INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 11, Issue 9, (2021) E-ISSN: 2222-6990

Can Internal Control, Rules and Regulations and Technology Adoption influence Bank's Protection of Customers' Data Security?

Muhammad Haziq Al Hafiz Mat Yusof[1], Kamaruzzaman Muhammad[2], Saiful Anuar Sabarudin[3], Erlane K Ghani[4]

[1]Affin Bank Berhad, Malaysia, [2,3,4]Universiti Teknologi MARA Selangor, Malaysia

Email: saifu367@uitm.edu.my

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v11-i9/10855 DOI:10.6007/IJARBSS/v11-i9/10855

Published Date: 20 September 2021

Abstract

The emergence of the internet led to issues concerning privacy and data protection of the customers in the banking industry. Of consequence, the banks have initiated several strategies to protect their customers. Among the strategies adopted by the banks include implementing good internal control and rules and regulations. The banks also have adopted technology in protecting their customers. However, there is yet limited study that has examined these factors from the contexts of customers' data protection of the banks. This study aimed to examine the factors influencing employees' understanding of customers' data security. Specifically, this study examined the effect of internal control, rules and regulations, and technology adoption on Malaysian banks' protection of customers' data security. Utilising questionnaire as the research instrument, this study obtained responses from 220 bank employees. Based on the multiple regression analysis, this study showed that internal control and technology adoption have a significant positive effect on banks' protection of customers' data security. However, this study could not provide evidence on the significant effect of rules and regulations on customers' data security protection. The findings of this study highlight the importance of protecting the customers' data security to financial institutions. They also underscore the significant impact of data theft on individuals and organisations since customers' information or data is a precious commodity in today's world.

Keywords: Internal Control, Technology, Data Security, Customers, Banks

Introduction

Technology plays an important role in the operations of a company, and the financial sector has been one of the biggest supporters of technological advances (Ghani & Said, 2010). Financial institutions have been using programmable computing machines in many advanced countries since 1940. In the 1980s, the Malaysian banking industry began using computers

in everyday operations. Technology is getting better and better with the progress of time. Financial technology plays an important role in the delivery of financial and banking services through modern technological advancements driven by computer programmes and algorithms (Ozili, 2017). With the advancement of information technology, many industry players, governments, and academia have found it easier to collect and store personal information all around the globe. The days where people were asked to write their personal data are long gone as vital information can be obtained through one click. Big Data technology allows one to collect and process voluminous data since there are increasing concerns on the privacy and protection of online users (Karat et al., 2005).

Zharova and Elin (2017), in their study, mentioned that banks are seriously considering the use of Big Data. They further added that, in 2015, 11 financial institutions have used modern technology to analyse Big Data. Other banks also plan to implement these technologies. Their study claimed that personal data refers to a person's personal information, usually known only to the owner, close family, and friends. The particulars may include his address, telephone number, identity card number, sex, and birth date. Given their sensitive nature, these data should not be easily gained, openly transferred, or used without much control in daily transactions. Such transactions vary from application of memberships, registrations, and business activities. Unguarded data transfer gets worse when such transactions take place across a number of sectors, such as finance, retail, service providers, education, and health. Lack of data security has led to increased data theft cases, particularly in Malaysia.

To combat the issue of data theft, Malaysian lawmakers introduced the personal data legislation in 1998. Hassan (2012) noted that the law was subsequently amended in 2003 after considering inputs from public comments. The primary purpose of the Personal Data Protection Act (PDPA) is to monitor any person's collection, holding, processing or usage of personal data to protect an individual's personal data and to safeguard that individual's privacy interest. This monitoring will help build consumer trust and create a level playing field where the abuse of personal information cannot lead to a competitive advantage. In addition, the internal control of the banking industry has played a major role in avoiding data theft and leakage to the public. On 24 June 2004, the former Chairman of the Public Company Accounting Oversight Board, William McDonough, claimed that good internal control is one of the most powerful deterrents to fraud, which can help protect the investors from the types of financial reporting scandals that the Sarbanes-Oxley Act seeks to prevent.

This study aimed to examine the factors influencing the banks' protection of customers' data security. Specifically, this study examined the effect of rules and regulations, internal control, and technology adoption on the protection of customers' data security by public banks in Malaysia. The findings of this study may assist the banks and other related parties in obtaining information and references on important values of customers' information. They could also be a reference on how customer's information or data could be protected. The next section provides the literature review. Section three explains the research methodology, followed by Section four that presents the results and discussion. The last section concludes this study.

Literature Review

Customers' Data Security

Under the current landscape, personal data is on its way to becoming a very important commodity of the information economy. Personal data refers to any personal information about an entity known only to the owner, family, and friends (Yusof et al., 2016). The

information may include address, telephone number, and identity card number, among others. Despite the sensitive nature of these data, they can be easily obtained and used freely in daily transactions without much control using advanced technology. The development of information technology has provided opportunities for many organisations, particularly financial institutions, to acquire customer data very conveniently. Financial institutions are required to obtain customer data for many reasons, such as risk profiling, reducing the risk of bad and dubious debts, searching debtors, and facilitating more efficient collection services.

Geeta (2011) stated in her studies that there are different ways in which data security of the consumer can be infringed, and identity thefts occur. Theft of identity can occur using the following methods:

a) *Dumpster diving.* The perpetrator digs through garbage in search of bills or other records containing personal information about the individual.
b) *Skimming.* When processing the customer's credit/debit card, the perpetrator snips the card numbers using a special storage device.
c) *Phishing*. The caller claims to be from a financial institution or organisation and sends spam or pop-up messages to get the client to share his private information.
d) *Changing your address*. The perpetrator moves the financial records of the customer to another location by changing the address of the customer.
e) *Old-fashioned stealing*. The perpetrator steals a belonging (e.g., wallet) of the person that contains his personal information.
f) *Pretexting*. The perpetrator makes false claims to gain a customer's private information from financial institutions, telephone companies, or other similar organisations.

Studies have suggested that identity theft is a single area of concern for consumers. For example, many consumers would prefer to switch to a banking institution with stronger personal data security (Geeta, 2011). This preference is because if the customers feel that their personal data is not well secured, their satisfaction gets compromised. Customer satisfaction is one of the main trust-building qualities in financial services that would result in higher revenue. Several companies store data from consumers at an unprecedented speed, fuelled by emerging technologies, such as tablets, and applications for data mining and data processing. Earley (2015) claimed that the availability of computerised data in companies has slowly increased over the years. However, recent advances in the processing of fast cloud storage and the increase in social networks have changed the ease of data access and the types of data that can be accessed and stored for later use.

Often, security risk cannot be detected by many companies due to three factors (Abidin et al., 2019). The first factor is that they do not appreciate the magnitude of this risk. The second factor is that the organisation does not have the expertise to make a reasonable evaluation of the key risk factors and find ways to mitigate the risk. The third factor is that the organisation may not allocate sufficient resources to address the risk. In addition, Amirudin et al., (2017) stated that large and medium-sized organisations typically commit adequate resources to data security risk management, but there is a lack of coordination among the business areas affected, such as human resources, information technology (IT), and information security (IS). There is too much focus on information and communication technology (ICT), but little attention is given to the processes of the organisation, supervision, and due diligence. Failure by companies to address this issue contributes to the

usual circumstances of businesses that are adversely affected, resulting in unwanted consequences.

Internal Control

Internal control plays a vital part in fulfilling the responsibilities of an organisation. Eilifsen et al. (2017) noted that management is responsible to implement an internal control system that can provide assurance that the data can be properly protected and that information from the company is accurate for decision-making. If the information system does not generate reliable information, the organisation may not be able to make informed decisions on issues (Mohd Ali et al., 2020), such as product pricing and production costs. It would also not be able to provide information on profit and external reports for investors and other stakeholders. Ji, Lu, and Qu (2017) also stated that establishing a high-quality internal control system has been regarded as vital for ensuring high-quality financial reporting. Weak internal control can lead to material errors or even false financial disclosures.

The internal control of the banking industry has played a major role in avoiding data theft and leakage to the public. Eilifsen et al. (2017) claimed that internal control plays a crucial role in the way the company fulfils its obligations. Internal controls are used with respect to fraud to deter or detect fraud. Internal controls play an important role in preventing fraud by reducing the incentives for insiders and outsiders to commit fraud (Jermsittiparsert et al., 2019). Higgins (2012), in his study, discussed how poor internal control contributed to a major fraud at the Bank of China. Poor internal control will also lead to many problems, such as inaccurate financial reporting, failed loans, misappropriation, loss of investors' trust, and many more. Spatacean (2012) noted that one of the key challenges in the estimation of risk factors for fraud is that the real level of fraud at any point in time will always be an unknown variable. Internal control is one of the ways to identify and recognise where all the vulnerabilities are within the organisation's controls and where things have gone wrong before fraud comes to light. The study also concluded that the more effective the internal financial control is, the less is the extent of fraudulent financial reporting.

Higgins (2012) also stated that China's banking system differs significantly from the Western private, market-based system of financial institutions in that China's banks are state-owned and play an important role in the financing of business enterprises. On average, the Chinese government owns 53% of the total shares of a listed company, while the second-largest shareholder holds about 10%. In addition, a smaller size organisation may not require having all the components of internal control. However, Shi and Wang (2012) reported that these smaller organisations appear to be underperforming, participate in more earnings exploitation, and pay higher audit fees. Chalmers et al. (2019) suggested that smaller and more complex firms are correlated with poorer internal control. Poor internal control is also correlated with reduced independence and competence of the board and audit committee, increased financing costs, lower estimates of profits, and higher audit fees. This study believes that effective implementation of internal control has a positive impact on banks' protection of customers' data security. Hence, the hypothesis proposed is as follows:

H1: Effective internal control has a significant effect on customers' data security protection.

Rules and Regulation

Rules can be defined as guidelines for completing certain tasks or doing things correctly and are bound to legal requirements (Abidin et al., 2009). Both rules and regulations are present

everywhere and act as a legal compass to ensure all parties are protected (Ilias et al., 2020). In their study, Zainal Abidin et al. (2019) stated that countries in the European Union are subjected to the data protection directive specifically to address this issue. The worrying trend of customer data theft has also happened in Malaysia. Hence, to combat the issue of data theft, Malaysian lawmakers had regulated personal data legislation in 1998 with the sole intention of building user confidence and creating a level playing field where the misuse of private information cannot result in competitive advantage. Hassan (2012) found that the bill was subsequently revised in 2003 after taking into account public commentaries. It is later known as the Personal Data Protection Act (PDPA) to protect a person's personal data. However, it also normalises any person collecting, holding, processing or using another person's personal information through any other person for legitimate purposes and with the data owner's permission.

The Central Bank of Malaysia provides specific guidelines to all financial institutions in the country to ensure the establishment and maintenance of a sound management of data and MIS (Abidin et al., 2009). The guidelines are also used to create a corporate culture that reinforces the importance of data completeness and data quality and to ensure adequate and effective data protection control. The Management Committee maintains that the Board of Directors meets this condition with proper oversight. Raab and Szekely (2017) reported that local systems are very dependent on the way the data protection authorities (DPAs) conduct their role of protecting personal data. The explanation is that most countries are blamed for implementing legislation to protect privacy without developing infrastructure that provides the enforcement powers with administrative machinery that can facilitate or enable compliance, good practice or other criteria. However, the DPAs are not systematic in their function; some DPAs may prioritise enforcement, others may focus on public education, and some may be closely involved in legislation and regulatory recommendations. Raab and Szekely (2017) noted that they need to consider the effects of data protection and data privacy on the widespread use of information and communications technology (ICTs), where large-scale analysis on personal data through a wide range of interests is standard. Through the financial industry's perspective, such incident could and would lead to many implications, such as commercial, reputation, regulatory and legal risks, and penalties. Hence, the second hypothesis that was proposed is as follows:

H2: Rules and regulations have a significant effect on customers' data security protection.

Technology Adoption

Technology plays a vital role in the operations of an enterprise, and one of the largest adopters of technological advances has been the financial sector. Ahlan (2015) reported that financial institutions have started to use programmable computing machines in many advanced countries since 1940. In the 1980s, the banking industry in Malaysia started using computers throughout the daily operations. With the rapid changes and modernisation, technology is getting better and better. As part of technological advancement, financial technology plays a vital role in delivering financial and banking services through modern technological innovations led by computer programmes and algorithms (Ozili, 2017). The passage of the 2002 Sarbanes-Oxley Act (SOX), through the provisions of its Section 404, greatly expands the auditors' internal control role. This expansion has resulted in a substantial increase in demand for skilled audit personnel, resulting in staff shortages and increasing audit costs. It also creates an opportunity to simplify audit processes to boost the

auditors' performance further. Hence, it comes as no surprise that many internal auditors are now at the forefront of introducing such modern technologies for audit automation and continuous auditing. Most companies in the financial industry are trying to eliminate manual work through Robotic Process Automation (RPA) to cope with increasing workloads and ease the pressure. The introduction of RPA would also create a new internal control and risk management environment.

Internal auditors play an increasingly important role in a business environment that is evolving at a faster rate than ever before (Chuah, 2018). With the vast uncertainties of an influx of disruptive powers, the internal audit role must keep pace to help the company understand and manage the associated risks, achieve planned automation results, and continue to innovate to add value. Chuah (2018) stated that key internal audit opportunities inside smart automation programmes would help integrate governance, risk, and control concerns throughout the life cycle of the automation system as an enterprise develops and implements the programme. Auditors would also have the opportunity to help identify opportunities for the organisation to integrate automation-enabled control activities within the business processes and functions. Eventually, the internal audit agency would draw on advances in intelligent automation to improve the efficacy and productivity of its activities.

Studies have also suggested the use of new technology equipped with data-driven fraud detection as a control measure to detect and prevent fraud from happening. This new technology is vital due to its ability to offer precision, operational efficiency, and cost efficiency, which the traditional control measures are no longer able to offer, and banks are no longer able to afford such disadvantages (Lessmann et al., 2015). Hence, banks can no longer rely on traditional control measures to protect their customers' data security. Furthermore, Kahyaoglu and Caliyurt (2018) mentioned that, at the international level, current business surroundings had created a necessity of having a safe and, more importantly, secure digital infrastructure for commercial transactions. One of the methods is by having advanced technology integrated with daily transactions. Hence, the third hypothesis proposed is as follows:

H3: Technology adoption has a significant effect on customers' data security protection.

Research Design

Sample Selection

The employees of a bank in Malaysia. The bank is a public listed company with 110 branches throughout Malaysia as at December 2020. Specifically, this study selected the employees who are stationed under the Group Risk Division, Group Internal Audit Division, and Group Compliance Division. The motive behind the selection is that these divisions are involved in many core functions and represent the three lines of defence of a company. In addition, the three divisions are responsible for providing a good blueprint and control measure for the bank to protect its customer data security, which is a highly sought commodity. Roscoe (1975) suggested that the minimum sample size should be at least 10% of the population, and the appropriate sample size should not be larger than 500 but must not be less than 30. Hence, in this study, the sample size was determined as 300 employees. Questionnaires were distributed to the respondents based on convenient sampling.

Research Instrument and Data Collection

This study used the questionnaire survey as the research instrument. The questionnaire was developed based on reviewing previous studies with some modifications to suit the context of this study. There were five sections in the questionnaire. The first section, Section A, requested the respondents to provide their understanding of the importance of having an efficient control measure in protecting customers' data and the protective tools used in their current company. Section B requested the respondents to indicate the importance of internal control that reflects the existing control measure in protecting customers' data. Section C requested the respondents to indicate the importance of IT infrastructure that reflects the existing control measure in protecting customers' data. Section D requested the respondents to indicate the importance of rules and regulations that reflects the existing control measure in protecting customers' data. Section A to Section D utilised the 5-point Likert scale from 1 'strongly disagree' to 5 'strongly agree'. The last section, Section E, covered the general information about the respondents' demographic profile, such as gender, age, position, experience, and others.

The questionnaires were distributed to the respondents through email and Google Form. The respondents were approached beforehand to explain the purpose of this study and the importance of them participating in the questionnaire survey. In all, 220 employees participated in the survey, resulting in a response rate of 73%.

Results and Discussion

Customers' Data Security

Table 1 presents the details of the descriptive statistics for all constructs of customers' data security in descending order. The results show that the mean scores for all items range from 4.4364 to 4.8545. The overall mean score for customers' data security is 4.7121. This score indicates that the respondents agree on the importance of protecting customers' data. In addition, the highest standard deviation is 0.80946 for item 'It is important for employees to monitor and ensure that customers' data is solely used for business purposes', while the lowest standard deviation is 0.35581 for item 'It is important for every party to be involved in protecting personal data as a legal socio obligation'.

Table 1
Descriptive Statistics of Customers' Data Security

List of Item	Mean	Std. Deviation
It is important for every party to be involved in protecting personal data as a legal socio obligation	4.8545	.35581
Enhancing customers' data security helps to protect customers' privacy and avoid unwanted interference	4.8182	.38925
Financial institutions obtain consent from the customers before proceeding to use the data for business purposes.	4.4364	.68755
It is important for employees to monitor and ensure that customers' data is solely used for business purposes	4.5818	.80946
Financial institutions are responsible in protecting their customers' personal data from any misuse or data leak	4.7818	.49781
Personal information obtained by the financial institutions is for internal use and not to be sold to external party	4.8000	.55777

List of Item	Mean	Std. Deviation
All Items	4.7121	0.5497

Internal Control

Table 2 presents the details of the descriptive statistics for all constructs of internal control security in descending order. The mean scores for the items related to internal control range from 4.7273 to 4.4909. The overall mean score for internal control is 4.61. This score indicates that the respondents agree on the importance of protecting customers' data. The highest standard deviation is 0.87924 for item 'Internal control is said to be effective if it is implemented across the company', while the lowest standard deviation is 0.42004 for item 'Financial institutions need to have a strong internal control to prevent a breach of customers' personal data'.

Table 2
Descriptive Statistics of Internal Control

List of Item	Mean	Std. Deviation
Financial institutions need to have a strong internal control to prevent a breach of customers' personal data	4.8364	.42004
Financial institutions need to constantly improve their internal control to be aligned with the current business environment	4.7273	.52545
Internal control is said to be effective if it is implemented across the company	4.4909	.87924
Internal control is effective due to its ability to prevent fraud on a timely manner	4.4727	.76629
Internal control is a companywide control measure with its tone set by the management level	4.4909	.69048
Weak internal control increases the likelihood of fraud occurring in an organisation	4.7091	.45837
Internal control is said to be weak if there is a lack of segregation of duties and poor control environment	4.5091	.57325
All Items	**4.61**	**0.6161**

Rules and Regulations

Table 3 presents the details of the descriptive statistics for all constructs of rules and regulations in descending order. The mean scores for all items related to rules and regulations range from 4.2000 to 4.7455.

Table 3
Descriptive Statistics of Rules and Regulations

List of Item	Mean	Std. Deviation
The bank's policies and procedures are tailored to its business and risk appetite	4.4182	.62925
I am aware of the Personal Data Protection Act (PDPA), which is enforced to protect customers' personal data	4.7455	.51705
I am aware of the implication of failure to comply with the PDPA	4.6182	.62334
The internal policies and procedures are periodically reviewed to meet the evolving legal and regulatory obligation	4.3455	.86534
Employees are given relevant exposure to the rules and regulations periodically	4.2000	.80277
The bank needs to meet the requirement set by the regulators in protecting customers' personal data.	4.5818	.59910
Supervision by the regulators on the internal policy is vital to ensure effective implementation of the PDPA	4.5455	.74082
All Items	**4.49**	**0.6825**

The overall mean score for rules and regulation is 4.49, indicating that the respondents basically agree on the importance of protecting customers' data. The highest standard deviation is 0.86534 for item 'The internal policies and procedures are periodically reviewed to meet the evolving legal and regulatory obligation', while the lowest standard deviation is 0.51705 for item 'I am aware of the Personal Data Protection Act (PDPA), which is enforced to protect customer's personal data'.

Technology Adoption

Table 4 presents the details of the descriptive statistics for all constructs of technology adoption in descending order. The overall mean is 4.43, indicating that the respondents agree on the importance of protecting customers' data. The highest standard deviation is 0.90825 for item 'The company has better and more sophisticated IT infrastructure to protect customers' personal data', while the lowest standard deviation is 0.51705 for item 'The company needs to invest in updating its IT infrastructure to adapt to the current challenges'.

Table 4
Descriptive Statistics of Technology Adoption

List of Item	Mean	Std. Deviation
The company has financially allocated its resources in acquiring or developing its IT system or database in ensuring protection of customers' personal data	4.3273	.77111
The company has better and more sophisticated IT infrastructure to protect customers' personal data	4.0909	.90825
The IT infrastructure within the organisation, which includes the information system, serves as a tool to detect any potential data leak	4.3273	.72148
A company with outdated technology is vulnerable to potential data breach	4.5818	.68559
The company needs to invest in updating its IT infrastructure to adapt to the current challenges	4.7455	.51705
Employees must be able to adapt and be familiar with the IT infrastructure to execute their daily task	4.5091	.74219
The company needs to ensure effective user access matrix to avoid any potential wrongdoing	4.4909	.63458
Unfamiliarity with the IT infrastructure could lead to potential customer data breach to be undetected	4.4182	.71209
All Items	**4.43**	**0.7112**

Preliminary Analyses

Table 5 shows the results of the reliability test. The results show the values of Cronbach's alpha for every factor (variable). The Cronbach's alpha for internal control, rules and regulations, and technology adoption are all above 0.80, i.e., 0.804, 0.880, and 0.864, respectively. Meanwhile, customers' data security has a value of 0.629 for Cronbach's alpha. George and Mallery (2003) interpreted the result of Cronbach's alpha as good if it is above 0.80 and questionable if it is from 0.6 to 0.69. Therefore, the results of Cronbach's alpha in this study indicate that the items or statements used could reliably measure each variable examined.

Table 5
Reliability of Construct

Variable Name	No. of Items	Cronbach's Alpha
Customers' Data Security	6	0.629
Internal Control	7	0.804
Effectiveness of Rules & Regulations	8	0.880
Technology Adoption	7	0.864

Table 6 presents the normality test for this study. The results show that the values of skewness and kurtosis for all variables in this study are in the range of -1.154 to 0.133. These values imply that the mean scores for customers' data security, internal control, rules and regulations, and technology adoption are normally distributed.

Table 6
Normality Test

Variable Name	Normality Test		
	Skewness	Kurtosis	Mean
Customers' Data Security	-1.142	0.133	4.712
Internal Control	-0.709	-0.833	4.605
Effectiveness of Rules & Regulations	-1.154	1.441	4.436
Technology Adoption	-0.765	-0.219	4.494

Pearson Correlation Analysis

A correlation analysis was conducted using the Pearson Correlation Coefficient to determine the relationship between the variables. The test results indicate a positive correlation between customers' data security and the three variables mentioned above.

Table 7
Pearson Correlation Analysis

Variables	Customers' Data Security	Internal Control	Rules & Regulations	Technology Adoption
Customers' Data Security	1.000	0.527 (0.000)	0.257 (0.000)	0.533 (0.000)
Internal Control		1.000	0.564 (0.000)	0.594 (0.000)
Rules & Regulations			1.000	0.508 (0.000)
Technology Adoption				1.000

The results indicate r = 0.527 (p = 0.000) between customers' data security and internal control, and r = 0.257 (p = 0.000) between customers' data security and effectiveness of rules and regulations. The results for the third variable, which test the correlation between customers' data security and technology adoption, show r = 0.533 (p = 0.000). In addition, as shown in the table, none of the correlation coefficients exceeds 0.80, indicating that a multicollinearity issue does not exist.

Multiple Regression Analysis

Table 8 shows the summary of the multiple regression results for the model and the statistics of its overall fit. The table shows that 36.8% of the variation in customers' data security is explained by the variation in internal control, effectiveness of rules and regulations, and technology adoption. The F-test is used for the overall significance of a multiple regression model. It shows whether or not there is a linear relationship between all of the independent variables and the dependent variable. Based on the F-value in Table 8, the model is deemed significant [$F(3,51) = 9.882$, $p < 0.001$], which implies that at least one of the independent variables has a significant linear relationship with customers' data security (dependent variable).

Table 8
Multiple Regression Results

Variables	Unstandardized Coefficient Beta	t-value	Significance
Constant	2.620	6.127	0.000
Internal Control	0.304	2.592	0.012
Rules & Regulations	-0.099	-1.110	0.272
Technology Adoption	0.252	2.660	0.010
R square (R^2) = 0.368 F-value = 9.882 Significance = 0.000			

It can also be seen in Table 8 that the p-value of internal control (p-value = 0.012) and technology adoption (p-value = 0.010) are both less than 0.05, indicating that there is evidence that internal control and technology adoption affect customers' data security at the 5% significance level (p-value = 0.05). The test results indicate that H1 and H3 are supported. Meanwhile, the effectiveness of rules and regulations returns a p-value of 0.272 (p-value > 0.05), implying that it does not significantly affect customers' data security. Therefore, H2 is not supported.

The Multiple Regression Equation is as follows:
Customers' Data Security = 2.620 + 0.304 (Internal Control) - 0.099 (Rules & Regulations) + 0.252 (Technology adoption) + e
This study examined the effect of internal control implementation in protecting customers' data security of a bank in Malaysia. The hypothesis for the first objective was 'effective internal control has a significant effect on customers' data security'. The test results

indicated a positive relationship. The results are aligned with previous studies discussed in Section 2. Ji et al. (2017) stated that establishing a high-quality internal control system has been regarded as a vital instrument to ensure high-quality financial reporting. Weak internal control can lead to material errors or even false financial disclosures. Therefore, the first objective of this study was achieved, which implied that internal control has a positive effect in protecting customers' data.

This study also showed the effect of rules and regulations on customers' data security protection. The hypothesis proposed for the second objective was 'rules and regulations have a significant effect on protecting customers' data security'. However, the test results for this objective indicated that rules and regulations do not influence customers' data security. This outcome is partially aligned with Chan and Lin (2007), which found that new regulations and policies often conflict with the employees in terms of their execution and implementation. This conflict leads to adapting to new regulations and policies being extremely challenging. This study also showed the effect of technology adoption on protecting customers' data security. The hypothesis proposed for this third objective was 'technology adoption has a positive relationship with customers' data security'. The test results indicated a positive relationship between the two variables. This outcome is aligned with Abidin et al (2017), which mentioned that having an advanced and professional system will give an incredible advantage of combining rules and profile extraction for fraud detection. Overall, the findings of the study provided evidence that internal control and technology adoption have a significant positive influence on protecting customers' data security.

Conclusion

This study was conducted due to the rise of customer data theft in the fast-changing landscape of cyberspace, where customers' data could be obtained easily. This study predicted that internal control, rules and regulations, and technology adoption have a positive influence on customers' data protection by utilising the fraud triangle theory, which incorporated factors such as pressure, opportunities, and rationalisations as the causes of fraud.

This study showed that internal control has a significant positive effect on how a bank and its employees protect its customers' data. This result is consistent with Eilifsen et al. (2017), which demonstrated that internal control is one of the major components of how an organisation meets its responsibilities as a whole. Moreover, the management of the organisation has the responsibility to design and maintain a system of internal control that provides reasonable assurance that assets and records are properly safeguarded and its information is reliable for decision making. In addition, this study showed that rules and regulations do not significantly. affect the bank and its employees in protecting their customers' data security. One possible reason could be due to new regulations and policies that are conflicting with the employees' behaviour that led them to find adapting to the new regulations and policies to be extremely challenging. Finally, this study showed that technology adoption has a significant positive effect on how the bank and its employees protect the customers' data.

This study is not without limitations. First, the scope of this study is limited to the employees of one bank only, particularly those stationed under the bank's Group Risk Division, Group Internal Audit Division, and Group Compliance Division. Hence, the findings of this study may not be generalisable to all banks in Malaysia. Future studies could extend this study to

incorporate employees from other banks. Secondly, this study used a convenient sampling technique rather than a random sampling technique, which may result in the findings not representing the entire population. Future studies may use other sampling techniques in order to make the findings more generalisable.

In summary, this study contributes to the literature on personal data protection. In particular, it provides empirical evidence on the factors that influence customers' data protection by financial institutions. The findings can assist banks and their employees in adding value to their existing processes in protecting their customers' data security.

References

Abidin, M. A. Z., Nawawi, A., Salin, P. A. S. A. P. (2019), Customer data security and theft: A Malaysian organisation's experience, *Information and Computer Security*, 27(2), 81-100

Ahlan A.R. (2015). Managing it innovation: a study of information technology implementations in Malaysia. PhD Thesis, Cardiff University, UK

Amirudin, N. R., Nawawi, A., Salin, P. A. S. A. (2017). Risk management practices in tourism industry – A case study of resort management. *Management and Accounting Review*, 16(1), 55-74.

Chalmers, K., Hay, D., Khlif, H. (2019). Internal control in accounting research: A review. *Journal of Accounting Literature*, 42(1), 80-103.

Chang, E. S., Lin, C. S. (2007). Exploring organisational culture for information security management. *Industrial Management & Data Systems*, 107(3), 438-458.

Chuah, H. (2018). Internal audit and robotic process automation. Retrieved from KPMG: https://assets.kpmg.com/content/dam/kpmg/nl/pdf/2018/advisory/internal-audit-and-robotic-process-automation.pdf

Earley, C. E. (2015). Data analytics in auditing: Opportunities. *Business Horizons*, 58(5), 493-500

Eilifsen, A., Glover, S. M., Prawitt, D. F., Abbas, M. S. Z., Nazri, S. M. S.N., Salleh, K., Johari, R. J. (2017). Principles of auditing and assurance services in Malaysia. McGraw Hill Education.

Geeta, D. V. (2011). Online identity theft - an Indian perspective. *Journal of Financial Crime,* 18(3), 235-246

Ghani, E. K., Said, J. (2010). Digital reporting practices among Malaysian local authorities. *Electronic Journal of E-Government*, 8(1), 33-44

Hassan, K. H. (2012). Personal data protection in employment: New legal challenges for Malaysia. *Computer Law & Security Review*, 28(6), 696-703

Higgins, H. N. (2012). Learning internal controls from a fraud case at Bank of China. *Issues in Accounting Education*, 27 (4), 1171–1192

Ilias, A., Ghani, E. K, Baidi, N., Abdul Rahman, R. (2020). XBRL adoption: An examination on the Malaysian business reporting system (MBRS). *Humanities and Social Sciences Letters*, 8(2), 202-214.

Janvrin, D., Bierstaker, D. J. (2008). An examination of audit information technology use and perceived importance. Accounting Horizons, 22(1), 1-21.

Jermsittiparsert, K., Ambarita, D. E., Mihardjo, L. W. W., & Ghani, E. K. (2019), Risk return through financial ratios as determinants of stock price: A study from Asean region, *Journal of Security & Sustainability Issues*, 9(1), 199-210

Ji, X. D., Lu, W., Qu, W. (2017). Voluntary disclosure of internal control weakness and earnings: Evidence from China. *The International Journal of Accounting*, 52(1), 27-44.

Karat, J., Karat, C. M., Brodiea, C., & Feng, J. (2005). Privacy in information technology: Designing to enable privacy policy management in organisations. *International Journal and Human-Computer Studies*. 63 (1–2), 153–174.

Kahyaoglu, S. B., Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*, 33(4), 360-376

Lessmann, S., Baesens, B., Seow, H. V., Thomas, L. C. (2015). Benchmarking state-of-the-art classification algorithms for credit scoring: An update of research. *European Journal of Operational Research*, 247(1), 124-136

Ali, M., Ayop, N. F., Ghani, E. K, Hasnan, S. (2020). The effect of employees' perception on internal control mechanisms towards employee fraud prevention. *Journal of Critical Reviews*, 7(18), 972-986

Ozili, P. K. (2017). Impact of digital finance on financial inclusion and stability. *Borsa Istanbul Review*,18(4), 329-340

Prince, C. (2017). Do consumers want to control their personal data? Empirical evidence. *International Journal of Human Computer Studies*, 110(1), 21-32

Raab, C., Szekely, I. (2017). Data protection authorities and information technology. *Computer Law & Security Review*, 33(1), 421–433

Roscoe, J. T. (1975). Fundamental research statistics for the behavioural sciences (2nd ed.) New York: Holt Rinehart & Winston.

Shi, W., Wang, R. (2012). Dynamic internal control performance over financial reporting and external financing. *Journal of Contemporary Accounting & Economics*, 8(2), 92-109

Spatacean, I. (2012). Addressing fraud risk by testing the effectiveness of internal control over financial reporting case of Romanian financial investment companies. *Procedia Economics and Finance*, 3(1), 230 – 235

Yusof, N. A., Ahmad, N. A., Mohamed, Z. (2016). A study on collection of personal data by banking industry in Malaysia. *Journal of Advanced Research in Business and Management Studies*, 2(1), 39–49.