Customer data security and theft: a Malaysian organization's experience

Mohd Aizuddin Zainal Abidin and Anuar Nawawi
Faculty of Accountancy, Universiti Teknologi MARA, Shah Alam, Selangor, Malaysia, and
Ahmad Saiful Azlin Puteh Salin
Faculty of Accountancy, Universiti Teknologi MARA, Perak, Malaysia

Received 7 April 2018
Revised 29 June 2018
Accepted 30 June 2018

Abstract

Purpose – This study aims to identify weaknesses in current internal control systems in protecting customer data and the drivers that motivate employees to steal customer data and the impact of customer data theft on the organization.

Design/methodology/approach – A case study approach was taken to investigate and analyze internal control system weaknesses. One organization that involved investor and treasury services was selected as a case study in this research. A mixed method of data collection, specifically survey questionnaires and observations, was used.

Findings – This study revealed that employees are aware of the policy to protect customer data in their organization. Ironically, customer data theft still occurred despite the company having an internal control system. The main concern was the attitude of the employees to adhere to the policies in place, which becomes the major cause of internal control violation. Employees tend to ignore policies and standard operating procedures, providing opportunities for data theft and fraud to occur, although they realize this will result in a severe impact on the reputation of a company.

Research limitations/implications – The results provide further confirmation of the fraud triangle theory, i.e. opportunity on the possible causes of the data theft and fraud, supporting prior empirical research and surveys conducted by researchers and global professional firms on fraud. This study, however, was conducted on only one organization with limited participation from employees because of the sensitivity of the nature of the topic.

Practical implications – This study provided recommendations that can be a reference for companies and regulatory bodies in preventing customer data theft cases, such as regular training and awareness campaigns to the staff, stringent recruitment policies, close monitoring on the accessibility of customer data and continuous use of advanced technology to prevent a data breach.

Originality/value – This study is original, as it focuses on an organization that operates in the financial services industry, which is one of the most attacked sectors for data theft and cybercrime activity globally. Furthermore, this kind of research is rare in fraud literature, particularly in developing markets such as Malaysia. The findings of this study are inferred from the direct observation of the organizational and employee work environments, activities and behaviors, which are private and confidential and difficult to access by researchers for publication in academic journals.

Keywords Malaysia, Internal control, Customer information

Paper type Case study

Introduction

Over the past few years, companies in every industry sector around the globe have seen their sensitive internal data lost, stolen or leaked to the outside world. For example, British Airways frequent flyers accounts were hacked, while names, addresses, home

Information & Computer Security
Vol. 27 No. 1, 2019
pp. 81-100

2056-4961
DOI 10.1108/ICS-04-2018-0043

numbers and emails were taken by cyber attackers of JPMorgan Chase. Other data breaches have included Anthem, Target, Home Depot, eBay and LinkedIn.

A wide range of high-profile data loss incidents has cost organizations millions of dollars in direct and indirect costs (Blasco *et al.*, 2015) and resulted in tremendous damage to performance (Martin *et al.*, 2016), brands and reputations. Hinz *et al.* (2015) revealed that the announcement of data theft by an organization directly affects its share price. Examples of data loss incidents include hacking, a clone of debit and credit card, the sale of customer account details to external parties, the loss of laptops, USB sticks, backup tapes and mobile devices. The vast majority of these incidents resulted from the actions of internal users and trusted third parties, and most have been unintentional. As the financial services industry is responsible for preventing its customers' data from loss or theft, getting data protection wrong can introduce commercial, reputation, regulatory and legal penalties. This becomes more difficult as the criminal sees the high value of personal information for identity theft, fraud and espionage (Allison *et al.*, 2005; Furnell, 2002; Newman and Clarke, 2003; Wall, 2007; Holt and Lampke, 2010; Holt *et al.*, 2016), which motivates them to steal data from individuals and the organization.

According to a report from the Financial Crime and Intelligence Division of the UK, many firms are failing to identify all aspects of the data security risk they face for three main reasons. First, some do not appreciate the gravity of this risk; second, some do not have the expertise to make a reasonable assessment of key risk factors and devise ways of mitigating them; and third, many fail to devote or coordinate adequate resources to address this risk (Financial Crime and Intelligence Division, 2008). In addition, while large- and medium-sized firms generally devote adequate resources to data security risk management, there is a lack of coordination among relevant business areas such as information technology, information security, human resources and physical security. There is too much focus on information and communication technologies (ICTs) controls and too little on office procedures, monitoring and due diligence. Failure to manage this risk will negatively impact firms' normal situations that result in unwanted consequences (Amirudin *et al.*, 2017).

According to the report from Ernst and Young (2011), about 2,000 customer records from a national retail bank were stolen by employees prior to leaving and joining a competitor firm. The records included customer bank account numbers, social security numbers and other highly sensitive personal data such as tax returns and pay statements. This is consistent with Hassan *et al.* (2016) and Saibon *et al.* (2016) who revealed that security of information is one of the obstacles for the taxpayer to comply with the technology-based tax submission.

This situation also occurs in Malaysia. Based on a survey conducted by PricewaterhouseCoopers Malaysia, 42 per cent of Malaysian organizations see an increased risk of cyber threats (PricewaterhouseCoopers Malaysia, 2016). This is because, as a developing country, Malaysia has started on its journey to become a developed nation by increasing the usage of computer technology and Internet penetration. Unfortunately, this progress will incidentally increase opportunities for electronic theft (Holt, 2007; Holt and Graves, 2007; Newman and Clarke, 2003; Taylor *et al.*, 2006; Wall, 2007) and organized crime (Grabosky, 2007). Sen and Borle (2015), for example, found that investment in information technology security corresponds to a higher risk of data breach incidents due to wrong decisions in information technology security investments. This worsens when the cost to install the security features requires a huge capital investment. This is supported by Das and Khan (2016), who found that cost is one of the obstacles for smartphone users to adopt security

software that can protect them from the targeted information theft. The Computer Security Institute (2007) reported that businesses in the USA lost millions of dollars due to the theft of confidential data. For identity theft, approximately eight million people were victimized by identity thieves and these victims lost nearly $16bn (Synovate, 2003).

Because of that, this study is significant in understanding the current issues of customer data theft in the Malaysian context. One organization, Bank ABC Services, has been selected as a case study for this research. This company is selected because, based on the survey conducted by the PricewaterhouseCoopers, the financial services industry remains one of the most attacked sectors for cybercrime activity (PricewaterhouseCoopers Malaysia, 2016). In addition, as a part of allowing the research to be conducted in their premise and providing access to certain confidential information, this organization is of interest for the research because there was an issue of customer data protection currently under discussion in the organization, justifying its selection. Based on an informal discussion with a few employees, it was found that this organization was experiencing problems in its operation and administration. For example, employees have opportunities to grab customer information, as there is no proper supervision to prevent the possibility of that information leaking to an outsider or a competitor. Threats of data loss from internal users have always been a risk in financial institutions due to the capabilities and opportunities that arise around them. Sekaran and Bougie (2013) also emphasized that picking the right case for the study is crucial for a successful case study research. Thus, selecting this organization has met the criteria and objectives of this study.

This study serves several purposes. The first is to examine the weaknesses in the current internal control system of ABC Bank Services in protecting its customer data. The second is to identify the factors that might motivate an employee of ABC Bank to steal customer data. Finally, this study will determine the impact of customer data theft on ABC Bank Services as a whole. Specifically, this study intends to answer the following research questions:

RQ1. How effective are the internal control systems in protecting the customer data?

RQ2. What are the factors that motivate employees to commit data fraud?

RQ3. What are the impacts of customer data theft toward the organization?

This study will contribute to the research in several ways. First, it will provide significant findings on customer data theft practices and its related preventive program practices by companies in Malaysia. Second, this study can be a reference for Malaysian companies and regulatory bodies such as the Central Bank of Malaysia, Securities Commission of Malaysia and Malaysian Personal Data Protection Department in improving policy and strengthening the current enforcement of rules and regulations. Last, this study can add to the theoretical framework and body of literature on data protection and customer data theft in emerging and developing countries, which are currently scarce in the literature. Prior studies have concentrated more on situations in developed countries such as the USA, UK and Continental Europe.

This paper is organized as follows: Section 2 is the literature review, followed by the research methodology in Section 3. Section 4 contains findings and discussion, while Section 5 is the conclusion. Section 6 contains research limitations and suggestions for future research.

Literature review

Data protection in Malaysia

Countries in the European Union are subjected to the Data Protection Directive (95/46/EC), but in the USA, no comprehensive data protection legislation has been established. Malaysia has its own version of regulations to protect data and information of an individual person, called the Personal Data Protection Act 2010 (PDPA). This Act, also known as Act 709, applies to any person who processes and has control and power over personal data processing in relation to commercial transactions in Malaysia. Contravention of this Act will be subject to a fine of not exceeding RM 300,000 or imprisonment not exceeding two years or both. This Act outlines a few important principles as follows.

General principle: The organization cannot use personal data unless consent is given by the individual in question. If processed, it must be lawful, have a direct purpose with the individual and be adequate and not excessive for the specific purpose.

Notice and choice principle: Organizations must inform the individual in writing that his/her data are being processed, a description of the data that are being processed and the purpose of the process. The individual has a right to correct wrong data and choose to limit the data only to the persons or organization specified by the individual.

Disclosure principle: The organization must seek consent from the individual whether he/she allows his/her data to be disclosed or not disclosed to the third party

Security principle: The organization must take sufficient steps in protecting personal data from loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction. This includes any effort and sufficient security measures related to the place or location where the data are stored, equipment used to store the data, person or staff that have access to the data and situations in which the data are being transferred. The same principle is also applicable if the organization outsources this data processing process to another entity.

Retention principle: The organization cannot keep personal data longer than necessary for the fulfillment of the specific purpose. The data must be deleted and destroyed if no longer required.

Data integrity principle: The data used by the organization must be accurate, complete, not misleading and up-to-date.

Access principle: Individuals must be granted access to modify his/her data if the data are found to be incomplete, inaccurate, misleading and/or out-of-date.

Financial institutions are also subject to the guidelines on data management and management information system (MIS) framework issued by the Central Bank of Malaysia. This guideline requires financial institutions to establish and maintain a sound data management and MIS, create a corporate culture that reinforces the importance of data integrity and data quality and maintain effective controls over data security and privacy. The responsibility to ensure that these requirements are fulfilled is on the shoulders of the senior management, with appropriate oversight by the board of directors of the respective financial institutions.

Prior study on customer data theft

Customer data theft can occur in various ways. One is by computer hackers that steal data online. The computer hackers are expert in using a computer and related technology, e.g. internet and software (Holt, 2007; Holt and Bossler, 2008). For example, in a shared website hosting environment, if the attacker is able to compromise the targeted website, the other website that also used the same server is also vulnerable to data theft (Tran *et al.*, 2016). It

also can be done manually (easy) such as stealing personal information from mailboxes or during a robbery (Allison *et al.*, 2005; Copes and Vieraitis, 2009; Gordon *et al.*, 2007; Morris, 2010). These hackers or cyber attackers are usually motivated by financial and economic drivers (Furnell, 2002; Gordon, 2000; Gordon and Ma, 2003; James, 2005; Hutchings and Holt, 2016).

Data stealing is one of the four categories of cybercrime typology proposed by Wall (2001), i.e. cyber-deception/theft. Three other categories are cyber-trespass, cyber-porn and obscenity and cyber-violence. Cyber-deception and theft include the use of the Internet to steal information or illegally acquire items of value, whether from individuals or corporations (Holt and Bossler, 2014). This is made possible when fraudsters adopt various fraud scheme environments, most notably email from Nigeria and work at home schemes (Grabosky *et al.*, 2001; Holt and Graves, 2007; King and Thomas, 2009; Newman and Clarke, 2003).

To combat data theft, various efforts are taken. The easiest is by using protective software that consists of antivirus, ad-aware and spyware programs. This software is created to identify and prevent malicious software from copying sensitive personal information from individual computer systems (Bossler and Holt, 2009; Choi, 2008; Taylor *et al.*, 2014).

Firewalls are also quite popular to help a company avoid data theft. They can be used by two means (Nazario, 2004; Szor, 2005). First, hardware firewalls, which are installed in router technology and e-mail servers to defend computer systems attached to a network, thus decreasing the likelihood of attackers penetrating a network to compromise individual computers. Second, software firewalls, which operate on individual computer systems and provide immediate alerts to possible compromising traffic and malicious attackers (Holt and Turner, 2012).

Arguably, the individual alone is the best defense to protect against being cheated and prevent an identity from being stolen. This can be done if the person has good knowledge of the various internet crimes and takes proactive measures against being trapped in this cybercrime (Bossler and Holt, 2009; Choi, 2008; Grabosky and Smith, 2001; Wall, 2007). Holtfreter *et al.* (2015), for example, found that individuals with less self-control have a higher tendency to make transactions from unknown emails, which increases the probability to fall into an identity-theft scheme.

Knowledge of computer technology and operating systems also will reduce the possibility of becoming a victim because users can identify what is the correct anti-virus program to be used and quickly detect errors and malfunctions caused by the malware (Szor, 2005; Choi, 2008; Furnell, 2002; Holt and Bossler, 2008). With knowledge, the person will also limit himself/herself from interacting with strangers who possibly exposed themselves to the unintended consequences (Choi, 2008; Holt and Bossler, 2008). In addition, that person will not open unknown spam or suspect email that contains attachments and information that is "too good to be true" (Szor, 2005; Taylor *et al.*, 2010). Finally, the person also will not hesitate from using complex passwords and not be lazy to change them regularly to avoid the password being easily predicted (Furnell, 2002; Nazario, 2004; Taylor *et al.*, 2010).

Theoretical framework.

Fraud triangle theory. The phenomenon of a customer data theft can be explained by using the fraud triangle theory introduced by Cressey (1973). According to this theory, fraud is caused by pressure, opportunities and rationalizations. Pressure can take on many forms, e.g. employment and financial pressure. For example, Ermongkonchai (2010) found that

financial gains are the main reasons for employee malpractice in an organization, thus indicating financial pressure. Schuchter and Levi (2016) found that difficult and unrealistic key performance expectations are the kind of pressure experienced by most fraudsters in Switzerland and Austria, thus indicating employment pressure.

The opportunity to commit fraud is frequently associated with weak governance, poor internal controls and accountability (Karim *et al.*, 2018; Nawawi and Salin, 2018; Shariman *et al.*, 2017; Rahim *et al.*, 2017; Omar *et al.*, 2016; Zakaria *et al.*, 2016; Suhaimi *et al.*, 2017; Husnin *et al.*, 2013). For example, unavailability of clear standard operating procedures permits the fraudster to manipulate financial transactions, thus stealing a company's assets. The final causes, rationalization, relate to the justification by the fraudster to legalize his/her action. For example, a clerk may use a company's assets for personal use if he/she observes other people also doing the same, but no disciplinary action is taken. Deng *et al.* (2014), for example, found that construction workers in China rationalize their action when other people also behave dishonestly. Thus, they choose to be indifferent with others.

Description of the case study

ABC Bank Services is an international investor and treasury services company that offers global custody services, including safekeeping, settlement, corporate actions, income collection, proxy voting, tax services and entitlement processing. This company aims to deliver custodial, advisory and financing and other services to safeguard assets, maximize liquidity and properly managing risk of their client. In 2015, the company has more than US $3tn worth of assets under its administration. The company established and provides services in more than 15 locations across continents, e.g. in America, Europe and the Asia Pacific, including Malaysia. The clients of ABC Bank Services consist of international financial institutions such as Hong Kong Shanghai Bank (HSBC), Julius Bar, Vontobel, Robeco, Deutsche Bank, Mediolanum, Morgan Stanley and American Express. The wide range of highly reputable clients shows that protecting customer data is one of the utmost key elements in the ABC Bank Services process.

Customer data protection in ABC Bank Services. ABC Bank Services has adopted a privacy policy (the "policy") outlining the minimum standards required to protect confidential information, personal information and sensitive information. Confidential information is the information that is protected by confidentiality provisions in the client's agreement or by Bank Secrecy Laws of certain jurisdictions. Confidential information may include personal information of the institutional clients of ABC Bank Services. Personal information is the information that is related to an identified or identifiable individual. Sensitive information relates to racial or ethnic origin, political opinions and membership, religious belief, profession or trade association, sexual preference, criminal records or health information.

This policy incorporates internationally recognized privacy principles defined by the Organization for Economic and Cooperative Development (OECD) via guidelines for the protection of privacy and trans-border flow of personal information. These principles form the foundation for which country-specific legislation has been based, including in Luxembourg, Canada and the UK. This policy is intended to govern ABC Bank Service's actions as they relate to the collection, use and disclosure of identifiable individuals' confidential information, personal information and sensitive information held by ABC Bank Services in any business, operational and functional unit in any jurisdiction. This policy sets out minimum standards applicable to all ABC Bank Services companies, subsidiaries and employees. In addition, ABC Bank Services companies and subsidiaries should follow any

local legal, regulatory and/or policy requirements with respect to the protection of privacy if it is more stringent than this policy.

The policy is also applied to the collection, use and disclosure of information held by ABC Bank Services on the identifiable individuals and clients, including the disclosure of such information between ABC Bank Services and to the third-party service suppliers. The policy applies regardless of the format in which the confidential information, personal information or sensitive information was collected or held or when it was collected.

Privacy incidents reporting on abuse of clients' data. Employees of ABC Bank Services are required to report any breach of privacy or client confidentiality. Incidents can occur that threaten the privacy of the client or employee's information and can negatively impact the trust and reputation of ABC Bank Services. Various types of these incidents include misdirected faxes and emails to unauthorized recipients, mislabeled statements going to the wrong party, improper storage and disposal of information and loss or theft of computer equipment, laptops, blackberries and physical files.

Below are the steps that must be followed if a breach of privacy or confidentiality occurs.

Step 1: Within the first 30 min of discovery. Employees need to gather preliminary details and inform the compliance department via phone call or email. The compliance department will determine areas or units that need to assist in managing and reporting the incident. The employees will prepare the earlier or first draft of the privacy incident report. The first draft should be forwarded to compliance within 24 h of the incident being detected.

Step 2: Sensitivity of data. The privacy incident report requires employees to identify the type of information released. To properly assess the severity of the incident and determine who needs to be immediately informed, it is critical to know if the information contained personal sensitive information that could be used to perpetrate identity theft or sensitive corporate information that could embarrass ABC Bank Services or a client or if it is relatively harmless information.

Step 3: Details of incident. The employee will collect more data and confirm the details of how the incident occurred and how it was detected. Action plans and escalation protocols will depend on the sensitivity of data and details of the incident.

Step 4: Action plan. In this final step, the compliance department will review all action plans relating to incidents involving personal information. Action plans involving information technology and/or other areas will be reviewed and need to be accepted by the other unit or personnel prior to accepting and approving plans in the incident report. Each action plan should include a process to inform the affected client(s) and offer an apology. Any exceptions to informing a client must be approved by a senior manager.

Research methodology

Data collection method

Data for this study were obtained from primary resources. Two methods of data collection were used, i.e. survey questionnaire and observation. There are several advantages to using more than one data collection method. First, multiple sources of evidence will reduce the biasness of the findings drawn from a single method (Bowen, 2009). Second, the findings' credibility will be enhanced, as the researcher is able to vary and cross-examine the findings from various resources (Eisner, 1991).

Survey questionnaire

A set of structured questions was chosen as data collection instruments. This method of data collection was chosen because the answers from the questions can be reliably aggregated and comparisons can be made to questions to ensure that each survey is

presented with exactly the same questions in the same with confidence. Two sets of scale were posed to the respondents to obtain their perspective on customer data theft. First, "Yes" and "No." Second, respondents need to indicate from a scale of 1 = strongly agree, 2 = agree, 3 = neither agree nor disagree, 4 = disagree to 5 = strongly disagree on the given statements. These scales and measures were chosen because of their simplicity and ease of use (Neuman, 2009).

Survey questions were constructed from the prior literature. The initial questions were validated by experts who have relevant experience with the topic of the research to enhance the construct validity. After getting feedback, the questions were refined so that no questions were redundant and too sensitive, which may have an impact on the willingness of the respondents to answer the questions.

The survey was conducted and covered various employment levels, starting from the lower-level employees up to the top management. Total respondents who contribute to these questionnaires were 50 staff members who came from various departments, including operational control, settlement, transaction management, shareholder services and fund accounting.

Observational studies

Observation is selected because the data collected through this method in which the event is normally and routinely occurring are generally more reliable and free from bias. The influence of the environment to the predetermined outcome is easily recorded (Sekaran and Bougie, 2013). In this study, the researcher observed the organizations and employees' work environment, activities and behaviors toward adhering to the company's policy of protecting client data privacy. The researcher played the role of the participant–observer. Here, the researcher became a part of the work team and examined the work practices in preventing customer data from being exposed to theft.

Findings and discussion

Respondent profiles

The respondents were asked about their personal background profiles in the early part of the questionnaires. Table I shows the demographic profile of respondents who answered the questionnaire. About 60 per cent (n = 30) male and 40 per cent (n = 20) female staff answered the questionnaire. The table also shows the age of the respondents. Most respondents were between the ages of 26-31 (40 per cent, n = 20), followed by the respondents from the ages of 20-25 (34 per cent, n = 17), 32-37 (24 per cent, n = 12) and finally 38and above. In terms of length of services, a majority of the respondents have worked for ABC Bank Services between two and three years (50 per cent, n = 25). The number of new workers is also quite substantial [approximately 40 per cent (n = 20)]. Most of the respondents are from the transaction management team (30 per cent, n = 15), followed by operation control (26 per cent, n = 13), settlement (18 per cent, n = 9), shareholder services (16 per cent, n = 8) and fund accounting (10 per cent, n = 5).

Internal control systems in protecting customer data

In this section, the study examined the opinion of respondents on the internal control system of ABC Bank Services. Table II provides the respondents' views on the organization's internal control systems to protect customer data. The majority of respondents (70 per cent, n = 35) agreed that ABC Bank Services have an update procedure in protecting customer data. Having an update procedure is important, as the procedure is one of the mediums that

Respondent profile	*n*	(%)
Gender		
Male	30	60
Female	20	40
Age		
20-25	17	34
26-31	20	40
32-37	12	24
38 and above	1	2
Length of service		
Less than a year	20	40
2-3 years	25	50
4 years and above	51	10
Department		
Transaction management	15	30
Operation control	13	26
Settlement	9	18
Shareholder services	8	16
Fund accounting	5	10

Table I.
Demographic profile of the respondents

Opinion on the organization's internal control systems	Yes	No
ABC Bank Services has up-to-date procedures in protecting customer data	70% ($n = 35$)	30% ($n = 15$)
ABC Bank Services regularly communicates updates and reminders of the policies and procedures in protecting customer data	100% ($n = 50$)	0% ($n = 0$)
Employees of ABC Bank Services are given appropriate training for their job function and responsibilities in relating to customer data protection	44% ($n = 22$)	56% ($n = 28$)
Each department in the ABC Bank Services has periodic staff meetings or other means of ensuring that relevant information impacting the department's business is communicated throughout the department	40% ($n = 20$)	60% ($n = 30$

Table II.
Internal control system effectiveness

can be used to mitigate customer data theft. They also agreed that ABC Bank Services regularly communicates and updates the policies and procedures in protecting customer data (100 per cent, $n = 50$). However, the majority of staff (56 per cent, $n = 28$) think that they are not given appropriate customer-data-protection-related training for their job function and responsibilities. Both job functions and responsibilities are important, as these will educate staff about their responsibilities to safeguard client data. Furthermore, most of the respondents (60 per cent, $n = 30$) do not agree that each department in the ABC Bank Services has periodic staff meetings or other means of ensuring that relevant information impacting the department's business is communicated throughout the department.

The result indicates that, while the organization regularly communicates an update, the platforms or channels used are possibly ineffective and the information is unable to reach the targeted person successfully. In addition, this can be the result of poor monitoring by top management, which makes the majority the staff fail to update themselves with the latest information on the policy and procedures of the customer data protection in their organization. This will put the organization in jeopardy in regard to customer data theft

because prior literature shows that low resources to implement efficient internal controls (Hanno and Hughes, 1999) and management control systems (Suhaimi *et al.*, 2016) such as inadequate monitoring on lower-level employees contributed to corporate fraud and mismanagement (Puah *et al.*, 2009).

Table III supports this statement. It illustrates the awareness by staff on the ABC Bank Service's procedure on data protection. The table shows that most respondents are aware of the procedure, which can be downloaded from the intranet. However, there were major concerns, as most of the staff in ABC Bank Services had not read or reviewed the policy in many years. For example, a majority of employees (60 per cent, $n = 30$) read and reviewed the customer data protection policy more than two years ago. Consequently, they may not realize that possibly many rules and procedures, which they understand and practiced are already outdated and no longer applicable. This will leave customer data under threat of loss and prone to theft by an irresponsible person.

Factors of customer data theft

In this part, this study analyzed the factors of customer data theft based on the respondents' opinions. Based on Table IV, the highest factor chosen by respondents is nonunderstanding of individual responsibility toward protecting customer data (100 per cent, $n = 50$, mean = 1.8). This is not a surprise because the staff or human capital actually are the best stakeholders and important factors in preventing fraud and malpractices. Ignorant behavior by the staff, i.e. not being concerned with the repercussion effect of their negative behavior, will create many noncompliances in operating procedures and internal controls and, hence, loopholes for fraud. This is consistent with Lokanan (2014) and the report by KPMG Malaysia (2014), which found that insufficient internal is one of the reasons why fraud and assess misappropriation occur in the organization. The other factors, e.g. lack of awareness about the procedure on client data protection, nonadherence to the policy in protecting customer data and opportunity to steal customer data, are equally selected by the respondents (68 per cent, $n = 34$, mean 2.52). The inadequacy of staff scanning during the recruitment process is the last factor selected, indicating the organization has a good and appropriate human resource policy in preventing a potential fraudster from entering the organization.

Impacts of customer data theft

The last part in this survey is to study the opinion of Bank ABC Services staff about the impact of customer data theft to the organization Table V. All respondents strongly agree or agree (100 per cent, $n = 50$) that customer data theft will tarnish the reputation of ABC Bank Services, as it is one the top global custody banks in the world. Additionally, all the respondents also strongly agree that customer data theft will lower the confidence of the public toward ABC Bank Services as a whole. This is consistent with Johnson *et al.* (2014), who found that fraud that damages a company reputation will result in lower sales to the

Table III.
The last time staff read the customer data protection policy

Awareness by staff on the organization's procedure on data protection	Less than 6 months	1 year	2-3 years	4 years and more
The last time staff review and read the policy in protecting customer data	14% ($n = 7$)	25% ($n = 13$)	50% ($n = 25$)	10% ($n = 5$)

Opinion on the factor of the customer data theft	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Mean	SD
Unaware about the procedure on client data protection	0% ($n = 0$)	68% ($n = 34$)	12% ($n = 6$)	20% ($n = 10$)	0% ($n = 0$)	2.52	0.8142
Nonunderstanding of individual responsible toward protecting customer data	20% ($n = 10$)	80% ($n = 40$)	0% ($n = 0$)	0% ($n = 0$)	0% ($n = 0$)	1.80	0.4041
Nonadherence to the policy in protecting customer data	0% ($n = 0$)	68% ($n = 34$)	12% ($n = 6$)	20% ($n = 10$)	0% ($n = 0$)	2.52	0.8142
Opportunity to steal customer data	0% ($n = 0$)	68% ($n = 34$)	12% ($n = 6$)	20% ($n = 10$)	0% ($n = 0$)	2.52	0.8142
Inadequate checks before recruiting staff	0% ($n = 0$)	42% ($n = 21$)	26% ($n = 13$)	22% ($n = 11$)	10% ($n = 5$)	3.00	1.030

Notes: 1 = Strongly agree, 2 = agree, 3 = neither agree nor disagree, 4 = Disagree to 5 = strongly disagree

Table IV.
Factor of customer data theft

Table V.
Impacts of customer data theft

Opinion on the impact of customer data theft to the organization	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Mean	SD
Customer data theft will tarnish the reputation of ABC Bank Services as one of the top global custody banks in the world	66% ($n = 33$)	34% ($n = 17$)	0% ($n = 0$)	0% ($n = 0$)	0% ($n = 0$)	1.66	0.4785
Customer data theft will affect the confidence of the public toward ABC Bank Services	56% ($n = 28$)	44% ($n = 22$)	0% ($n = 0$)	0% ($n = 0$)	0% ($n = 0$)	1.56	0.5014

customer and, hence, decrease company performance, while Lu *et al.* (2010) suggest that cybercrime has a devastating financial impact on an organization as a whole.

Findings from the observation

Based on the observation of employees under the operation control team, it was found that most employees do not follow the policy of protecting customer data. Below is a selected list of standard operating procedures of the staff toward customer data based on the ABC Bank Services policy and the findings from the observation of the study:

SOP 1. Printed documents containing confidential information must be stored in a locked desk or storage area when not in use. It was found that some of the printed documents containing client information were only put in his/her personnel file and not stored in a locked desk.

SOP 2. Never leave original or photocopies of confidential documents around printers and fax machines and left unattended. Always log off the computer when leaving for the day or away from the desk for an extended period of time. Lock the computer workstation by pressing Ctrl-Alt-Del keys and then click on the lock workstation bar.

It was found that there were a few confidential documents around the printer and fax machines and left unattended. In addition, several staffs do not log off their computers while away from their workstations.

SOP 3. Always maintain "clean desk" policy before leaving for the day. All confidential reports, data and records must be kept in a proper storage shelf or cabinets and not on the open areas or floors.

Some of the staff do not adhere to the "clean desk" policy. There are a few client instructions on their workstation.

Based on the findings above, it was clear and consistent with the prior findings discussed in quantitative results that the biggest factor that can lead to data theft is the ignorance of the responsibility to protect customer data. This is evidenced during the observation that shows that the chances of data theft in organizations are due to human factors, albeit sufficient standard operating procedures to protect customer data. Salin *et al.* (2017); Khadijah *et al.* (2015); Manan *et al.* (2013) and Baldock (2016) posit that many corporate scandals occurred due to employee misconduct and unethical practices. This is worse if a company has weak governance mechanisms, poor transparency and lack of accountability (Shariman *et al.*, 2018; Salin, 2017; Nor *et al.*, 2017; Ahmad *et al.*, 2016; Husnin *et al.*, 2016; Asmuni *et al.*, 2015; Hashim *et al.*, 2014; Jaafar *et al.*, 2014; Hamid *et al.*, 2011).

The chances or risk of customer data theft can be reduced if employees are more responsible toward their job and have a sense of accountability toward the customers. The reasons may be consistent with the findings in Table III, in which the majority of employees have not read the data protection policies for a long time. This, however, is again possibly due to human factors, as employees do not have any initiative to refresh and update their memory and knowledge about customer data protection policies. Worse, the employee may know and understand the standard operating procedures but simply chooses to ignore or not to comply with those procedures. This supports the prior survey conducted by the Association of Certified Fraud Examiners (ACFE) (2008), which found that fraud was still detected, even though the organization has a well-established internal control in place, while a survey conducted by PricewaterhouseCoopers found that the employees remain the most cited sources of compromise for cybercrime activities (PricewaterhouseCoopers, 2016).

Conclusions

The main objective of this study is to examine weaknesses in the current internal control system of ABC Bank Services in protecting its customer data. Findings show that the employees of ABC Bank Services are aware that there is a policy of protecting customer data in the organization. However, the main concern is the attitude of the employees to adhere to the policy in place. The result of the survey and observational study shows that employees tend to ignore such policies and standard operating procedures, which establishes opportunities for data theft and fraud to occur. This confirms the fraud triangle theory, which predicts that opportunities are among the important factors before fraud can occur in an organization. This situation requires the internal control systems in ABC Bank Services to be improved and upgraded, particularly in the controls related to personal behaviors. There are a few recommendations suggested to the organization generally and ABC Bank Services particularly.

Training and awareness

The company generally and ABC Bank Services particularly must provide dedicated resources, including time and money, to update various rules, guidelines, policies and procedures related to data security management and protection. However, these rules, guidelines, policies and procedures will not bring any benefits if the employees are not aware of or simply ignore them. This guidance need to be understood and applied as an important part of their daily work process and responsibility. The findings of this study documented that many instances of loss of customer data were due to the staff not having knowledge, forgetting or not understanding the related policies and procedures. To overcome this problem, comprehensive training and awareness programs (including re-training and re-awareness program) need to be conducted to all the staff. In addition, this training can be made compulsory to be attended by the staff annually as a part of their job performance evaluation.

To ensure this training is effective and have an impact on participants, the training also needs to be conducted in the most innovative and attractive way such as case-study-based and problem-based learning. Simple but highly memorable and easily understandable materials related to data security management can be prepared. The focus of the training also needs to be centralized on the risk, particularly financial risk, as a result of the poor data security management and legal risk due to the incompliance of legal and regulatory requirements on customer data protection. In addition, staff needs to understand the importance of data security related to their work and what they need to do, to comply with the relevant standard operating policies and procedures.

Staff scanning and recruitment

The other effort that can be taken by the company is to properly scan and recruit a high-quality and ethical staff to work with the organization. This is important to avoid the company from accidentally hiring a fraudster or a person who become a criminal. Advance personality testing to detect fraudsters and criminal behavior can be used. Although the initial cost is high, but in the long run it is worth paying because the risk of financial and nonfinancial loss from customer data theft is much higher.

Monitoring access to customer data

Customer data accessibility must be restricted and highly controlled. Certain customer segments only can be accessed by particular people while the customers' other demographic data profiles only can be accessed by other employees related with their job. This can limit

the exposure of data stealing in the large scale. Access control can be used to track the access trail, so that the organization can know exactly, which employee accesses particular data at a specific time and location. Multilevel authorization is also effective in preventing employees from accessing and copying customer data that do not relate to his/her roles and tasks.

Overseeing third-party access

Outsourcing certain aspects of a business is typical. However, this also will risk and expose a business to the possibility of customer data theft. Examples of outsourcing tasks to third parties include printing and postage services, off-site archival or storage services that keep hard copies of customer data, cleaning services and supplying of ICTs related hardware and software and security personnel. Certain precautions need to be taken to limit exposure. Due diligence needs to be conducted before hiring third-party services and ensuring this company does not have criminal records. Their services also need to be closely monitored. This can be done by conducting surprise audits to ensure their services are not violating the outsourcing agreement and following the required policies and procedures. A good audit quality is a key to protect the interest of the various stakeholders in the company (Jais *et al.*, 2016).

Use of advanced technology

Technology is easily outdated. Outdated technology risks data theft that uses more sophisticated technology. Thus, technology such as antivirus, antispyware, firewall and its related protection software are highly useful to prevent data from illegal downloading. This technology allows a company to capture nontrusted sites on the Internet set up purposely to steal customer data. By installing this software, a nontrusted website can be totally banned and prevented from being opened.

Prevent from outside access

Data not only can be stolen from the inside but also from the outside. Thus, a high-quality firewall from a reputable supplier can be used to prevent outside attack. Network access also needs to be remotely secured and restricted by using a virtual private network. A data encryption strategy can also be used when transmitting private and highly confidential files, although internal email or intranet.

Research limitations and suggestion for future research

This study has several limitations. First, only one company gave permission for the research to be conducted on its premises via observation and questionnaires distributed to its employees. The sensitivity of the issues makes it difficult to find other companies to participate in the research. Because of this, the findings may not be generalized to other organizations because of different structures, cultures, business climates and operations unique to a company.

Second, this study only employed straightforward questions about internal controls and data theft, while the number of questions is also quite small. Many employees were unable to participate due to limitations of time available and being occupied at the workplace. Some of them also refused to participate due to the sensitivity of the nature of the topic.

Thus, future research can be conducted with some improvement. Studies can be conducted to investigate the relationship of data theft with organizational determinants, such as internal control weaknesses and behavioral determinants, such as organizational commitment and ethical conduct. Understanding and awareness of these determinants will help organizations to decrease data theft risk.

Other research methods such as market surveys can also be used to gather large amounts of information. More participants from employees and organizations can be invited to participate so that the findings and conclusions can be generalized in the bigger picture.

Comparisons among industries such as banking, finance, construction and others also can be examined for specific data theft characteristics according to the industry. Thus, a company can use the proper standard operating procedures and internal control design to combat data theft specific to the nature of their business.

References

Ahmad, N.M.N.N., Nawawi, A. and Salin, A.S.A.P. (2016), "The relationship between human capital characteristics and directors' remuneration of Malaysian public listed companies", *International Journal of Business and Society*, Vol. 17 No. 2, pp. 347-364.

Allison, S.F., Schuck, A.M. and Lersch, K.M. (2005), "Exploring the crime of identity theft: prevalence, clearance rates, and victim/offender characteristics", *Journal of Criminal Justice*, Vol. 33 No. 1, pp. 19-29.

Amirudin, N.R., Nawawi, A. and Salin, A.S.A.P. (2017), "Risk management practices in tourism industry – a case study of resort management", *Management and Accounting Review*, Vol. 16 No. 1, pp. 55-74.

Asmuni, A.I.H., Nawawi, A. and Salin, A.S.A.P. (2015), "Ownership structure and auditor's ethnicity of Malaysian public listed companies", *Pertanika Journal of Social Science and Humanities*, Vol. 23 No. 3, pp. 603-622.

Association of Certified Fraud Examiners (ACFE) (2008), *Report to the Nations on Occupational Fraud and Abuse*, ACFE, Austin.

Baldock, G. (2016), "The perception of corruption across Europe, Middle East and Africa", *Journal of Financial Crime*, Vol. 23 No. 1, pp. 119-131.

Blasco, J., Tapiador, J.E., Peris-Lopez, P. and Suarez-Tangil, G. (2015), "Hindering data theft with encrypted data trees", *Journal of Systems and Software*, Vol. 101, pp. 147-158.

Bossler, A.M. and Holt, T.J. (2009), "On-line activities, guardianship, and malware infection: an examination of routine activities theory", *International Journal of Cyber Criminology*, Vol. 3 No. 1, pp. 400-420.

Bowen, G.A. (2009), "Document analysis as a qualitative research method", *Qualitative Research Journal*, Vol. 9 No. 2, pp. 27-40.

Choi, K.S. (2008), "Computer crime victimization and integrated theory: an empirical assessment", *International Journal of Cyber Criminology*, Vol. 2 No. 1, pp. 308-333.

Computer Security Institute (2007), "Computer crime and security survey", available at: www.cybercrime.gov/FBI2006.pdf (accessed 19 April 2007).

Copes, H. and Vieraitis, L.M. (2009), "Bounded rationality of identity thieves: using offender-based research to inform policy", *Criminology and Public Policy*, Vol. 8 No. 2, pp. 237-262.

Cressey, D.R. (1973), *Other People's Money*, Montclair: Patterson Smith.

Das, A. and Khan, H.U. (2016), "Security behaviors of smartphone users", *Information and Computer Security*, Vol. 24 No. 1, pp. 116-134.

Deng, X., Wang, Y., Zhang, Q., Huang, J.X. and Cui, J. (2014), "Analysis of fraud risk in public construction projects in China", *Public Money and Management*, Vol. 34 No. 1, pp. 51-58.

Eisner, E.W. (1991), *The Enlightened Eye: Qualitative Inquiry and the Enhancement of Educational Practice*, Collier Macmillan, Toronto.

Ermongkonchai, P. (2010), "Understanding reasons for employee unethical conduct in Thai organizations: a qualitative inquiry", *Contemporary Management Research*, Vol. 6 No. 2, pp. 125-140.

Ernst and Young (2011), *Data Loss Prevention – Keeping Your Sensitive Data out of the Public Domain*, London: Ernst and Young.

Financial Crime and Intelligence Division (2008), *Data Security in Financial Services*, The Financial Services Authority, London.

Furnell, S. (2002), *Cybercrime: Vandalizing the Information Society*, Boston: AddisonWesley

Gordon, S. (2000), "Virus writers: the end of the innocence? ", Cambridge, MA: IBM Thomas J. Watson Research Center.

Gordon, S. and Ma, Q. (2003), *Convergence of Virus Writers and Hackers: Fact or Fantasy?*, Symantec, Cupertine, CA.

Gordon, G.R., Rebovich, D.J., Choo, K. and Gordon, J.B. (2007), *Identity Fraud Trends and Patterns: Building a Data-Based Foundation for Proactive Enforcement*, Center for Identity Management and Information Protection, Utica College.

Grabosky, P. (2007), "The internet, technology, and organized crime", *Asian Journal of Criminology*, Vol. 2 No. 2, pp. 145-161.

Grabosky, P.N. and Smith, R. (2001), "Telecommunication fraud in the digital age: the convergence of technologies", in D. Wall (Ed.), *Crime and the Internet*, New York, NY: Routledge, pp. 29-43.

Grabosky, P., Smith, R.G. and Dempsey, G. (2001), *Electronic Theft: Unlawful Acquisition in Cyberspace*, Cambridge University Press.

Hamid, A.A., Haniff, M.N., Osman, M.R. and Salin, A.S.A.P. (2011), "The comparison of the characteristics of the Anglo-Saxon governance model and the Islamic governance of IFIs", *Malaysian Accounting Review*, Vol. 10 No. 2, pp. 1-12.

Hanno, D.M. and Hughes, T.A. (1999), "Defending your dollars", *Strategic Finance*, Vol. 81 No. 2, pp. 56-60.

Hashim, M.F., Nawawi, A. and Salin, A.S.A.P. (2014), "Determinants of strategic information disclosure – Malaysian evidence", *International Journal of Business and Society*, Vol. 15 No. 3, pp. 547-572.

Hassan, N., Nawawi, A. and Salin, A.S.A.P. (2016), "Improving tax compliance via tax education – Malaysian experience", *Malaysian Accounting Review*, Vol. 15 No. 2, pp. 243-262.

Hinz, O., Nofer, M., Schiereck, D. and Trillig, J. (2015), "The influence of data theft on the share prices and systematic risk of consumer electronics companies", *Information and Management*, Vol. 52 No. 3, pp. 337-347.

Holt, T.J. (2007), "Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures", *Deviant Behavior*, Vol. 28 No. 2, pp. 171-198.

Holt, T.J. and Bossler, A.M. (2008), "Examining the applicability of lifestyle-routine activities theory for cybercrime victimization", *Deviant Behavior*, Vol. 30 No. 1, pp. 1-25.

Holt, T.J. and Bossler, A.M. (2014), "An assessment of the current state of cybercrime scholarship", *Deviant Behavior*, Vol. 35 No. 1, pp. 20-40.

Holtfreter, K., Reisig, M.D., Pratt, T.C. and Holtfreter, R.E. (2015), "Risky remote purchasing and identity theft victimization among older internet users", *Psychology, Crime and Law*, Vol. 21 No. 7, pp. 681-698.

Holt, T.J. and Graves, D.C. (2007), "A qualitative analysis of advanced fee fraud schemes", *The International Journal of Cyber-Criminology*, Vol. 1 No. 1, pp. 137-154.

Holt, T.J. and Lampke, E. (2010), "Exploring stolen data markets online: products and market forces", *Criminal Justice Studies*, Vol. 23 No. 1, pp. 33-50.

Holt, T.J. and Turner, M.G. (2012), "Examining risks and protective factors of on-line identity theft", *Deviant Behavior*, Vol. 33 No. 4, pp. 308-323.

Holt, T.J., Smirnova, O. and Chua, Y.T. (2016), "Exploring and estimating the revenues and profits of participants in stolen data markets", *Deviant Behavior*, Vol. 37 No. 4, pp. 353-367.

Husnin, A.I., Nawawi, A. and Salin, A.S.A.P. (2013), "Corporate governance structure and its relationship with audit fee – evidence from Malaysian public listed companies", *Asian Social Science*, Vol. 9 No. 15, pp. 305-317.

Husnin, A.I., Nawawi, A. and Salin, A.S.A.P. (2016), "Corporate governance and auditor quality – Malaysian evidence", *Asian Review of Accounting*, Vol. 24 No. 2, pp. 202-230.

Hutchings, A. and Holt, T.J. (2016), "The online stolen data market: disruption and intervention approaches", *Global Crime*, pp. 1-20.

Jaafar, M.Y., Nawawi, A. and Salin, A.S.A.P. (2014), "Directors' remuneration disclosure and firm characteristics – Malaysian evidence", *International Journal of Economics and Management*, Vol. 8 No. 2, pp. 269-293.

Jais, K.M., Nawawi, A. and Salin, A.S.A.P. (2016), "Reduction of audit quality by auditors of small and medium size audit firms in Malaysia: a case of premature sign-off of audit documents", *Journal of Accounting, Business and Management*, Vol. 23 No. 2, pp. 1-12.

James, L. (2005), *Phishing Exposed*, Rockland: Syngress.

Johnson, W.C., Xie, W. and Yi, S. (2014), "Corporate fraud and the value of reputations in the product market", *Journal of Corporate Finance*, Vol. 25, pp. 16-39.

Karim, N.A., Nawawi, A. and Salin, A.S.A.P. (2018), "Inventory control weaknesses – a case study of lubricant manufacturing company", *Journal of Financial Crime*, Vol. 25 No. 2, pp. 436-449.

Khadijah, A.S., Kamaludin, N. and Salin, A.S.A.P. (2015), "Islamic work ethics (IWE) practice among employees of banking sectors", *Middle-East Journal of Scientific Research*, Vol. 23 No. 5, pp. 924-931.

King, A. and Thomas, J. (2009), "You can't cheat an honest man: Making ($$$s and) sense of the nigerian e-mail scams", in Schmalleger F. and Pittaro M. (Eds), *Crimes of the Internet*, Prentice Hall, River, NJ, pp. 206-224.

KPMG Malaysia (2014), *Fraud, bribery and Corruption Survey 2013*, KPMG Malaysia, Kuala Lumpur.

Lokanan, M.E. (2014), "How senior managers perpetuate accounting fraud? Lessons for fraud examiners from an instructional case", *Journal of Financial Crime*, Vol. 21 No. 4, pp. 411-423.

Lu, H., Liang, B. and Taylor, M. (2010), "A comparative analysis of cybercrimes and governmental law enforcement in China and the United States", *Asian Journal of Criminology*, Vol. 5 No. 2, pp. 123-135.

Manan, S.K.A., Kamaluddin, N. and Salin, A.S.A.P. (2013), "Islamic work ethics and organizational commitment: evidence from employees of banking institutions in Malaysia", *Pertanika Journal of Social Science and Humanities*, Vol. 21 No. 4, pp. 1471-1489.

Martin, K.D., Borah, A. and Palmatier, R.W. (2016), "Data privacy: effects on customer and firm performance", *Journal of Marketing*, Vol. 81 No. 1, pp. 36-58.

Morris, R.G. (2010), "Identity thieves and levels of sophistication: findings from a national probability sample of american newspaper articles 1995-2005", *Deviant Behavior*, Vol. 31 No. 2, pp. 184-207.

Nawawi, A. and Salin, A.S.A.P. (2018), "Employee fraud and misconduct: empirical evidence from a telecommunication company", *Information and Computer Security*, Vol. 26 No. 1, pp. 129-144.

Nazario, J. (2004), *Defense and Detection Strategies against Internet Worms*, Artech House, Boston, MA.

Neuman, W.L. (2009), *Social Research Methods – Qualitative and Quantitative Approaches*, Pearson, Toronto.

Newman, G. and Clarke, R. (2003), *Superhighway Robbery: Preventing e-commerce Crime*, Willan Press, Cullompton.

Nor, N.H.M., Nawawi, A. and Salin, A.S.A.P. (2017), "The influence of board independence, board size and managerial ownership on firm investment efficiency", *Pertanika Journal of Social Science and Humanities*, Vol. 25 No. 3, pp. 1039-1058.

Omar, M., Nawawi, A. and Salin, A.S.A.P. (2016), "The causes, impact and prevention of employee fraud: a case study of an automotive company", *Journal of Financial Crime*, Vol. 23 No. 4, pp. 1012-1027.

PricewaterhouseCoopers (2016), *The Global State of Information Security Survey*, PricewaterhouseCoopers LLP, New York, NY.

PricewaterhouseCoopers, Malaysia (2016), *Economic Crime from the Board to the Ground: Why a Disconnect Is Putting Malaysian Companies at Risk*, PricewaterhouseCoopers, Kuala Lumpur.

Puah, C.H., Voon, S.L. and Entebang, H. (2009), "Factors stimulating corporate crime in Malaysia", *Economics, Management, and Financial Markets*, Vol. 4 No. 3, pp. 87-99.

Rahim, S.A.A., Nawawi, A. and Salin, A.S.A.P. (2017), "Internal control weaknesses in a cooperative body: Malaysian experience", *International Journal of Management Practice*, Vol. 10 No. 2, pp. 131-151.

Saibon, N.A., Nawawi, A. and Salin, A.S.A.P. (2016), "E-filing acceptance by the individual taxpayers – a preliminary analysis", *Journal of Administrative Science*, Vol. 13 No. 2, pp. 1-14.

Salin, A.S.A.P. (2017), "Malaysian private entities reporting standards – benefits and challenges to SMEs", *International Journal of Academic Research in Business and Social Sciences*, Vol. 7 No. 11, pp. 1302-1320.

Salin, A.S.A.P., Manan, S.K.A., Kamaluddin, N. and Nawawi, A. (2017), "The role of Islamic ethics to prevent corporate fraud", *International Journal of Business and Society*, Vol. 18 No. S1, pp. 113-128.

Schuchter, A. and Levi, M. (2016), "The fraud triangle revisited", *Security Journal*, Vol. 29 No. 2, pp. 1-15.

Sekaran, U. and Bougie, R. (2013), *Research Methods for Business: a Skill Building Approach*, John Wiley and Sons, West Sussex.

Sen, R. and Borle, S. (2015), "Estimating the contextual risk of data breach: an empirical approach", *Journal of Management Information Systems*, Vol. 32 No. 2, pp. 314-341.

Shariman, J., Nawawi, A. and Salin, A.S.A.P. (2017), "Public sector accountability – evidence from the auditor general's reports", *Management and Accounting Review*, Vol. 16 No. 2, pp. 231-257.

Shariman, J., Nawawi, A. and Salin, A.S.A.P. (2018), "Issues and concerns on statutory bodies and federal government – evidence from Malaysian auditor general's report", *International Journal of Public Sector Performance Management*, Vol. 4 No. 2, pp. 251-265.

Suhaimi, N.S.A., Nawawi, A. and Salin, A.S.A.P. (2016), "Impact of enterprise resource planning on management control system and accountants' role", *International Journal of Economics and Management*, Vol. 10 No. 1, pp. 93-108.

Suhaimi, N.S.A., Nawawi, A. and Salin, A.S.A.P. (2017), "Determinants and problems of successful ERP implementations – Malaysian experience", *International Journal of Advanced Operations Management*, Vol. 9 No. 3, pp. 207-223.

Synovate (2003), *Federal Trade Commission – Identity Theft Survey Report*, available at: www.ftc.gov/os/2003/09/synovatereport.pdf. (accessed 13 July 2016)

Szor, P. (2005), *The Art of computer Virus Research and Defense*, Addison Wesley, Upper Saddle River, NJ.

Taylor, R.W., Fritsch, E.J. and Liederbach, J. (2014), *Digital Crime and Digital Terrorism,* Upper Saddle, Prentice Hall, River, NJ.

Taylor, R.W., Caeti, T.J., Loper, D.K., Fritsch, E.J. and Liederbach, J. (2006), *Digital Crime and Digital Terrorism,* Upper Saddle, Pearson Prentice Hall, River, NJ.

Tran, T.T.G., Le, D.Q. and Tran, T.D. (2016), "Virtualization at file system level: a new approach to secure data in shared environment", *International Journal of Computer Theory and Engineering*, Vol. 8 No. 3, pp. 223-228.

Wall, D. (2001), "Cybercrimes and the internet", in D. S. Wall (Ed.), *Crime and the Internet*, Routledge, New York, NY, pp. 1-17.

Wall, D.S. (2007), *Cybercrime: The Transformation of Crime in the Information Age*, Polity Press, Cambridge.

Zakaria, K.M., Nawawi, A. and Salin, A.S.A.P. (2016), "Internal controls and fraud – empirical evidence from oil and gas company", *Journal of Financial Crime*, Vol. 23 No. 4, pp. 1154-1168.

About the authors

Mohd Aizuddin Zainal Abidin received his master's degree in Aaccountancy from University Teknologi MARA, Malaysia. He has many years of experience in accounting and auditing in public and private international organizations.

Anuar Nawawi is a Lecturer at the Faculty of Accountancy, Universiti Teknologi MARA, Malaysia. He received PhD in Commerce (Accounting) from the University of Adelaide, South Australia. He also holds a professional qualification of the Chartered Institute of Management Accountants (Passed Finalist), an affiliate Registered Financial Planner and a master's degree in Accounting (with distinction) from Curtin University of Technology, western Australia. He has taught a variety of courses centered on the accountancy discipline. Among them are financial accounting, auditing, management accounting, taxation, financial management, strategic management, computerized accounting and research methodology. His research interests are diverse, including areas such as management accounting, strategic management, forensic accounting and corporate governance.

Ahmad Saiful Azlin Puteh Salin is a Senior Lecturer at the Faculty of Accountancy, Universiti Teknologi MARA Perak Branch Tapah Campus. He received PhD in corporate governance and ethics from the Edith Cowan University, Australia. He also a Fellow Member of the Association of Chartered Certified Accountant, UK (ACCA, UK), a full member of Malaysian Institute of Accountants (MIA) and a member of Malaysian Insurance Institute (MII) and Qualitative Research Association of Malaysia (QRAM). He has taught a variety of courses in corporate governance, business ethics, taxation, financial accounting and reporting, management accounting, costing and integrated case study. His research interests focus primarily in the field of governance, Islamic and business ethics, financial reporting, management, accounting education, SMEs and public sector accounting. He published many articles in local and international journals and was appointed as a reviewer in several international journals and conferences. Ahmad Saiful Azlin Puteh Salin is the corresponding author and can be contacted at: ahmad577@perak.uitm.edu.my