care, schools, housing and planning, waste collection, licensing, business support, registrar services, and pest control (6). In (7), a survey was done on 109 local governments, which revealed that a local government typically faces six commonly occurring security threats (see Figure 1).

2.1 Physical Asset Loss

Physical loss is a risk to an organization's IT peripherals such as laptops, network devices, and servers. In government organizations, physical asset loss cases typically happen due to no proper storage for the assets, natural disasters, careless handling, or improper hardware maintenance. These cases can lead to data being lost permanently and this will also lead

Correspinding author: Poon Ai Phin, Advanced Informatics Department, Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Jalan Sultan Yahya Petra, 54100, Kuala Lumpur, Malaysia. E-mail: aiphin@graduate.utm.my.

to the public services disruption. In a survey (7), it was stated that 52% of respondents blame hackers as the biggest culprits while in reality, it is done by the regular users of the assets, who are the employees of the local government, which accounts for 44%, and only 4% is actually done by hackers. For example, (8) reported that the Bahamas Public Treasury's computer systems went offline when a water leak damaged the servers hosting an e-government service. Bahamas State Minister for Finance, Michael Halkitis, stated that the incident was due to the leakage on the third floor of the Treasury Building, which affected the second floor where the servers were situated. No online services were available for a few days, which severely impacted the daily operations of the Public Treasury.

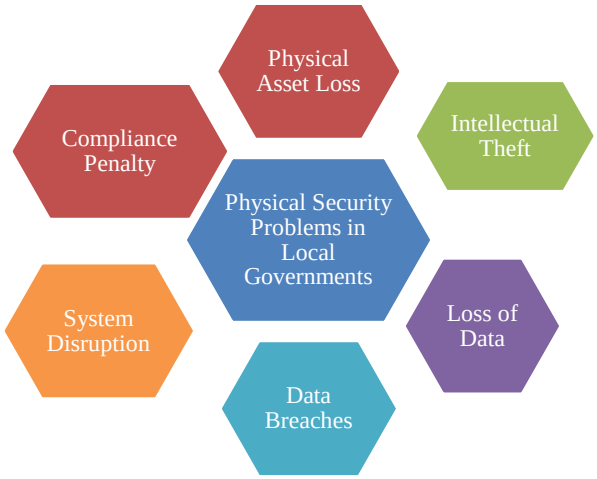

Figure 1: Types of Security Threats faced by a Local Government

2.2 Intellectual Theft

Intellectual theft refers to the act of stealing or using without permission another person's intellectual property such as trade secrets, software, contracts, grants, and agreements. Intellectual theft leads to reputation damage, loss of competitive advantage, and financial expenses. According to (7), malware is the cause of 43% of intellectual theft cases. As reported in a piece of news by the Guardian (9), ten Chinese nationals were charged by U.S. Justice Department for intellectual theft through phishing schemes, malware, and domain hijacking into a French aerospace company in 2015, which was developing engines with a U.S. company. It is also alleged that the same culprit hacked into other aerospace companies that are manufacturing the engine parts using Sakula malware in Massachusetts, Arizona, and Oregon. Later, it was revealed that the attack was actually done by two employees of Jiangsu Province Ministry of State Security (JSSD), six hackers, and two employees of the French aerospace company.

2.3 Loss of Data

Data loss is a situation where information is lost or damaged by failure to properly store, process, or transmit whether by intentionally erasing, session hijacking, malware, IoT exploits, human mistakes, or software failure. Data loss can lead to a service disruption for employees and the public, and local government may face lawsuits from citizens if sensitive data such as financial information is lost or falls into the wrong hands and are used for blackmail, phishing, or fraud. According to a survey (7), 53% of the data loss is due to human errors and is done by the local government's IT team members, and only 11% is done by hackers. In a report released by (10), a thief stole a computer belonging to the Department of Veterans Affairs (VA) in Maryland, United States, which contained unencrypted data of 26.5 million veterans and service personnel such as name, social security numbers, birth dates, and disability ratings. The case was reported, and the stolen computer was recovered later by the police. After forensic examination by FBI, it was reported that no data had been compromised. However, in 2009, VA was sued by five veterans on alleged invasion of privacy lawsuit and reached an agreement to pay them $20 million for identity theft risk.

2.4 Data Breaches

A data breach is a situation where data is copied, transmitted, viewed, stolen, or used by an unauthorized individual through phishing or human mistakes. It may occur due to lost devices or wrongly configured databases. A survey conducted by (7) reveals that 56% of the data breach cases are due to human mistakes, and only 39% are due to phishing. In a report, *A Breach of Trust*, it was revealed that 4,236 data breach cases occurred in the United Kingdom's Local Authorities between April 2011 and April 2014 (11) as compared to 1,035 data breaches between July 2008 and July 2011 (12). A Lewisham City Council's social worker who accidentally left a bundle of papers on the train, which contained data of 10 children and third-party information in relation to sex offenders, police reports, and child protection reports, decided to resign during the disciplinary procedures (11).

2.5 System Disruption

System disruption occurs when an IT system cannot execute any functions for a period due to either power failure, natural disasters, malicious attack by insiders or outsiders, or human mistakes. In a local government environment, unplanned downtime in their services will lead to the government officials' failure to schedule any appointments, manage citizen's complaints, or record their attendance using electronic records management (ERM) system in their daily routine. In (7), it was reported that 63% of system disruption cases in local governments are due to power failure, while only 28% are due to hackers' activities. In a piece of news published by SA News (13), it was reported that the power failure event at the State Information Technology Agency (SITA) severely affected the systems of a few government departments in South Africa, including the presidency was course by Tshwane power failure. After an investigation into the matter, it was later found out that the event occurred due to a failed backup generator in SITA. This incident caused all government operations, which used critical data such as birth, marriages, death, smart ID, and passport services, to get unavailable for a few days. As a result, SITA executives were blamed for their lack of disaster recovery procedures and backup plans. They apologized, but SITA reputation has since damaged.

2.6 Compliance Penalty

Government organizations need to comply with a few laws and regulations regarding physical security, such as the Federal Information Security Management Act (FISMA) (14), NIST 800-171 (15), Criminal Justice Information Services (CJIS) (16), the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (17), and General Data Protection Regulation (GDPR) (18). Violation in compliance with those standards such as FISMA can lead to a cutting back of funding from the federal government for local governments or even reputation damage. Failure to comply with those standards will lead to prosecution and fines (7). According to a report released by (19), the Alaska Department of Health and Social Services (DHSS) and the state's Medicaid agency both agreed to pay the Department of Health and Human Services (HHS) $1.7 million to settle HIPAA violations. Investigations revealed that the breach of data happened because a portable storage device with electronic personal health information (ePHI) of a MedicaID user was stolen from the vehicle of a DHSS employee. In the report, it was also stated that DHSS did not fulfil risk analysis requirements, and also it did not take into consideration the following: sufficient risk management measures, security training for its employees, properly management of devices, and media encryption.

3 Physical Security Solutions in Local Governments

In (20), Atlanta City Government was reported being attacked by an Iranian hacker group via SamSam's ransomware in March 2018, which led to their system disruption, where utilities and court services daily routine had to be done by filling in forms manually. $2.6 million government fund was later re-delegated to recover this incident, upgrade their IT infrastructures, and implement new government policies. The results of a survey conducted by (21) showed that 44% of local governments are regularly facing cyber-attacks incidents, while 41% are unaware of such attacks. In 50% of cases, the local governments, as admitted by themselves, cyber-attacks incidents are not counted or recorded. The survey concluded that local governments clearly need to improve their level of physical security to mitigate the threat of malicious hackers. The solutions taken by local governments are presented in Figure 2.

3.1 Outsourced IT Services

Outsource refers to a business practice that hires another company or individual to handle operations, perform task, or provide services previously done by the organization's own employees such as Information Technology services that involves programming, technical support, and software development, call service functions, manufacturing processes, customer service, human resources, and financial functions such as payroll and bookkeeping (22). An organization can outsource not only certain services, but also an entire department such as the IT department or a part of the department. The researchers in (23) stated that the new city of Sandy Springs, Georgia, has outsourced most of its core functions and programs, while only employing a few in-house employees as a strategy to lower the cost of employing workers with specialized skills and experiences needed. According to Deloitte's 2016 survey on outsourcing (22), 35% of the organizations surveyed stated that they are able to focus on innovation values with the outsourcing partnership.

Figure 2: Solutions by Local Governments to Security Threats

3.2 Developing Incident Response Plan

According to (24), Incident Response (IR) plan is a set of instructions aiming to give help to IT staff in responding, detecting, and recovering from network security incidents threatening daily work such as data loss, service outrage, and cybercrime. This plan is important for mitigating security risks and preparing the organization for a range of threatening events. In a survey done by (25) in 2016, it was revealed that only 33.7% of local governments in the United States had developed their own IR plan. In addition, a report released by (26) stated that the Nevada Local Government is the first local government that is leading in developing their own IR plan and using it in their communities by taking into consideration cybersecurity incidents and other hazards while making use of their existing exercise program.

3.3 Security Awareness Training

Security awareness program or Security Education Training and Awareness (SETA) programs refer to methods of educating the organization's employees about the danger of online scams and phishing (27). In (28), the authors argued that local governments are victims of cyberattacks and data breaches with 95% of the incidents occurred because of human error (29). Human error can be in the form of using default usernames and passwords, lost laptops or bring your own device (BYOD), wrong system configuration, poor management patches, and disclosure of employees' private information in social network sites (SNS). The local government of the City of Riverside, California, has made it a compulsory for its employees to take Securing the Human course from SANS Institute online

(29). Lea Deesing, the chief innovation officer of Riverside, believes that this training manages to change employee's behaviour because it does not focus on teaching and testing employee's knowledge on a set of rules (like the case in security training), but rather it focuses on changing human behaviour and making security as part of the workplace culture (29).

3.4 Standardized Policies and Guidelines

According to (30), a policy is a formal statement supported by the organization's senior management for repeated and common use in the organization, which includes rules and characteristics of the specific system or issue. Standard refers to mandatory actions or rules that support the policy, which is consensus organization-wide on which standard should be used. Guidelines, on the other hand, refer to recommendations or best practices employees can carry out when specific standards do not apply. The U.S. states and local governments need to comply with data breach notification laws, where government agencies have personal information of residents to notify them of any unauthorized access to their personal information (31).

3.5 Implementing Physical Security Controls

Physical security refers to the control of access into organizations, buildings, rooms, and IT peripherals (2) where they include gates and locks, guards, environment controls such as smoke detectors, fire alarms, and extinguishers, uninterrupted power supply, and protection from water damage (32). New York State Government, in their local government management guide, has listed out 12 top areas of concern in their IT security, including physical security where any unauthorized access activity identified by an intrusion detection system (IDS) is to be reviewed and any suspected violation must be investigated (32).

3.6 Restricted Access to Personally Identifiable Information

According to (33), personally identifiable information (PII) refers to employee's personal information such as social security number, name, birth records, biometric records, and information linked to the organization where they work. PII should be deleted when not needed for business purposes to avoid identity theft. Identity theft happens when a person's personal information is used by an unauthorized person to commit fraud (34). A local government may store not only the PII of its employees, but also that of the residents such as the resident's name, address, contact number, credit card information, and email address. Therefore, the only employee who is doing the processing of these data should be authorized to access sensitive data. The access is controlled by using role-based system when creating user accounts (35). National Institute of Standards and Technology (NIST), U.S., has developed guides for local governments to address this issue effectively (33).

4 Case Study

In Malaysia, the Ministry of Housing and Local Government (KPKT) and the Ministry of Federal Territories (KWP) are responsible for Malaysia's local governments (36), which comprise 12 city councils, 39 municipal councils, and 98 district councils (37). According to (37), the municipal council refers to a local authority in urban or town centre that has a population of over 150,000 residents and with annual revenue exceeding RM20 million. A municipal council holds various private information about the residents of the area. The authors in (38) stated that municipal council generates revenue from license payments, fines, and other fees for chargeable services, which consist of the residents' full names, identity numbers, home addresses, phone numbers, email addresses, and credit/debit card details. In general, the present research is done among municipal councils in Malaysia. Specifically, Kota Bharu Municipal Council Islamic City (KBMC) was chosen because it does not employ any physical access control provided by the Ministry of Housing and Local Government (39). Security problems faced by KBMC (see Figure 3) were derived through conducting a study using a mixed method of quantitative (questionnaire and observation) and qualitative (interview) techniques. The respondents were eight IT Department employees.

Figure 3: Security Problems in KBMC

4.1 Zero-security Awareness Knowledge

According to (40), security awareness refers to the process of training and educating employees of an organization regarding IT security. It comprises developing a program to educate employees, through which the employees are learning to be accountable for their work and actions, and steps are taken to determine the effectiveness of the organization's security measurements. As stated by the CIO of KBMC Mr. Khairulzani bin Said (through the interviews held), the only security awareness program carried out is the printing of posters about cybersecurity by IT Department's personnel and distributing them to every department to inform all employees about the security threats, but there is no an awareness campaign or training provided to the employees. After the distribution, there is no action taken to gather any feedback or receive inquiries from

the employees regarding the posters. Due to the lack of security awareness, a break-in case happened; two computers were stolen from the Building Control Department and a break-in attempt into the President's car was reported. The break-in cases were reported to the police, but the stolen computers have not been recovered until today. The two cases have negatively impacted the management of KBMC and the head of the IT Department.

4.2 Insufficient Fund

IT Department works under the Management Services Department, where they share the same resources and finance. Therefore, IT daily expenses are under the control of the Director of the Management Services Department. Most of the financial allocation is used to maintain the organization's daily expenditure such as paying employees' salary, utility bills, subscription fees, and wear and tear of the building expenses. As for IT peripherals or solutions, it is only approved when there is a leftover from the monthly expenses and no fund is allocated solely for IT expenses. As a result, spoilt smoke detector in IT Department is not repaired, fire extinguisher at IT Department's entrance only maintain till 2014, IT Department's door card access system is not working anymore and is replaced by key and lock, Closed-circuit televisions (CCTV) at the IT Department entrance and Finance Department are not working, and most of the desktop computers use by IT personnel have aged more than five years and can no longer accommodate the current technology workload.

4.3 No Support from Top Management

The top management of KBMC does not consider physical security as an important element because it does not generate any income for the organization. Assessment fees and license fees are the management utmost priority as allocation from KPKT is not enough to cover all KBMC daily operation expenses. Therefore, no financial support is allocated for any physical security in their yearly budget report. For that reason, any new purchases are only approved if there is any excess from the monthly operating expenses. This forces the IT Department to prioritize which asset to buy and any maintenance is not done inhouse to minimize the cost. Therefore, the spoilt smoke detector and door card access are not in their priority list as they focus on renovating the server which hosted KBMC portal and other online systems. To substitute the function of door card access, they use key and lock and rely solely on the two rotating enforcement officers. Since the smoke detector is not functioning, the IT Department is now a smoke-free office room.

4.4 IT Peripherals not Properly Monitored

IT asset in KBMC is solely under the authority of IT Department; thus, working asset is allocated at IT Department office room while the faulty asset is allocated at Technician room which is allocated on the ground floor waiting to be repaired. Every time an employee leaves the organization, their computer is passed over to the new employee without checking. If the computer is faulty, it is the responsibility of the new employee to inform the IT Department. The researcher observed that none of the previous employees' computers is formatted before passing over to the new employee. The computer stores the private information of the previous employee such as ID and Password of various systems used at KBMC, credit and debit card information, Facebook and Gmail access as it is set to be remembered by the computer. An IT officer, Mr. Sanusi Bin Mukhtar, said that the previous employee should make sure that any private information is deleted before passing over the computer to IT Department. However, this piece of knowledge is not distributed among employees of KBMC. The researcher also found that the computer store in the IT Department office room is not logged in detail for easy reference. It takes a few minutes to search for a particular computer as there are many computers scattered in the room, even with a serial code sticker pasted on the computer.

4.5 Visitors not Monitored in Shared Environment

KBMC is sharing the same compound with Exam Branch of Ministry of Education Kelantan and Accounting General Kelantan Branch (as shown in Figure 4). Visitors entering the compound are free to move around the compound. The map provided below shows that there are three entrances into the compound: main entrance which is guarded by two rotating enforcement officers, right-side pedestrian access that is not guarded by enforcement officer or CCTV, and left pedestrian access that is next to a housing area and guarded by a guard employed by Accounting General Kelantan Branch. At night, only the two enforcement rotating officers walk around the compound. Data gathered from interviewing eight IT Department employees revealed that there has been a break-in case at C Block of KBMC where two computers from the Building Control Department were stolen. It is suspected that the burglar came into the compound from the left pedestrian access that is shaded by two big trees. In addition, a break-in attempt has been reported into the President's car during the late evening, which was suspected done by a visitor entering the compound. In the cases mentioned above, none of the culprits was managed to be caught by any of the rotating enforcement officers from the guardhouse.

4.6 Minimum Access Control

KBMC secure their building with minimum access control; they solely rely upon only two rotating enforcement officers at the guardhouse. There is neither CCTV nor smoke detector, and lights are off at night in all office rooms and corridors. Only a few lights are on at the main parking area, while right and left pedestrian entrances are locked after 5 pm. The grills at four staircases and entrance to payment and services counter are also locked after 5 pm. There is not grill on any windows of the building, and all windows can be opened. All windows view is blocked from outside view with cabinets and shelves in the office room to make room for crowded officer desk. The entrance to all office rooms is locked with key and lock and the key is stored at the guardhouse. The last person leaving the office room is responsible to send the door key to the guardhouse.

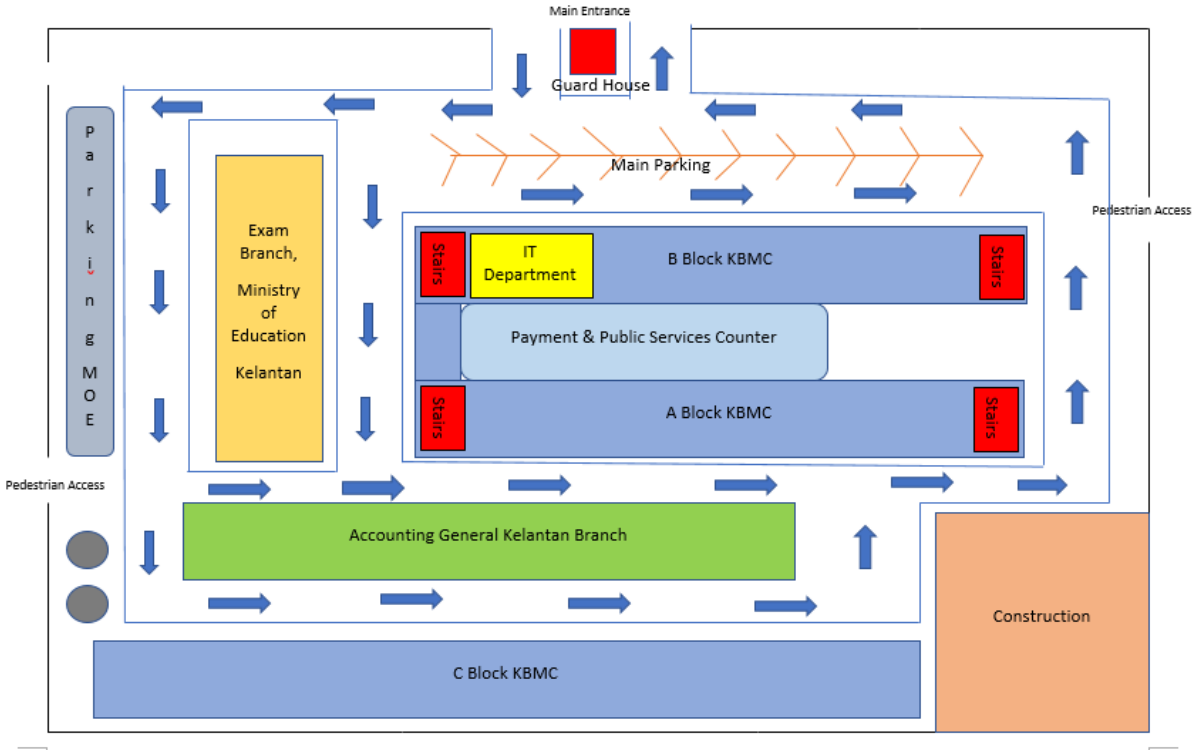

Figure 4: KBMC Compound

The researcher observed that once a visitor manages to access the compound, they can access into KBMC building through payment and public services counter, the back entrance of KBMC building, and the four staircases to the upper floor of the building. There is a grill on each of the staircases, but it is open during office hours. At the payment and services counter, there is an enforcement lady officer monitoring the queue number at payment, but her desk is facing the counter, not the entrance; thus, visitors entering are not monitored. There is also no CCTV available inside the payment and public services counter; therefore, any visitor entering the counter can also enter other departments such as Finance Department. The entrance to the four staircases is blocked from the main road and there is no light in the corridor during the night. The light is also off in all office rooms at night. During office hours, any visitor who manages to enter the compound can go up to the roof of the building without being monitored from the four staircases. The visitor entering the office room cannot be monitored because the wooden cabinets and shelves are blocking the windows view. However, data gathered from interviews revealed that there has not been any fire broke out in the building nor any terrorist entering the building till now.

5 Discussion

This section discusses if KBMC is able to adapt the solutions used by other local governments to solve their security problems. The discussion will take into consideration findings from surveys, observations, and interviews held with eight employees of the IT Department. Findings revealed that insufficient fund is the main reason due to which the KBMC authorities cannot solve their security problems. Without sufficient funding, the IT Department cannot afford to outsource their IT services to other companies and implement physical security controls such as smoke detector, card access door system, CCTV, and fire extinguisher. Therefore, KBMC is left with solutions that do not require any extra funding such as development of incident response plans, security awareness training, providing standardized policies and guidelines, and restricting access to PII. However, from observation, the top management of KBMC is not supportive of physical security as it does not bring any profit to the organization. Therefore, there is no instruction to the IT Department to develop any incident response plan or develop any standardized policies and guidelines. Top management and employees of KBMC have zero security awareness and knowledge since any training regarding the security awareness and restricted access to PII has not been provided for them.

The discussion concludes that security awareness training is the most suitable solution to KBMC's security problems. Awareness training is needed to be given to top management and all employees of KBMC so that the top management can understand the importance of physical security and the employees know their responsibility towards their daily work routine and ways to prevent a cyberattack incident occurrence.

As mentioned earlier, KBMC has insufficient funds for security solutions; and interviews and observations revealed that they have an insufficient number of IT staff to carry out security awareness programs. The available eight IT staffs in the IT Department need to take care of IT-related matters of all the employees in their daily work routine. Therefore, the researcher proposes KBMC to use a free security training

that is available free online and easy to use such as Wizer (41). This online solution comprises mobile and desktop applications, short training videos, a learning management system, and progress reporting of each employee. This security program is crucial to maintain a sustainable security culture among the employees of the organization as this one-time event will transform into a lifecycle that will generate security awareness for a long time with the primary goal of fostering change for a better security environment (42).

6 Conclusion

Considering the findings, we can conclude that not all organizations, especially government-connected ones, manage to deal with IT risks effectively. Hackers are commonly accused as culprits, while research shows that in many cases, the actual culprits are the employees of the organization itself. The topmost courses of data breaches are due to human error, poor employee training programs or employees who are not aware of their responsibility, and the lack of physical security awareness. Data protection training is not compulsory in the municipal councils (7); however, the researcher strongly feels that this should be a compulsory course for the employees handling personal information in an organization. In addition, the Ministry of Housing and Local Government of Malaysia should enforce a rule asking all local governments to develop their own physical security policies or employ physical security from the ministry.

Ethical issue

Authors are aware of and comply with, best practices in publication ethics specifically with regard to authorship (avoidance of guest authorship), dual submission, manipulation of figures, competing interests and compliance with policies on research ethics. Authors adhere to publication requirements that the submitted work is original and has not been published elsewhere in any language.

Competing interests

The authors declare that there is no conflict of interest that would prejudice the impartiality of this scientific work.

Authors' contribution

All authors of this study have a complete contribution to data collection, data analyses, and manuscript writing.

References

1. Rouse M. Security [Internet]. TechTarget. [cited 2019 Sep 27]. Available from: https://searchsecurity.techtarget.com/definition/security.
2. kisi. Understanding Access Control Systems [Internet]. kisi. [cited 2019 Sep 27]. Available from: https://www.getkisi.com/access-control
3. Hutter D. Physical Security and Why It Is Important [Internet]. 2019 [cited 2019 Sep 14]. Available from: https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120.
4. Harris S. All in one CISSP Exam Guide [Internet]. 6th Editio. Polisetty Veera Subrahmanya Kumar, editor. New York: McGraw Hill; 2013. 1472 p. Available from: https://eduarmandov.files.wordpress.com/2017/05/security-cissp-all-in-one-exam-guide-6th-edition.pdf.
5. Britannica. Local Government [Internet]. Encyclopaedia Britannica. [cited 2019 Sep 28]. Available from: https://www.britannica.com/topic/local-government.
6. Local Government Association. What is local government? [Internet]. Local Government Association. [cited 2019 Sep 28]. Available from: https://www.local.gov.uk/about/what-local-government.
7. Brooks R. IT Risks in Government Sector [Internet]. netwrix. 2018 [cited 2019 Sep 28]. Available from: https://blog.netwrix.com/2018/12/19/infographics-it-risks-in-government-sector-regular-users-pose-a-bigger-threat-to-data-than-hackers.
8. Turnquest A. E-government system down after leak [Internet]. The Tribune. 2012 [cited 2019 Sep 28]. Available from: http://www.tribune242.com/news/2012/aug/01/e-government-system-down-after-leak.
9. The Guardian. Chinese spies charged in US with trying to steal jet engine secrets [Internet]. The Guardian. 2018 [cited 2019 Sep 28]. Available from: https://www.theguardian.com/us-news/2018/oct/31/chinese-spies-charged-in-us-with-trying-to-steal-jet-engine-secrets.
10. IDWISE. The Veterans Affairs Data Breach of 2006 [Internet]. IDWISE. 2006 [cited 2019 Sep 28]. Available from: https://identity.utexas.edu/veterans-and-active-service-personnel/the-veterans-affairs-data-breach-of-2006.
11. Big Brother Watch. A Breach of Trust [Internet]. 2015 [cited 2019 Jun 6]. Available from: https://www.bigbrotherwatch.org.uk/wp-content/uploads/2015/08/A-Breach-of-Trust.pdf.
12. Big Brother Watch. Local Authority Data Loss [Internet]. 2011 [cited 2019 Jun 6]. Available from: https://www.bigbrotherwatch.org.uk/la-data-loss.pdf.
13. SA News. Home Affairs back online following SITA power outage [Internet]. South African Government News Agency. 2018 [cited 2019 Sep 28]. Available from: https://www.sanews.gov.za/south-africa/home-affairs-back-online-following-sita-power-outage.
14. U.S. Department of Commerce. NIST. Federal Information Security Management Act (FISMA) Implementation Project [Internet]. National Institute of Standards and Technology. 2014 [cited 2019 Sep 28]. Available from: http://csrc.nist.gov/groups/SMA/fisma/index.html.
15. Ross R, Viscuso P, Guissanie G, Dempsey K, Riddle M. Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. NIST Spec Publ 800-171 [Internet]. 2014 [cited 2019 Sep 28];1–34. Available from: http://dx.doi.org/10.6028/NIST.SP.800-171.
16. U.S. Department of Justice. Criminal Justice Information Services (CJIS) Security Policy [Internet]. CJIS Advisory Policy Board. 2019 [cited 2019 Sep 28]. Available from: https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center.
17. Office for Civil Rights. Summary of the HIPAA Security Rule [Internet]. Office for Civil Rights. 2013 [cited 2019 Sep 28]. Available from: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.
18. Wolford B. What is GDPR, the EU's new data protection law? [Internet]. GDPR.EU. [cited 2019 Sep 28]. Available from: https://gdpr.eu/what-is-gdpr.
19. Becker's Health IT & CIO Report. Alaska Medicaid Settles HIPAA Security Case for $1.7M [Internet]. Becker's Health IT & CIO Report. 2012 [cited 2019 Sep 28]. Available from: https://www.beckershospitalreview.com/healthcare-information-technology/alaska-medicaid-settles-hipaa-security-case-for-17m.html.
20. Lasky S. The Ransomware Scourge That Threaten Today's City Governments [Internet]. Security Iinforwatch.com. 2019 [cited 2019 Oct 28]. Available from:

https://www.securityinfowatch.com/cybersecurity/information-security/anti-virus-and-malware-defense/article/21089478/the-ransomware-scourge-that-threaten-todays-city-governments.
21. ICMA. Cybersecurity: Protecting Local Government Digital Resources [Internet]. ICMA. Washington; 2017 [cited 2019 Oct 28]. p. 64. Available from: https://icma.org/sites/default/files/18-038 Cybersecurity-Report-hyperlinks-small-101617.pdf.
22. Rouse M. What is outsourcing? - Definition from WhatIs.com [Internet]. TechTarget. 2018 [cited 2019 Oct 22]. Available from: https://searchcio.techtarget.com/definition/outsourcing.
23. Bradbury MD, Waechter GD. Extreme outsourcing in local government: At the top and all but the top. Rev Public Pers Adm. 2009 Sep;29(3):230–48.
24. Cisco. What Is an Incident Response Plan for IT? [Internet]. [cited 2019 Oct 25]. Available from: https://www.cisco.com/c/en/us/products/security/incident-response-plan.html.
25. ICMA. Cybersecurity 2016 Survey [Internet]. ICMA. 2016 [cited 2019 Oct 25]. Available from: https://icma.org/sites/default/files/309075_2016 cybersecurity survey_summary report_final.pdf.
26. Ewing S. Nevada Leads by Example in State and Local Government Cyber Security Practices - Security Boulevard [Internet]. Security Boulevard. 2019 [cited 2019 Oct 25]. Available from: https://securityboulevard.com/2019/03/nevada-leads-by-example-in-state-and-local-government-cyber-security-practices.
27. Moramarco S. 7 Benefits of Security Awareness Training [Updated 2019] [Internet]. Inforsec. 2019 [cited 2019 Oct 28]. Available from: https://resources.infosecinstitute.com/7-benefits-of-security-awareness-training.
28. Alvarez M. The changing face of IT security in the government sector [Internet]. IBM Security. 2016 [cited 2019 Oct 28]. Available from: https://www.ibm.com/downloads/cas/YQZM86DB.
29. Newcombe T. Can Security Awareness Training Change Behavior and Reduce Risk? Govenment Technology [Internet]. 2016 [cited 2019 Oct 28]; Available from: https://www.govtech.com/security/Can-Security-Awareness-Training-Change-Behavior-and-Reduce-Risk.html.
30. Spoden C. Differentiating Between Policies, Standards, Procedures, and Guidelines [Internet]. FRSecure. 2017 [cited 2019 Oct 30]. Available from: https://frsecure.com/blog/differentiating-between-policies-standards-procedures-and-guidelines.
31. Greenberg P. Security Breach Notification Laws [Internet]. National Conference of State Legislatures. 2018 [cited 2019 Oct 30]. Available from: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
32. DiNapoli TP. Local Government Management Guide: Information Technology Governance. New York; 2019.
33. McCallister E, Grance T, Kent K. Guide to protecting the confidentiality of personally identifiable information (PII). Spec Publ 800-122 Guid. 2010;1–59.
34. USA.gov. Identity Theft [Internet]. USA.gov. 2019 [cited 2019 Oct 31]. Available from: https://www.usa.gov/Identity-theft#item-206115.
35. Infosec. Security Awareness Checklist for Local Government [Internet]. Infosec. 2018 [cited 2019 Oct 31]. Available from: https://resources.infosecinstitute.com/security-awareness-checklist-for-local-government.
36. Commonwealth Local Government Forum. The Local Government System in Malaysia [Internet]. 2018 [cited 2019 Sep 24]. Available from: www.clgf.org.uk/malaysia.
37. Jabatan Kerajaan Malaysia. General Questions [Internet]. [cited 2019 Sep 24]. Available from: http://jkt.kpkt.gov.my/en/SoalanLazim/Umum-JKT%26PBT.
38. Commonwealth Local Government Forum. Malaysia [Internet]. 2018 [cited 2019 Sep 28]. Available from: www.clgf.org.uk/malaysia.
39. Bahagian Khidmat Pengurusan K. Garis Panduan Keselamatan Fizikal Kementerian Perumahan dan Kerajaan Tempatan (KPKT) [Internet]. Putrajaya; [cited 2019 Mar 28]. Available from: http://www.kpkt.gov.my/resources/index/user_1/MENGENAI KPKT/GARIS PANDUAN/GP_KESELAMATAN_FIZIKAL_KPKT.pdf.
40. Fahey R. Security Awareness -- Definition, History, and Types [Internet]. Infosec. [cited 2019 Sep 28]. Available from: https://resources.infosecinstitute.com/category/enterprise/securityawareness.
41. Friedlander G. No Money? Free Security Training for Government [Internet]. Wizer. 2019 [cited 2019 Nov 7]. Available from: https://security-awareness-training-program.com/index.php/2019/04/28/no-money-free-security-training-for-government.
42. Romeo C. 6 ways to develop a security culture in your organization [Internet]. TechBeacon. [cited 2019 Nov 7]. Available from: https://techbeacon.com/security/6-ways-develop-security-culture-top-bottom.

Author Profile:

Poon Ai Phin is a student in Universiti Technology Malaysia doing her master's degree in Information Assurance.

Dr. Hafiza binti Abas is a senior lecturer in Universiti Teknologi Malaysia specialize in Augmented Reality, Multimedia, Special Needs, Physical Security, Education Technology.

Dr. Norshaliza Binti Kamaruddin is a senior lecturer in Universiti Teknologi Malaysia specialise in Image Processing and Computer Vision.