Journal of Economics, Business and Market Research (JEBMR) 2024
SciTech Central Inc., USA Vol. 3(2)
733-750

PERCEPTIONS OF THREATS AND MITIGATION STRATEGIES IN COMPUTERISED ACCOUNTING INFORMATION SYSTEMS IN SRI LANKA

A L M Najimudeen*

Accountant, Ministry of Justice, Sri Lanka.

Received 07 June 2024; Revised 16 June 2024; Accepted 19 June 2024

ABSTRACT

This research investigated the perceptions of source of security threats, list of security threats and mitigation strategies in Computerized Accounting Information Systems (CAIS) among different job roles in Sri Lanka. The study focused on Executive Financial Professionals, non- Executive Financial Professionals, and IT Managers, examining their views on sources of threats, causes of risks, and preventive measures. Data analysis involved frequency distributions, ANOVA, and Kruskal-Wallis tests.

Findings revealed insights into the respondents' perspectives on the frequency and severity of threats, the causes of risks, and the effectiveness of preventive measures. Key highlights included the prevalence of man-made disasters as the primary source of risk, with power outages, outsider hackers, and employees as subsequent threats. The study emphasizes the common sharing of passwords as a major daily threat in CAIS in Sri Lanka.

The one-way ANOVA results supported significant correlations between job roles and various aspects of CAIS security, including sources of threats, actual threats, and preventive measures. Notably, viruses, outsider hackers, employees, cloud accounting, and weak internal control were recognized as significant sources of threats across different job categories. Kruskal-Wallis tests further investigate differences in the distribution of security threats and preventive measures among job roles. Varied perceptions are observed, with some threats such as viruses, outsider hackers, and weak internal control showing significant differences in susceptibility or exposure across job types.

In conclusion, the study supported the alternative hypothesis, indicating a substantial association between job roles and identified sources of risks and threats in CAIS. The findings underscore the importance of tailoring preventive measures to address the diverse perspectives within the workforce. Recommendations include enhancing training programmes, updating security protocols, and adopting cloud computing for improved CAIS security.

Keywords: Perceived security threats, Computerized accounting information system, Sources of security threats, Mitigating security threats

INTRODUCTION

The great development in information technology and its availability have led currently to an increase in the organizations'

***Correspondence to:** A L M Najimudeen, Accountant, Ministry of Justice, Sri Lanka; Tel: +94777696683; E-mail: almnajimudeen@gmail.com

dependence in their work on the computerized programs and systems in different fields and at all levels (Hanini, 2012). The evolution of computerized accounting information systems has brought about significant advancements. However, this improvement has also exposed these computerized accounting information systems to various crucial risks concerning their security and safety. Protecting information from computerized accounting systems has become a more desirable concern for organizations, recognizing it as a valuable asset. The rapid advancement in information technology, the wide spread of user-friendly software applications and the over reliance on information system by organizations to perform their operations have increased security threats to the information system which in turn have affected business activities (Abu-Musa, 2006; Salehi, 2010). Organizations implementing strong information security measures stand to reap numerous benefits, including access to accurate information, an expedited decision-making process, enhanced productivity, increased profitability, and overall growth. Boards that overlook the significance of addressing information security expose both the organization and themselves to potential risks. The organization and its board members are accountable to stakeholders, clients, and other entities that may suffer harm in the absence of a suitable information security program.

Information systems face threats that can be either intentional or unintentional, originating from internal or external sources. These threats encompass technical conditions like program bugs and disk crashes, natural disasters such as fires and floods, environmental issues like electrical surges, human factors including lack of training, errors, and omissions, unauthorized access through hacking, and the risk of viruses. Furthermore, emerging threats like business dependencies, relying on third-party communications carriers or outsourced operations are gaining significance and have the potential to lead to a loss of management control and oversight. These threats are generally classified as hardware, software, data and communication lines as well as network threats. Organizations must put in place adequate measures to ensure the protection of information assets through effective policy, controls, and standardized procedures and control testing (Muhrtala & Ogundeji, 2013).

Due to the effects of digitization of business and intense use of internet, a new epitome has emerged which is acknowledged as cloud computing (Dimitriu & Matei, 2014). Symantec Cloud SOC analysis found that 25 per cent of all shadow data (business data stored in the cloud without IT's consent or knowledge) is "broadly shared," increasing its risk of exposure. Three per cent of this "broadly shared" data is compliance related (Symantec, 2017).

It is known that there are potential security threats in using computerized accounting information system. As a result, adopting appropriate security control measures over the CAIS of an organization and its related peripherals has become an issue of concern to many organizations (Abu-Musa, 2001).

RESEARCH PROBLEM

The advancements in computer technology, and cloud computing coupled with the widespread availability of user-friendly accounting software, have prompted organizations to aspire to adopt and implement up-to-date Computerized Accounting Information Systems (CAIS).

The utilization of accounting software has notably simplified computer usage, streamlined complex tasks, and facilitated faster, more accurate, and more cost-efficient accounting processes compared to manual systems. CAIS handles both financial and non-financial transactions that directly affect the processing of financial transactions (Muhrtala & Ogundeji, 2013).

However, the adoption of this advanced technology has also introduced significant risks pertaining to the security and integrity of CAIS. It is accurate to assert that potential challenges include computer-related errors, fraudulent activities, inaccuracies in financial and non-financial information, violations of internal controls, theft, fires, and sabotage within financial and accounting records. Every organization must remain vigilant about potential security threats that could pose challenges to their CAIS and implement relevant security controls to prevent, detect, and address such breaches.

Objective of the Research

The primary goal of the research is to examine perceived security threats in CAIS through the utilization of a suggested security threat checklist. This checklist for CAIS security will be formulated by drawing upon existing literature and insights from previous studies.

Research Hypothesis

The present study seeks to explore the following research hypothesis:

- H0: There are not significant variations among individuals, both executive financial professionals and non-executive financial professionals, regarding their levels of concern related to perceived security threats that pose challenges to their computerized accounting information systems (CAIS).
- H1: There are significant variations among individuals, both executive financial professionals and non-executive financial professionals, regarding their levels of concern related to perceived security threats that pose challenges to their computerized accounting information systems (CAIS).

LITERATURE REVIEW

The rapid development of IT, availability of user-friendly accounting software and the increased competition have forced companies to adapt CAIS in order to remain competitive whereas threats to CAIS are unavoidable in the dynamic environment (Rajeshwaran & Gunawardana, 2009). There are two aspects to computer security threats; physical and electronic (Daily and Lueblfing, 2000). Physical security threats encompass natural disasters, fire damage, water damage, and power loss.

On the other hand, electronic security threats, such as computer viruses, spoofing, and network damage, are more conspicuous as they involve safeguarding data from crimes like computer viruses, data manipulation, information sabotage, and spoofing.

Loch et al conducted an important investigation in this field in 1992. The investigation involved a survey aimed at assessing the percentage of concerns among Management Information Systems (MIS) executives regarding security threats in microcomputer, mainframe computer, and network environments. The study's findings highlighted that natural disasters and unintentional actions by employees ranked as top threats through all three assessment methods. External threats accounted for 37%, while internal threats held a majority with 62.4% of weighted votes, indicating an almost 2-to-1 preference for internal threats over external ones. These results affirmed the assertions of experts that the most significant threats originate from within organizations. Furthermore, the study identified that in a microcomputer environment, the most critical perceived threats included accidental destruction of data by employees, unintentional entry of erroneous data by employees, and insufficient control over media. For mainframe computers, the top three threats were unintentional entry of erroneous data by employees, natural disasters, and accidental destruction of data by employees. In the network environment, the prominent threats comprised natural disasters, external access to systems (hack and weak points), and ineffective control measures.

In 1996, Davis undertook an investigation in Threats to Accounting Information System Security Survey. Davis' survey disclosed that 95% of respondents perceived a moderate or higher overall risk to CAIS security. Varied security risks were acknowledged across different computing environments, with microcomputers linked to external networks deemed the riskiest, while mainframes were considered the least threatened. The top threats to microcomputers included accidental data entry, data destruction, and computer viruses. Minicomputers faced issues like unauthorized data and system access, accidental data entry, and weak information system duties. Mainframes were threatened by accidental data entry, natural disasters, and unauthorized internal access.

In 1997, Ryan and Bordoloi conducted research to investigate how companies transitioning from a mainframe to a client/server environment assessed and implemented security measures to safeguard against potential security threats. The study's findings revealed that, for the two computing environments, the average rating of seven out of the fifteen potential security threats exhibited significant differences ($p = 0.05$). In each instance, the perceived risk was rated higher in the mainframe environment.

In 1997, Henry conducted a significant study to understand the nature of accounting systems and security practices. Henry aimed to gauge the alignment between theoretical concepts and actual implementation. His survey identified seven fundamental security methods for CAIS, including encryption, password access, data backup, virus protection, authorization for system changes, physical system security, and periodic

audits. The survey results indicated that 80.3% of companies backed up their accounting systems, while 74.4% implemented password security. However, only 42.7% employed virus protection measures. Less than 40% of respondents utilized physical security and authorization for system changes. Encryption was used by only 15 companies for accounting data. Nearly 45% of the sample underwent some form of audit for their accounting data.

Dr Ahmad A. Abu-Musa conducted a study in perceived CAIS within Saudi organizations. The survey results disclosed that nearly half of the surveyed Saudi organizations experienced financial losses stemming from both internal and external CAIS security breaches. Statistical findings identified the most significant perceived security threats, including the accidental and intentional entry of erroneous data, unintentional data destruction by employees, password sharing among employees, introduction of computer viruses to CAIS, suppression and destruction of output, unauthorized document visibility, and inappropriate distribution of prints and information. The recommendation is to fortify security controls in these vulnerable areas and raise awareness about CAIS security issues among Saudi organizations for enhanced protection.

In Rajeshwaran & Gunawardana, (2009) conducted an empirical examination of security controls in CAIS among selected listed companies in Sri Lanka. The study's results highlighted inadequacies in the implementation of CAIS security controls and significant variations among listed companies in terms of the sufficiency of these controls.

In Hanini, (2012) studied the risks associated with CAIS within Jordanian banks, along with the underlying reasons for these risks and potential preventive measures. The study identified several risks threatening the security of CAIS in Jordanian banks. These risks encompassed the intentional entry of inaccurate data by employees, vulnerability to viruses, unauthorized access to system outputs, and the potential impact of natural or human-induced disasters. The study highlighted a significant factor contributing to these risks-the lack of experience among bank employees in safeguarding information. This manifested in inadequate training on security measures before commencing their duties and the absence of an effective recruitment system to ensure suitable placement of individuals with the necessary skills.

In Muhrtala & Ogundeji, (2013) conducted a research in what potential threats do CAIS face due to IT deployment in business, particularly in developing economies, Nigeria. Results indicated that employees and external entities pose significant threats to information assets in computerized accounting when not adequately controlled. This underscores the importance of implementing strict authorization procedures, limiting access to authorized users based on a "need to know" basis. Additionally, management should enforce regular logging and monitoring of logical access, implement policies on segregation of duties, and maintain transaction logs for enhanced security.

Wang & He, (2013) conducted a research in analysis on the security of accounting information system in 2013. The security of a computerized accounting system is of paramount importance. Instances such as hardware system failures, software malfunctions, unexpected power outages, memory damage, computer viruses, and network attacks by hackers can jeopardize the integrity of the system. Additionally, the proficiency and diligence of the system operator contribute significantly to the overall quality of the computerized accounting system. The failure to address these issues can result in system breakdowns and the potential loss of crucial accounting data.

Bansah, (2018) studied about the threats of using CAIS in the banking industry in 2018. This study explored the susceptibility of CAIS in the banking industry in Ghana to vulnerabilities through a descriptive survey. The research investigated the sources and causes of risks affecting CAIS in financial firms, along with available preventive measures. The study identified power outages, employee-related risks, viruses, and external threats as the most concerning sources of threats to CAIS. Regarding the causes of risks, findings highlighted issues such as accidental entry of erroneous data, unauthorized copying of system output, infrequent backups, outdated security software, unauthorized data access, internal control weaknesses, and absence of written policies as major contributors to CAIS threats.

In Kuczynska Cesarz, (2021) conducted a research in Selected areas of threats to the security of accounting information system. The study highlighted the extensive reliance on computer programmes to support accounting systems significantly contributes to the vulnerability of accounting information, despite the regulatory safeguards in place. While it is currently inconceivable to manage companies' finances without modern technological solutions, it is crucial to remain cognizant of the potential downsides associated with digitization, which is an integral aspect of cyberspace. Recognizing these challenges is essential for navigating the future development of entities in the context of an increasingly digitized landscape.

In Semlambo, Mfoi & Sangula, (2022) did a research in Information Systems Security Threats and Vulnerabilities: A Case of the Institute of Accountancy Arusha (IAA). The findings highlighted key factors impacting the security of information systems at IAA, encompassing human factors, policy-related issues, work environment considerations, and demographic factors.

RESEARCH METHODOLOGY

The research utilized a questionnaire survey, focusing on listed firm’s Sri Lanka. Five hundred and seventy questionnaires have been randomly distributed among different type of listed firms in Sri Lanka. Data were collected from two key groups within each firm: the group head of finance or divisional head of the financial department and the staffs who works in finance department.

Data from the targeted respondents was obtained through self-administered questionnaires. Aligned with the study's objectives and the relevant literature, the questionnaire items primarily comprised close-ended questions. The nature of these items was structured using a six-point Likert scale, with response options ranging from never to more frequently or daily (never, less than once a year, once a year to monthly, once a month to week, once a week to daily and more frequently or daily). The questionnaire items were categorized into four sections: respondent job was divided into three parts IT Manager, Executive and Non- Executive, sources of risks threatening CAIS, causes of risks affecting CAIS, and preventive measures.

The study distributed 570 questionnaires to eligible participants employed in the listed firms in Sri Lanka. These surveys were disseminated through a combination of email communication and personal interactions to encourage substantial responses from the targeted population and staff members. A total of 303 respondents were sent back filled questionnaires, resulting in a noteworthy 53 per cent of initial response rate. However, 47 incomplete questionnaires were not included in the data analysis. The study concluded with 256 valid and usable questionnaires, reflecting a 45 per cent response rate. This response rate is deemed high for empirical surveys of this nature. A reliability test using the Alpha Cronbach model has been conducted on the questionnaire to investigate its internal consistency of questions and responses from respondents.

The data collected for this study underwent analysis using the Statistical Package for the Social Sciences (SPSS. Descriptive statistics, including frequencies and percentages, were employed to identify key characteristics within the research variables. Additionally, non- parametric tests, specifically the Kruskal-Wallis test and one-way ANOWA, were utilized to examine and assess the research hypotheses.

DATA ANALYSING

The reliability test outcome indicated in the **Table 1** that the questionnaire design is highly dependable. Furthermore, the collected data concerning the frequency of CAIS security threats in Sri Lankan, both executive financial professionals and non-executive financial professionals demonstrates high reliability and consistency (Cronbach's Alpha = 0.81).

Table 1. Reliability Statistics.

Cronbach's Alpha	N of Items
.806	39

Descriptive Analysis

As **Table 2** pointed out, 71 respondents were Executive Financial Professionals, 119 respondents were Non-Executive Financial Professionals and 66 respondents were IT Managers.

Table 2. Type of Job.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Executive	71	27.7	27.7	27.7
	Non-Executive	119	46.5	46.5	74.20
	IT Managers	66	25.8	25.8	100.00
	Total	256	100.0	100.0	

The findings presented in **Table 3** regarding source of risks in CAIS suggested that many respondents perceived Man-Made Disasters as the primary source of risk in CAIS in Sri Lanka. Power Outages, threats from outsider hackers, and employees were identified as the subsequent sources of threats to CAIS. Viruses, Cloud Accounting, and Weaknesses in Internal Control were considered lesser sources of threats in CAIS. Interestingly, Natural Disasters was reported as never being a source of threat to CAIS in Sri Lanka.

Table 3. Sources of Risks that Threaten in CAIS.

No	Source of Risk	Mode	Std. Deviation	Meaning
01	Power Outages	3	.545	Once a Year to Monthly
02	Viruses	2	1.154	Less than Once a Year
03	Natural disasters	1	.458	Never
04	Threat from Outsiders Hackers	35	.427	Once a Year to Monthly
05	Employees	3	.527	Once a Year to Monthly
06	Man-Made Disaster	4	1.137	Once a Month to Week
07	Cloud Accounting	2	1.156	Less than Once a Year
08	Weak internal control	2	1.173	Less than Once a Year

The results revealed in **Table 4** regarding the causes of risks threatening CAIS in Sri Lanka indicated that Intentional Damage of Files by Employees, Intentional Entry of Viruses, Suppression or Destruction of Output, and Sharing Information in Cloud Accounting were reported as never posing a threat to CAIS in Sri Lanka, Making Unauthorized Copies of System Files, and Unintentional Entry of Virus occurred the Less than Once a Year, Bad Data Entered Intentionally by Employee, Delay due to Miscommunication between MIS and Accounting Department, Not

Frequently updating System Security, Inappropriate Firewall/Antivirus, Lack of Standard Protocols and Policies , Weakness In Internal Control, System Fail or System Slow , and Theft of Data and Information were reflected as Once a Year to Monthly, Bad Data Entered Unintentionally by Employees, Unintentional Damage of Files by Employees, Lack of Frequent Backups, Access to Data by Unauthorized Personnel, Lack of Training, and Delaying in Updating Information on Another Server were reported to occur once a month to weekly. Remarkably, the Common Sharing of Passwords was identified as a major threat in CAIS in Sri Lanka, occurring daily among financial professionals in the country.

Table 4. Causes Contributing to the Risks that Threaten CAIS.

No	Threats	Mode	Std. Deviation	Meaning
1.	Bad Data Entered Unintentionally by Employee	4	.526	Once a Month to Week
2.	Making Unauthorized Copies of System Files	2	.716	Less than Once a Year
3.	Bad Data Entered Intentionally by Employee	3	.697	Once a Year to Monthly
4.	Unintentional Entry of Virus	2	1.156	Less than Once a Year
5.	Delay due to Miscommunication between MIS and Accounting Department	3	.557	Once a Year to Monthly
6.	Unintentional Damage of Files by Employees	4	.724	Once a Month to Week
7.	Intentionally Damage of Files by Employees	1	1.658	Never
8.	Intentional Entry of Virus	1	1.338	Never
9.	Lack of Frequent Back-ups	4	.583	Once a Month to Week
10.	Not Frequently updating System Security	3	1.053	Once a Year to Monthly
11.	Access to Data by Unauthorized Personnel	4	.838	Once a Month to Week
12.	Inappropriate Firewall/Antivirus	3	.535	Once a Year to Monthly
13.	Common Share of Password	5	1.157	More Frequently or Daily
14.	Lack of Training	4	.624	Once a Month to Week
15.	Lack of Standard Protocols and Policies	3	.493	Once a Year to Monthly
16.	Weakness in Internal Control	3	.429	Once a Year to Monthly
17.	Suppression or Destruction of Output	1	.557	Never
18.	Theft of Data and Information	3	.730	Once a Year to Monthly
19.	System Fail or System Slow	3	1.333	Once a Year to Monthly
20.	Delaying in Updating Information in Another Server	4	.719	Once a Month to Week
21.	Sharing Information in Cloud Accounting	1	.429	Never

The results displayed in **Table 5** outline preventive measures against threats to CAIS in Sri Lanka. Financial professionals indicated that their organizations undertake precautionary measures every day or more frequently to mitigate threats to CAIS in Sri Lanka. Appropriate Use of

Firewalls and Antivirus, Regular Backups for System Files, and the Implementation of Cloud Computing were identified as more frequent practices by organizations to mitigate security threats to CAIS in Sri Lanka. Prohibiting the Common Sharing of Passwords, Ensuring Frequent Antivirus Updates, Providing Adequate Training for Employees, Maintaining Strong Internal Control, and Ensuring the Effectiveness of Internal Auditing Activities were reported to occur once a month to weekly. Disciplinary Action Against Employees Involved in Fraudulent Activities was noted to happen less than once a year.

Table 5. Mitigating Features to Threats in CAIS.

No	Preventing Feature	Mode	Std. Deviation	Meaning
1.	Common Share of Password is not Allowed	4	1.038	Once a Month to Week
2.	There Is Appropriate Firewalls and Antivirus	5	.623	More Frequently or Daily
3.	Antivirus Is Updated Frequently	4	.329	Once a Year to Monthly
4.	Employees are Adequately Trained	4	.429	Once a Month to Week
5.	There Is Strong Internal Control	4	1.341	Once a Month to Week
6.	Internal Auditing Activities are Effective	4	1.022	Once a Month to Week
7.	There is Frequent Backups for System Files	5	.708	More Frequently or Daily
8.	Disciplinary Action Again Employees Who Made Fraud	2	.709	Less than Once a Year
9.	Cloud Computing	5	.427	More Frequently or Daily

Testing Research Hypothesis

The outcomes from the one-way ANOVA, as per Appendix 1, demonstrated significant correlations between distinct types of job holders

and various sources of threats to CAIS, causes of threats to CAIS, and mitigation actions for threats to CAIS.

Source of Threats to CAIS

Viruses, Threat from Outsiders Hackers, Employees, Cloud Accounting, and Weak internal Control were significantly most recognized sources of threats to CAIS in Sri Lanka.

Threats to CAIS in Sri Lanka

Making Unauthorized Copies of System Files, Bad Data Entered Intentionally by Employee, Unintentional Entry of Virus, Suppression or Destruction of Output, Unintentional Damage of Files by Employees, Intentionally Damage of Files by Employees, Lack of Frequent Back- ups, Common Share of Password, Lack of Training, Weakness in Internal Control, Theft of Data and Information, and Sharing Information in Cloud Accounting were considered the most prominently perceived significant threats to Computerized Accounting Information Systems (CAIS) in Sri Lanka.

Preventive Measures for Ensuring the Security of CAIS

Antivirus is Updated Frequently, Employees Are Adequately Trained, Internal Auditing Activities Are Effective, There Is Frequent Backups for System Files, and Cloud Computing were significantly implemented mitigation measures to diminish the perceived threats to CAIS in Sri Lanka.

In conclusion, the research strongly supports the alternative hypothesis, signifying a substantial association with the identified sources of risks for CAIS among different kind of job holders. These sources include viruses, outsider hackers, employees, cloud accounting, and weak internal control. Similarly, in the context of threats to CAIS, the alternative hypothesis is significantly accepted, particularly for unauthorized copying of system files, intentional and unintentional data manipulation, virus entry, output suppression or destruction, file damage by employees, lack of backups, password vulnerabilities, insufficient training, and weaknesses in internal control among executive and non-executive financial professionals, as well as IT Staffs.

The study underscored the significance of accepting the alternative hypothesis in proposing preventive measures to enhance CAIS security among different employment role. These measures include frequent antivirus updates, employee training, effective internal auditing, regular backups, and the adoption of cloud computing.

Kruskal-Wallis Test

Source of Threats to CAIS

The results were from Independent-Samples Kruskal-Wallis Tests conducted to assess potential differences in sources of threat to CAIS across different job categories.

Power Outages

The analysis indicated that there was no statistically significant difference in the distribution of power outages among the various job categories. This finding suggested that, for the studied population, the incidence of power outages is relatively consistent across different job types.

Viruses

The research revealed a statistically significant difference in the distribution of viruses across different job categories. This implied that there were variations in the susceptibility or exposure to viruses among individuals with different job roles.

Natural Disasters

The results suggested that there was no significant (p value. 143) difference in the distribution of natural disasters across job categories. This implied that, within the studied population, individuals from various job types experience similar levels of exposure or vulnerability to natural disasters.

Threat from Outsiders (Hackers)

The analysis indicated a significant (p value .000) difference in the perceived threat from outsiders (hackers) across different job categories. This finding suggested that certain job roles might be more prone to cyber security risks or perceive a higher level of threat from external sources.

Employees

The study revealed a significant (p value .897) difference in the distribution of employees across job categories. This suggested that the composition or characteristics of the workforce vary significantly among different job types.

Man-Made Disaster

The analysis indicated no significant (p value .297) difference in the distribution of man-made disasters among different job categories. This implied that, within the studied population, individuals across various job roles experience a similar level of exposure or susceptibility to man-made disasters.

Cloud Accounting

The research identified a significant (p value .003) difference in the distribution of cloud accounting across job categories. This suggested that individuals in different job roles might have varying levels of involvement or reliance on cloud accounting technologies.

Weak Internal Control

The study revealed a significant (p value .002) difference in the distribution of weak internal control across job categories. This implied that certain job roles may be more susceptible to issues related to internal

control weaknesses, warranting further investigation into the specific contributing factors.

The research revealed a statistically significant difference in the distribution of Viruses, Threat from Outsiders Hackers, Employees, Cloud Accounting, and Weak Internal Control across different job categories. This implies that there are variations in the susceptibility or exposure to source of threats to CAIS among individuals with different job roles.

Threats to CAIS in Sri Lanka

In the context CAIS, Independent-Samples Kruskal-Wallis Tests were conducted to analyze the distribution of certain security-related issues across different categories of job types. The results were summarized as follows:

Bad Data Entered Unintentionally by Employee

There was no statistically significant (p value .451) difference in the distribution of instances where bad data was entered unintentionally by employees across various job types.

Making Unauthorized Copies of System Files

There was a statistically significant (p value .000) difference in the distribution of unauthorized copies of system files among different job types.

Bad Data Entered Intentionally by Employee

No significant (p value .897) difference was found in the distribution of instances where bad data was intentionally entered by employees across various job types.

Unintentional Entry of Virus

There was a statistically significant (p value .001) difference in the distribution of unintentional entry of viruses across different job types.

Delay due to Miscommunication between MIS and Accounting Department

No statistically significant (p value .187) difference was observed in the distribution of delays attributed to miscommunication between Management Information Systems (MIS) and the Accounting Department across various job types.

Unintentional Damage of Files by Employees

There was a statistically significant (p value .000) difference in the distribution of instances where files were unintentionally damaged by employees across different job types.

Intentionally Damage of Files by Employees

There was a statistically (p value .010) significant difference in the distribution of instances where files were intentionally damaged by employees across different job types.

Intentional Entry of Virus

No statistically significant (p value .805) difference was found in the distribution of intentional entry of viruses across various job types.

Lack of Frequent Back-ups

There was a statistically (p value .000) significant difference in the distribution of instances where there was a lack of frequent data backups across different job types.

Not Frequently updating System Security

No statistically significant (p value .819) difference was observed in the distribution of cases where system security is not frequently updated across various job types.

Distribution Access to Data by Unauthorized Personnel

There was not enough evidence to conclude that there were significant (p value .209) differences in the distribution of unauthorized access across job types.

Distribution Inappropriate Firewall/Antivirus

Although the p-value .064 was lose to the significance level, you retain the null hypothesis, suggesting no significant differences in the distribution of inappropriate firewall/antivirus issues across job types.

Distribution Common Share of Password

There was strong evidence to suggest that the distribution of common sharing of passwords differed significantly across job types at the P Value of .000.

Distribution Lack of Training

The distribution of lack of training significantly (p value .000) differs across job types.

Distribution Lack of Standard Protocols and Policies

There is not enough evidence to suggest significant (p value .327) differences in the distribution of lack of standard protocols and policies across job types.

Distribution Weakness in Internal Control

The distribution of weaknesses in internal control significantly (p value .000) differed across job types.

Distribution Suppression or Destruction of Output

The distribution of suppression or destruction of output significantly (p value .000) differed across job types.

Distribution Theft of Data and Information

The distribution of theft of data and information significantly (p value .000) differed across job types.

Distribution System Fail or System Slow

There is evidence to suggested that the distribution of system fail or system slow differs significantly (p value .037) across job types.

Distribution Delaying in Updating Information in Another Server

The distribution of delaying in updating information in another server significantly (p value .035) differed across job types.

Distribution Sharing Information in Cloud Accounting

The distribution of sharing information in cloud accounting significantly (p value .000) differed across job types.

Outcomes indicated from Independent-Samples Kruskal-Wallis Tests conducted to evaluate perceived security threats to CAIS among different job categories. The finding pointed out a statistically significant difference in the spreading of Making Unauthorized Copies of System Files, Bad Data Entered Intentionally by Employee, Unintentional Entry of Virus, Suppression or Destruction of Output, Unintentional Damage of Files by Employees, Intentionally Damage of Files by Employees, Lack of Frequent Back-ups, Common Share of Password, Lack of Training, Weakness In Internal Control, Theft of Data and Information, and Sharing Information in Cloud Accounting among different job groups.

Preventive Measures for Ensuring the Security of CAIS

Common Share of Passwords was not Allowed

The high p-value (.771) suggests that there was no statistically significant difference in the distribution of responses regarding the common sharing of passwords across various job categories. Therefore, you retain the null hypothesis. In practical terms, it implies that perceptions of the common sharing of passwords are similar across different job types.

Appropriate Firewalls and Antivirus

The low p-value (.037) indicated a statistically significant difference in the distribution of responses regarding the presence of appropriate firewalls and antivirus across different job categories. Thus, reject the null hypothesis. This suggested that there were variations in perceptions regarding the adequacy of firewalls and antivirus protection among different job roles.

Antivirus Update Frequency

A very low p-value (.000) signifies a significant difference in the distribution of responses concerning the frequency of antivirus updates across job categories. Rejecting the null hypothesis suggested that employees in different job roles had varied opinions on how frequently antivirus updates should occur.

Employee Training Adequacy

The low p-value (.000) indicated a statistically significant difference in the distribution of responses regarding the adequacy of employee training across different job categories. Rejecting the null

hypothesis put forward that there were variations in perceptions regarding the sufficiency of training among employees in different roles.

Strong Internal Control

The p-value of .007 pointed out a statistically significant difference in the distribution of responses regarding the existence of strong internal control across job categories. Therefore, you reject the null hypothesis. This implied that there were differences in perceptions regarding the strength of internal controls among employees in different job roles.

Effectiveness of Internal Auditing Activities

The very low p-value (.000) sated a significant difference in the distribution of responses regarding the effectiveness of internal auditing activities across job categories. Rejecting the null hypothesis said that employees in different job roles had varied opinions on the effectiveness of internal auditing.

Frequent Backups for System Files

A low p-value (.000) specified a statistically significant difference in the distribution of responses concerning the frequency of backups for system files across job categories. It is rejecting the null hypothesis proposed that employees in different roles perceive the need for backups differently.

Disciplinary Action Against Fraudulent Employees

The p-value of .017 signified a statistically significant difference in the distribution of responses regarding disciplinary action against employees involved in fraud across job categories. Rejecting the null hypothesis suggested that perceptions of the need for disciplinary action vary among different job roles.

Cloud Computing Usage

The low p-value (.037) showed a statistically significant difference in the distribution of responses regarding the use of cloud computing across job categories. Therefore, the research accepted alternative hypothesis. This suggested that employees in different roles have varying opinions on the adoption of cloud computing.

In summary, these results highlight that perceptions to mitigate security threats differed significantly among employees with different job roles. This information can be valuable for organizations aiming to tailor their security measures, training programs, and policies to better align with the diverse perspectives within the workforce.

CONCLUSION AND RECOMMENDATION

Many organizations seek to implement computer-based accounting systems to enhance efficiency, accuracy, operational cost-effectiveness, and ease compared to manual systems. However, the realization of these benefits is sometimes hindered by security threats in

CAIS, which can vary across different roles (IT Staffs, Executive and Non- Executive Financial Professional.

This study aimed to highlight the significant differences in the frequency of source of security threats, the occurrence of security threats and mitigating action for security threats to CAIS. The results of both Kruskal-Wallis and one-way ANOVA tests indicated that, for the most part, there were significant differences among various job roles. However, some of variables, such Bad Data Entered Intentionally by Employee, Power Outages, Natural disasters Man- Made Disaster same categories, Bad Data Entered Unintentionally by Employee Man-Made, Delay due to Miscommunication between MIS and Accounting Department, Intentional Entry of Virus, Lack of Frequent Back-ups, Not Frequently updating System Security, Access to Data by Unauthorized Personnel , Lack of Standard Protocols and Policies Distribution Common Share of Password Is not Allowed were not significantly differed among various roles in CASI in Sri Lanka. It is imperative for every organization to prioritize the implementation of effective measures to mitigate threats to their computerized accounting information systems (CAIS).

Furthermore, there is potential for future research to expand beyond the scope of this study. Areas for additional investigation could encompass various levels of experience among individuals, diverse accounting software systems, and comparisons of security threats between countries, such as developed and developing nations.

REFERENCES

Abu-Musa, Ahmad, A. (2006). Evaluating the Security Controls of CAIS in Saudi organizations The Case of Saudi Arabia, *The International Journal of Digital Accounting Research*, *6*, 25-64.

Al Musa Ahama, A. (2001). Evaluating the Security threat of Computerized Accounting System. *The journal of American Academy of Busines*s, *9*, 9-30.

Bansah, E.A. (2018). The threats of using computerized accounting information systems in the banking industry. *Counting and Management Information Systems, 17*, 440-461.

Bansah E.A. (2018). The threats of using computerized accounting information systems in the banking industry, *Accounting and Management Information Systems*, *17*, 440-461.

Bercht, David & Martin, Male. (1996). Accounting Information System Ninth edition publication by Accounting horizons, 215-230.

Collins, Cartons J, (2000), How to Select the Right Accounting Software. *Journal of Accountancy*, 67-77.

Davis, Charles E, (1996). An Assessment of Accounting Information Security. *Journal of CPA*, 28-35.

Dimitriua O, Matei M, (2014). A New Paradigm for Accounting through Cloud Computing. *Procedia Economics and Finance, 15,* 840-846.

Ghazvini, A. Shukur, Z, (2016). Awareness Training Transfer and Information Security Content Development for Healthcare Industry. *International Journal of Advanced Computer Science and Applications, 7,* 361-370.

Greene, G. (2010). Assessing the Impact of Security Culture and the Employee-Organization Relationship on IS Security Compliance I. 5th Annual Symposium on Information Assurance, Albany, pp: 16-17.

Hanini E.A. (2012). The Risks of Using Computerized Accounting Information Systems in the Jordanian banks their reasons and ways of prevention. *European Journal of Business and Management*, *4*, 53-63.

Humaidi, N. & Balakrishnan, V. (2015). The Moderating Effect of Working Experience on Health Information System Security Policies Compliance Behavior. Malaysian *Journal of Computer Science*, pp: 70-92.

Jo Ann C, Carland (2001). Computer Security A Strategic Concern of Business Accounting Journal Publication by University of Tennessee at Martin.

Kagwiria, C. (2020). Cyber Security Skills Gap in Africa African Advanced Level Telecommunications Institute Nairobi.

Kuczyńska-Cesarz A. (2021). Selected areas of threats to the security of accounting information system, nżynieria. *Bezpieczeństwa Obiektów Antropogenicznych, 3,* 37-49.

Loch, K. D., Houston H. C., & Warkentin, M.E. (1992). Threats to Information Systems Todays Reality Yesterdays Understanding. *MIS Quarterly, 16(2),* 173-186.

Luehlfing, M. S., Daily, C. M., Philips Jr, T. J., & Murphy Smith, L. (2000). Defending the Security of the Accounting System. *The CPA Journal*, 62-65.

Lynn Hoffman. (2001). Security threats on Small Business Organization published by University of Colarado, pp: 1-15.

Mitra, T., & Gilbert, E. (2012). Have You Heard How Gossip Flows Through Workplace Email? Proceedings of the 6th International AAAI Conference on Weblogs and Social Media Dublin, pp: 242-249.

Muhrtala, T.O, & Ogundeji, M. (2013) Computerized Accounting Information Systems and Perceived Security Threats in Developing Economies the Nigerian Case, pp: 9-18.

Rajeshwaran, N. & Gunawardana, K. D. (2009). An Empirical Investigation of the Security Controls of Computerized Accounting Information Systems in the Selected Listed Companies in Sri Lanka, *Journal of Finance University of Sri Jayewardenepura*.

Ryan, S. D. & Bordoloi, B. (1997). Evaluating Security Threats in Mainframe and Client Server Environments. *Information & Management, 32*, 137-142.

Salehi, M. (2010). Usefulness of Accounting Information System in Emerging Economy: Empirical Evidence of Iran. *International Journal of Economics and Finance*, *2*, 186-195.

Semlambo, A. A, Mfoi, D.M, & Sangula, Y. (2022). Information Systems Security Threats and Vulnerabilities A Case of the Institute of Accountancy Arusha (IAA). *Journal of Computer and Communications*, 29-43.

Symantec (2017). Internet security threat report" Mountain View CA Symantec Corporation United States General Accounting Office (GAO) (2003). Information Security Computer Controls Over Key Treasury Internet Payment System Report to Congressional Requesters.

Wang, Y. (2012). Research on Security of Accounting Information System in the Era of Big Data. *Journal of Physics: Conference Series*, 1-6.

Watters, P.A. & Ziegler, J, (2016). Controlling Information Behavior: The Case for Access Control. *Behavior & Information Technology*, 268-276.

Weiter, James A, (1987). Computer, Business, and Security 2nd Edition Butterworth Publisher.