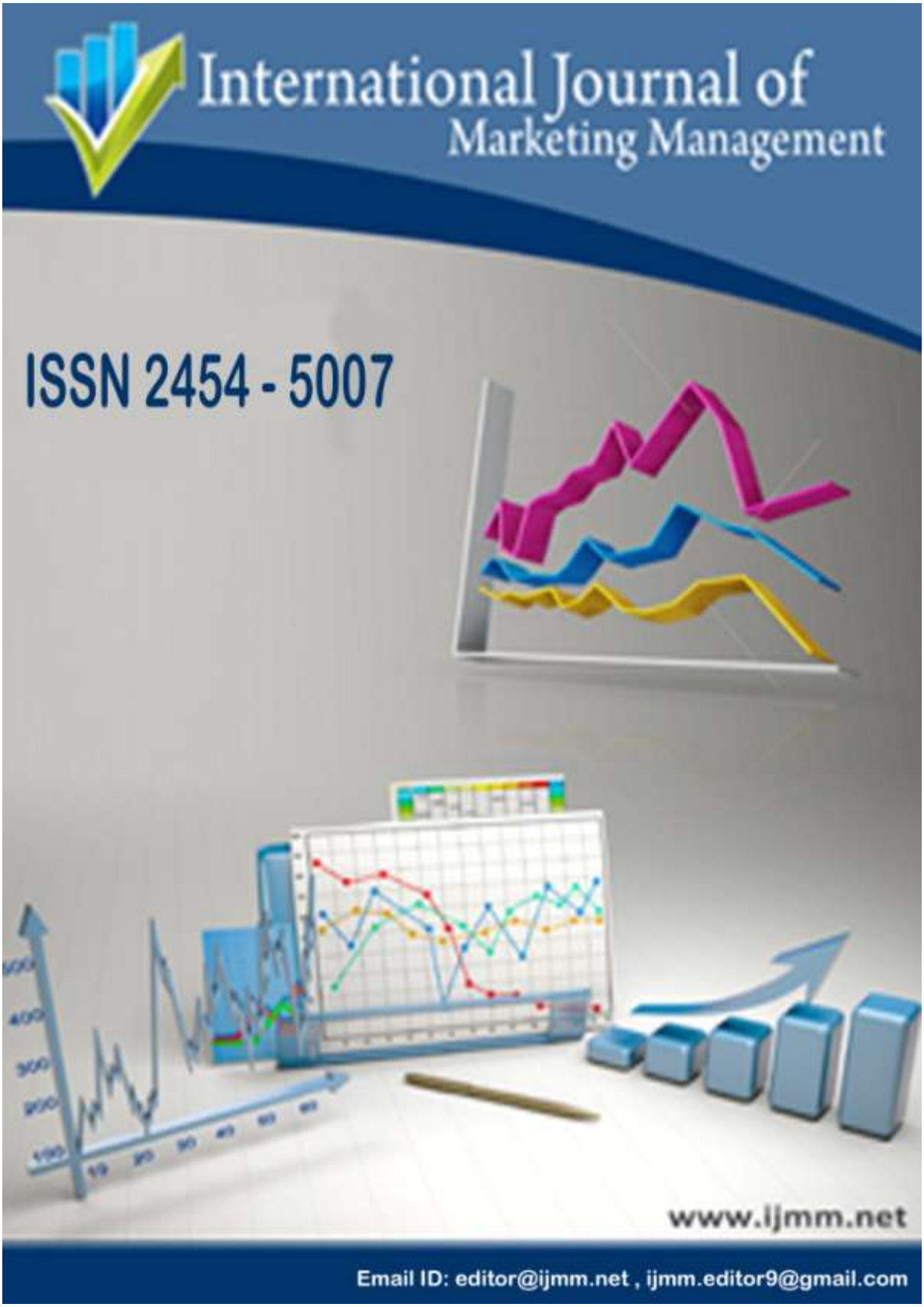
International Journal of
Marketing Management
ISSN 2454 - 5007
www.ijmm.net
Email ID: editor@ijmm.net , ijmm.editor9@gmail.com

International Journal of Marketing Management

ISSN 2454-5007, www.ijmm.net

Vol. 9 Issuse. 2,May 2021

IMPACT OF COMPUTERIZED ACCOUNTING PRACTICES OF SMALL BUSINESS IN THANJAVUR DISTRICT

T.Surulipal Dr.K.Baranidharan

Abstract: Financial and non-financial transactions that have an impact on the flow of money are handled by CAIS, a computerised system. For example, if a client's next of kin and/or address have been updated, this information is critical for future sales to that customer. Systems and software acquisition and implementation have become increasingly common as a result of the widespread adoption of user-friendly systems, as well as a desire to automate business processes. This has led organisations to acquire and implement systems and software in the form of turnkey systems, backbone systems, vendor-supported systems, and ERP systems. Commercial packages are becoming more sophisticated, thanks to technological advancements that have moved them away from the simplicity of in-house manufacture and distribution. There are many factors that have pushed businesses to use accounting software, such as the rise of commercial software that is less expensive than custom-built software; the emergence of industry-specific vendors who target their software to the needs of specific businesses; the growing demand for software by businesses; and

Introduction

the trend toward downsizing of organisational units and the move toward distributed data processing environments. Since then, accounting activities have been considerably simpler, quicker, and more precise.

A major benefit of using this poll is that it presents a pattern that can be used to compare results throughout the globe. These findings led to the employment of standard statistics, descriptions, and other analytical tools in the investigation of CAIS's most problematic threats. We gathered formal information from corporations in order to determine the most important aspects connected to CAIS risks. For strategic choices based on our suggestions, we'll take into consideration these elements.

Review of literature

Loch et al. conducted one of the most significant research in this field (1992). In order to better understand the security concerns in microcomputer, mainframe computer, and network systems, researchers performed a survey. An empirical study was conducted on a set of twelve potential security risks. Natural calamities; personnel mistakes (poor entry) were found to be to blame for the findings.nadequate management of media and unauthorised access to CAIS by hackers were among the top security dangers, as were theft and loss of information (including personal data).

Research Scholar Research Advisor
PG and Research Department of Commerce, Maruthupandiyar College Thanjavur -613 403

End-user mistakes may be minimised, and security measures applied more effectively, thanks to Siponen's (2000) conceptual framework for an organization's security awareness programme. Siponen (2000) stated that end-user abuse, misinterpretation, non-use, or improper implementation of information security approaches or processes renders them useless.

Hermanson et al. (2000) used a questionnaire to conduct an exploratory study to better understand how firms deal with their IT risks and how internal auditors evaluate those risks. An internal audit's primary emphasis is on conventional IT risks and controls, such as the protection of IT assets, data processing and data integrity and privacy.

Abu-Musa (2001) conducted a study in Egypt's banking industry to examine the security vulnerabilities posed by CAIS (EBS). A self-administered questionnaire with 19 CAIS security risks was used to poll the full population of the EBS (sixty-six bank headquarters). According to the study's statistical findings, the most significant security threats to CAIS in the EBS are: employee error in data entry, employee error in data destruction, virus introduction to the system, natural and human-made disasters, employee error in password sharing, and employee error in printing and distribution of information to those not entitled to receive it.

Use Abu-CAIS Musa's security threats list in this research to analyse the key perceived security dangers that CAIS faces in Saudi Arabian society. " CAIS security measures in financial institutions, such as banks, securities firms, and insurance companies, were examined by Coffin and Patilis (2001). According to the researchers, internal auditing is a valuable tool for detecting and analysing the security measures that are in place for the collection, use, and access of client information.

Over two hundred US organisations were questioned by White and Pearson (2001) to learn about the security measures in place to protect personal computer usage, email account management, and the safety of corporate data. According to the findings of the research, most of the questioned organisations need to improve their security controls. Computer technology has been used by a large number of organisations without adequate protections in place, according to the findings.

In Australia, the United Kingdom, and the United States, a study was conducted by Warren (2002) to look at computerised information system security procedures. The purpose of this research report was to examining security methods from several angles and determining if they vary from nation to country. Australian businesses have low levels of computer security, according to a recent report. Many of the security issues were discovered as a result of inadequate security processes. 45 percent of firms didn't budget for computer security, according to the findings.
There was no information security policy for 42% of UK firms. In addition, the study found that almost half of all firms cited financial restrictions as a barrier to computer security implementation.

While in the United States, the greatest money was lost due to identity theft and other forms of financial fraud. Differences between internal and external CAIS abusers were not substantial, however. US security policies seem to be more successful than those in Australia or the UK, according to the study

According to the research, non-economic performance should also be included in the reporting of Intellectual Capital (IC). An Extended Performance Reporting Framework was used to undertake a content study of the annual reports of selected Australian mining corporations to investigate voluntary reporting methods. Sample firms tended to put higher emphasis on intellectual capital (IC) data than non-economic performance data, according to the findings of the research.

The study's goal was to raise awareness among researchers and management of some of the AIS-related concerns about systems' resilience and flexibility in the face of rapidly changing environments. Paper based on a postal survey of Greek SME Chief Information Officers participating in AIS development/acquisition gives a snapshot of current trends. Findings from an extensive pilot study on the development and acquisition processes of Accounting Information Systems (AIS) by a sample of Greek enterprises were summarised in this article. As a result of globalisation and new business paradigms, organisations worldwide have come to recognise that traditional AIS systems are inflexible. Replacement prices are prohibitive for many organisations, yet they are necessary to stay competitive in today's market.

Between 1995 and 2001, the 22 returns model (Easton; Pae, 2003) was used to evaluate the valuation implications of conservatism in the oil and gas sector and accounting method choice. Accounting in the oil and gas business is, on average, impartial with regard to accounting regulations, but cautious when it comes to investments in projects with positive net present value, according to the research findings. The study's findings also indicated that in a situation where there is a lot of noise, it might be difficult for people

No matter what technique of accounting is used, security prices aren't affected because of the laws governing the business.

Analysis of the British Gas industry's external accountability and accounting changes from 1986 to 1998 has been offered in this article. When the British nationalised gas firm was turned into a private enterprise, several changes occurred. Those changes were mostly in the areas of public, commercial, and competitiveness. for which in-depth research was carried out.

The study's scope

Since most firms are increasing their IT expenditures, this trend will continue. In addition, the cost of information is under pressure due to current economic circumstances and competitiveness. In most cases, an information system is built utilising information technology to help a person with their work. In order to enhance decision-making, communication, and knowledge management, many businesses are establishing information systems. The accounting information system is the most important aspect of an organization's information system essential for making decisions.

Hunton, (2002) looked at the link between an automated accounting information system and an organization's efficiency and productivity. According to his findings, there was a direct link between an organization's accounting information system and its overall effectiveness. To compare and contrast the various accounting systems. Organizational tactics and performance were examined by Chang, Y. W. (2001). Research shows firms often change the AIS design to fit their chosen strategic direction because they understand that AIS may help with strategy management and improve overall performance (Chang, 2001).

The study's goals.

To examine the effectiveness of the chosen organisations' accounting information systems

To find out how much of the SSI's accounting information system divisions use advanced technology.

SSI that do not already use advanced systems may be able to replace them with systems that are more advanced.

Analyze the credentials and experience of the staff in order to determine their level of proficiency with cutting-edge technology.

Analyze and give suggestions for improvements to the security and accounting policies and practises at such firms.

Research Methodology

Here, the researcher explains how he came up with the technique he used, as well as the significance, purpose of the study, issue, and study hypotheses.

Accounting information systems used by small businesses are based on cutting-edge technology.

The firms' contemporary accounting information systems are managed by highly-skilled workers.

To guard against potential attacks to their accounting information systems, the corporations have implemented elaborate security measures.

The businesses adhered strictly to the requirements of the IFRS (AIS).

The data's origins

Since this is an empirical research, we will treat the original materials as if they were a questionnaire. Observation and interviewing. As a result, the prior research, journals, and reference materials were evaluated in accordance with the study's theoretical criteria.

Compilation of Information

Grouped into numerous working industries, respondents in Thanjavur ranged from manufacturing to retail merchandising to wholesale merchandizing. As a result, internal auditors, staff accountants, IS auditors, financial people, and IT experts were added to the list of professions to be reclassified. To provide an accurate representation of each demographic group, a random sample of forty (40) people was selected.

Analyzed Information

Response groups in the SSI in Thanjavur District do not see any major differences in the prevalence of security risks to CAIS, according to H01. For this study, 19 questionnaire questions were used to divide respondents into five (5) categories, each of which had a correlation to this hypothesis.

The hypotheses' conclusions are as stated.

It was out that the F-ratios for the first two assertions used to validate the claim that respondents' perceptions differed had p-values greater than 0.05, i.e. 0.338 and 0.835, with p-values of 1.144 and 0.363, respectively. There are no significant variations between groups in terms of how they see workers entering poor data when using CAIS's, as a result of this study. F-ratios of 3.038 and 5.645, p-values of 0.019 and 0.000, both less than 0.05, characterise the final two assertions in the table. As a result, we find that there are considerable variances.

the view of respondents in regard to accidental and deliberate data erasure by firm workers. It's possible that firms have varied security rules and procedures when it comes to workers' access levels on a "need to know" basis and access to data and information.

In the survey instrument, it was mentioned as the next set of risks that had to be studied. Among the respondent groups, there are no significant differences in their perceptions of unauthorised access to data or systems by employees (F-ratio 1.421; p-value 0.230);

outsider (hackers) unauthorised access to data or systems (F-ratio 1.567; p-value 0.186); and natural disasters like flooding and power outages (F-ratio 0.501; p-value 0.735). Respondents, on the other hand, vary considerably when it comes to employee password sharing with an F-ratio of 6.043 and a p-value of 0.000. Additionally, this may be in accordance with widely varying information access security standards, particularly those pertaining to identity and authentication processes.
Using the F-ratio and p-values, it was found that responding organisations all have similar opinions in areas such as man-made and natural disasters, such as fire and flood (F-ratio 0.490 and 0.733), the introduction or destruction of output (F-ratio 1.001; p-value 0.4090), and the creation of fictitious or incorrect output (F-ratio 1.001; p-value 0.4090). (F-ratio 0.739; p-value 0.567). This could support the likelihood that data security concerns include a wide range of issues, including accessibility, privacy, and integrity. Availability is hampered by the potential loss of data files due to human error or deliberate deletion.

. In order to discourage the use of external output devices such as flash discs and similar devices to prevent illegal copying of output from user computers, certain firms, particularly banks and insurance, regularly block users' access to external disc compartments (i.e. the CD drive).

F-ratios for "unauthorised documents visibility through the display on monitors or on paper" and "unauthorised persons shredding documents" (F-ratios of 3.038 and 3.361, respectively) indicate that subjects have differing views on these variables, as does data interception from remote locations (F-ratio of 3.106; p-value0.017).

Suggestions and Information Gathered

Facilities, computers, and telecommunications equipment that enable the processing of information assets should be monitored by management for compliance with the physical controls in place to protect CAIS.

When necessary, security guards should be employed as part of the overall physical security strategy. Use of biometric technologies, such as retinal scanners and hand geometry and fingerprint readers, should be employed widely when the perceived benefits surpass any related costs.
In order to guarantee the efficacy of CAIS's physical access restrictions, they should be monitored and assessed on a regular basis. The majority of the time, social engineering may beat physical security measures, thus management has to educate and remind staff of their responsibilities to maintain the confidentiality of company information.
The term "social engineering" refers to the employment of psychological tactics to obtain access to electronic systems by unauthorised individuals.

This includes social engineering techniques such as shoulder surfing (watching over the shoulders of authorised users and identifying key codes that provide access for information assets), claiming lost badges or key cards and convincing an authorised user to allow access; or piggybacking behind legitimate users with a valid key card. Despite the fact that implementing and maintaining logical security may seem more difficult, management should establish authorization processes based only on "need to know" information.

There should be a restriction on the programmes and data that authorised users may access. Logging and monitoring of logical access to systems and data should also be done on a frequent basis. Logs for access and transactions should be included in policies and processes. CAIS security personnel must always be on the lookout for possible unauthorised users of information systems who are capable of getting access to applications and data, and then educate users as necessary to prevent this from happening.

Some examples include dissatisfied internal workers, contractual personnel, suppliers or vendors (including cleaning and maintenance companies), partners, distant users and organisations with access to external information systems (such as the general public)... Effective security procedures and accompanying controls should be implemented by businesses.

Regular penetration testing are necessary to assure continuity. Breaking through access points by intimidation or sheer force or getting entry as a tourist and attempting to enter restricted areas are examples of such tests.

Security measures that safeguard information assets must be regularly reviewed, monitored and tested to ensure they are effective. Information technology security officers should be required to develop incident response processes, as well as standards for identifying, notifying and collecting proof of such disruptive incidents. These procedures should then be made mandatory for all IT security officers to follow going forward.

Conclusion

This study reviews prior studies on the elements that may influence the effective adoption of AIS in small and medium-sized businesses. It also includes the findings of research that show how AIS deployment affects the performance of small and medium-sized businesses. 66 Journal of Business, Economics, and Social Sciences The internal validity of earlier studies revealed that diverse techniques of analysis and assessment of factors associated with the performance of SMEs exist. Non-financial performance, which is currently restricted in SMEs, may be examined using a number of analytical approaches and various variables. AIS adoption, particularly in poor countries, remains an intriguing research issue based on the external validity, it may be inferred. There seems to be a research gap that might be a topic of debate in the future based on prior results.

Reference

1) Abernethy, MA. & Lillis, AM. (1995). (1995). The influence of manufacturing flexibility on management control system design. Accounting, Organizations & Society, 20(4): 241- 258.

2) Amidu, M. Effah, J. & Abor, J. (2011). (2011). E-Accounting practises among small & medium firms in Ghana. Journal of Management Policy & Practice, 12 (4):146-155.

3) Al-Eqab. & Ismail, NA. (2011). (2011). Contingency considerations and accounting information system design in Jordanian enterprises. IBIMA business Review, Article ID 166128, 1- 13.

4) Bledsoe, N. L. & Ingram R. W. (1997). (1997). Customer satisfaction via performance assessment. Journal of Cost Management, Winter, 43-50.

5) Boulianne, E. (2007). (2007). Revisiting fit between AIS design and performance with the analyser strategic type. International Journal of Accounting Information Systems, 8, 1-6.

Choe, J.M. (2002). The impact of management accounting information on organisational learning in a high-tech industrial environment. The European Journal of Information Systems, 11, 142-158.

7) Chu, W. (2007) (2009). From a Taiwanese public company, we can see the impact of family ownership on SME success. 353-373 in Small Business Economics, 33th edition.

Reynaldo Eztebanez (R), Eduardo Grande (E.U) & Carlos Colomina (CM) (2010). IT implementation: evidence from Spanish small and medium-sized enterprises (SMEs). Articles 39-57 in International Journal of Accounting and Information Management, Volume 18, Number 1, Spring 2007