E-COMMERCE AND CYBER CRIMES: THE ROLE OF THE ACCOUNTANTS

[1]Yunusa, A. (Mrs) and [2]Suleiman, A. I.

[1.] *Department of Accountancy, Federal Polytechnic, Idah, Kogi State*

[2.] *AMCS Ltd, Federal Polytechnic, Idah, Kogi State*

ABSTRACT

One of the most challenges faced by businesses these days is the need to be Information and Communication Technology (ICT) inclined in order to flourish, and embedded in this, is the fight against cyber-crime. Hence, this study is carried out to assess accounting and other control measures aimed at preventing cyber-crimes. In carrying out this research work, secondary methods of data collection were used for the collection of data. The secondary data were obtained from related literatures. The paper shows that e-commerce, no doubt, comes with a great advantage for business transaction. However, one has to face the battle, against cyber-crimes. It further revealed that the protection against cyber-crime, should cut across the organisation's board and not the government or ICT department alone. Organisations should increase training courses in electronic commerce for accountants in order to provide their establishments with a specialized staff who are ready and qualified to face the challenges and to solve the problems imposed by the Information Technology development.

Keywords: E-commerce, Cyber-crime, ICT and Accountants

INTRODUCTION

One of the pride of a business concern is its level of growth, and to ensure this, innovations and technological dynamism must be kept on check. Today, man is able to send and receive any form of data which may be an e-mail or an audio or video just by the click of a button. Rainer and Cegielski (2013), posit that Information Technology (IT) if properly used, can have enormous benefits for individuals, organizations, and the entire societies. So far, we have seen diverse ways in which IT has made businesses more productive, efficient, and responsive to consumers. Unfortunately, information technologies can also be misused, often with devastating consequences. In fact, the misuse of information technologies has come to the forefront of any discussion of IT.

Technologies are designed to improve commercial transactions using the Internet. However, we have not yet achieved an ideal world of painless and secured transactions utilizing the Internet as unresolved privacy issues of the purchaser have impeded further development of the technologies (Alberto, Avila and Violeta, 2007). Electronic Business which is commonly referred to as e-business, is the utilization of information and communication technology (ICT) in the conduct of business on the internet, not only in buying and selling, but also servicing customers and collaborating with business partners. Electronic business methods enable companies to link their internal and external data processing systems more efficiently and flexibly, in order to work more closely with suppliers and partners, and to better satisfy the needs and expectations of their customers.

According to WTO (2013), e-commerce has been hailed by many as an opportunity for developing countries to gain a stronger foothold in the multilateral trading system. E-commerce has the ability to play an instrumental role in helping developing economics benefit more from trade. Security services offering protection from security threats are: identification, authentication, confidentiality, integrity, access control, and non-reputation. Hence, e-business applications are doing

more than ever to increase efficiency and improve relationships with partners and customers.

The latest technologies like cloud computing, mobile computing, E-commerce, net banking etc., also need high level of security. Since these technologies hold some important information regarding a person, their security has become very important. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic wellbeing. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as a strong governmental policy. The fight against cyber-crime needs a comprehensive and a safer approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cyber-crime effectively. Governments all over the world are imposing strict laws on cyber securities in order to prevent the loss of some important information. Every individual must also be trained on this cyber security and save themselves from these increasing cyber-crimes.

Most players of the e-commerce are unable to safeguard private information in a very effective way and hence, cyber crimes are on the increase day by day. More than 60 percent of total commercial transactions are done online (Krell, Matook and Rohde, 2016). So, this field required a high quality of security for transparent and best transactions. This makes cyber security a vital and serious issue. The scope of cyber security is not just limited to securing the information in IT industry but also to various other fields like cyber space, etc.

Accountants are caught within the middle of e-commerce and cyber-crimes in carrying out their duties – either reporting the financial position of the firm or expressing their opinion with regard to the financial statement prepared by the company, looking at the control measures in place.

Unfortunately, not all that engage in the e-commerce are aware of the crimes that are associated with it and the possible control measures. There is almost an uncountable number of ways that an e-business setup could be attacked by hackers, crackers and disgruntled insiders. Common threats include hacking, cracking, masquerading, eavesdropping, spoofing, sniffing, Trojan horses, viruses, bombs, wiretaps, etc. This threats comes in form of crimes that can be perpetrated with the use of the internet. Also, where the organisation is aware of the cyber-crimes associated with the e-commerce, the battle is left to their IT department alone, even when the IT department may not be able to do it alone. Some organisation's IT section cannot do well than the perpetrators of the crimes, or even engage in it by some of the IT staff. Specifically, the management and their accountants in setting their internal control system, ignore the IT aspects of the control. Hence, this paper looks at the role of the accounting in e-commerce and cyber-crime.

REVIEW OF RELATED LITERATURE

Conceptual Framework

Electronic commerce, or e-commerce, is the buying and selling of goods and services on the Internet. Other than buying and selling, many people use Internet as a source of information to compare prices or look at the latest products on offer before making a purchase online or at a traditional store. E- Business is sometimes used as another term for the same process. More often, though, it is used to define a broader process of how the Internet is changing the way companies do business, the way they relate to their customers and suppliers, and the way they think about such functions as marketing and logistics. For the purpose of this study, e-commerce is taken to mean doing business electronically.

With the increasing diffusion of ICTs, more specifically the Internet, the global business community is rapidly moving towards Business to Business (B2B) e-Commerce. The buyers gain a clear advantage when the Internet gives them access to the global market, by which they can compare

prices across regions, find out whether prices vary by order fragmentation and get awareness about substitute products. Due to transparency of the market, customer can compare the services of various e-commerce sites easily. For instant, in the case of e-commerce, the competitors are one click away from customer. If clients are not happy with the products, prices or services offered by a particular e-commerce site, are able to change much more easily to another e-commerce site than in the physical. From the sellers' point of view, they don't need to have physical existence.

Internet and e-commerce are closely wrapped towards developed countries. But they can achieve tremendous benefits from developing countries if it is applicable as an ideal business purpose. E-commerce is a revolution in business practices (Ohidujjaman, et al, 2013). The term commerce is viewed as transactions conducted between business partners. Electronic commerce is an emerging concept that describes the process of buying and selling or exchanging of products, services and information via computer networks including internet (Anupam, 2011). Commercial transactions involve the exchange of value (e.g., money) across organizations or boundaries in return for products and services. Exchange of value is important for understanding the limits of e-commerce. Without an exchange of value, no commerce occurs (Laudon and Traver, 2016). E-business has changed processes within and between enterprises. Electronic Data Interface (EDI), widely introduced twenty five years ago on dedicated links between firms, showed how information could be directly passed from the operating systems of one enterprise to the processing, production and logistics systems of another enterprise (Clayton and Criscuolo, 2015). If implemented properly, E-commerce technologies can result in business process improvements and increased efficiencies. Leveraging Ecommerce technologies should result in the improvements to developing countries, but so far have not produced the desired results (Jeffrey, 2011). The main benefit from the customer's point of view is a significant increase and saves time and eases access from anywhere in the globe. Customers can place a purchase order at any time. The main benefits of ecommerce for customers are; reduction of transaction costs and the increased comfort.

However, the major challenges faced by the sellers and the buyers in carrying out business transactions through internet, is cyber crime, lack of private and public corporations to jointly grow the business of e-commerce and the lack of system security, reliability, standards, and some communication protocol. Customers lose their money if the website of ecommerce site is hacked. Most common problem of e-commerce website is not having enough cyber security. Financial institutions and banks in developing countries are reluctant in taking an active role to promote e-commerce (Saini, Rao and Panda, 2015). However, merchants need the involvement of banks to broaden the reach and appeal of ecommerce and to help prevent fraud and potential losses attributable to credit card fraud. But beyond the credit card approach, banks and other financial service intermediaries are challenged to develop alternative modalities for secured and reliable online transactions in environments where credit cards are not common place (Anupam, 2011). In many developing countries, even today, cash on delivery is the most accepted system, even cheques and credit cards are not readily accepted (Roni, 2012).

Cyber-crime is a term for any illegal activity that uses a computer as its primary means of commission and theft. The U.S. Department of Justice expands the definition of cyber-crime to include any illegal activity that uses a computer for the storage of evidence. Cyber-crimes include crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses as well as computer-based variations of existing crimes. These are identity theft, stalking, bullying and terrorism which have become major problems to people and nations.

Usually, in common man's language, cyber-crime may be defined as a crime committed using the computer and the internet to steel a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs. As day by day technology is playing a major role in a person's life. The cyber-crimes also will increase along with the technological advances.

There are various types of computer fraud and the abuse of techniques associated with white-collar crimes. In this context, the accountants play a vital role in detecting, preventing and reporting computer fraud. Accountants who specialize in fraud auditing and investigations are known as the forensic accountants. The forensic accountants are auditors trained in Information Technology Security Control Knowledge. These specialized auditors need to detect and prevent fraud to protect the information system of an organization. Auditors have to make use of fraud prevention techniques by making fraud less likely to occur, by increasing the level of difficulty for committing fraud by improving detection methods, reducing fraud losses and finally identifying sufficient and appropriate audit evidence to sentence fraud perpetrators with penalties upon the white-collar crimes. The need for computer forensic tools was stressed by Narayanan & Ashik, (2012) in the wake of increased cyber-crimes annually. The authors advocated computer forensic analysis tools to be used in a legal setting.

Cyber Security

Privacy and security of the data will always be top security measures that any organization takes care of. We are presently living in a world where all the information is maintained in a digital or a cyber form. Social networking sites provide a space where users feel safe as they interact with friends and family. In the case of home users, cyber-criminals would continue to target social media sites to steal personal data. Not only in social networking, but also during bank and other business transactions that a person must take all the required security measures. Cyber Security techniques include:

Access control and password security: The concept of user name and password has been fundamental ways of protecting our information. These may be among the first measures regarding cyber security.

Authentication of data: The documents we receive must always be authenticated before downloading, that is it should be checked if it has originated from a trusted and a reliable source and should not be altered. Authenticating of these documents is usually done by the anti-virus software present in the devices. Thus a good anti-virus software is also essential to protect the devices from viruses.

Malware scanners: This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.

Firewalls: A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach computer over the Internet. All messages entering or leaving the internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence, firewalls play an important role in detecting the malware.

Anti-virus software: Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that, it can check for the new viruses as soon as they are discovered. Anti-virus software is a must and basic necessity for every system.

Threats in an Electronic Accounting Environment

In recent times, technology has provided support to business activities. The accounting environment has also benefited immensely from this support. For instance, the alignment of

technology with accounting has resulted in improved accuracy of data, timely processing of information, efficient financial reporting and increased functionality of the information system (Ghasemi, Shafeiepour, Aslani & Barvayeh 2011; Romney & Steinbart, 2009; Nicolaou, 2000; Ezewoke, 2017). However, the relationship between technology and accounting has presented certain threats that may hamper on user and a stakeholder's satisfaction.

Potential threats facing accounting information in an electronic environment are entangled as the presence of one threat generates the presence of another. Some of the threats identified in this review are information system risk and security. Information system risk entails data loss, privacy distortion, unavailability of system, dissatisfactions with system deliveries and performance and affordability of vendor pricing (Brandas Megan & Didraga, 2015). 225

Security in the electronic environment situates around the confidential availability and integrity of the system. This is vital to protect the system from illegal access, secures the authenticity of the information from being modified or deleted while assuring the users of the availability of the system in delivery, storing and processing of information as at when needed (Elmaghraby & Lasavio, 2014). In addition, the ability to protect the accounting system from external intrusion that can cause damage to the system hardware (through illegal clones or snooping of hardware designs), software (through bugs or deployment errors), and the network system (through network monitoring or sniffing) is also vital (Jang-Jaccard & Nepal, 2014).

The classification of threats in an electronic environment is imperative to understand the vulnerabilities of using ICT in carrying out accounting transactions. Jouini, Rabai and Aissa (2014), classified threats in an electronic environment into threat source, agents, motivation, intentions and impacts. The source of threat concerns the internal and external sources of threats in the organisation. The threat agents can consist of human, environment or technological agent. The motivation for carrying out a threat can be malicious or non-malicious. The intention of carrying out a threat can be deliberate or accidental. The impacts of threat in the organisation can lead to the destruction or corruption of information, disclosure of information to unauthorised party, theft or denial of service, removal of privilege and illegal use of information.

The Role of the Accountant

The accountant performs a significant role in the running of an organisation. The accountant is the custodian of accounting/financial records of an entity. Accountants and auditors help to ensure that the firm runs efficiently, its public records kept accurately and on time. They perform these vital functions by offering an increasingly wide array of business and accounting services to their clients. Accountants help organisations to prepare financial statements and reports and perform financial analysis and interpretations of financial data to enhance decision making.

On the whole, an accountant performs functions such as preparing of financial statements and reports, interpreting and analysing financial statements, analysing financial performance, providing management team information to enhance planning, decision making and budgeting, ensuring compliance with relevant laws and regulations, and finally giving financial advice.

The advances in IT permit accounting information system to create more information. Although, more information is often better, this is only true to a point. There are limits to the amount of information that the human mind can effectively absorb and process. Information overload occurs when those limits are passed. Information overload is costly, because decision-making quality declines while the costs of providing that information increase.

The information which are created and documented by computerized accounting information system will be used by the interested users in different locations. According to Moscove & Simkin (1984), in their definition for AISs, insisted that AIS communicates financial information to both company's external and internal parties. In this situation, IT will be very helpful in transmitting accounting data and information to various locations, because data communication which refers to transmitting data to and from remote locations, enable AISs to transmit accounting data over local and wide area networks. Many accounting applications use data communications in normal business operations. For example, banking systems enable individual offices to transmit deposit and withdrawal information to centralize computer locations. Therefore, accountants must understand data communication concepts because so many AISs use them and because many clients acquire AISs that depend on data transmissions. Many AISs now use LANs or WANs for e-mail, sharing computer resources, saving software costs, gathering input data or distributing outputs. Wifi technology of the future, will significantly increase the ability of accountants to be mobile, yet connected to their offices as well as to their clients (Malik, 2003). Using IT for ease of operations by the accountant subject accounting work to fraudulent activities.

Furthermore, the connection between accounting and computer crimes and fraud is both straightforward and important (Bagranoff et al., 2010). Managers, accountants, and investors all use computerized financial accounting information to control valuable resources, authenticate accounting transactions, and make investment decisions. But the effectiveness of these activities can be lost if the underlying information is wrong, incomplete or seriously compromised. This is why digital information in itself, is a valuable asset that must be protected. The more managers and accountants know about computer crimes and fraud, the better they can assess risks and implement control measures in order to protect organizational assets.

Although, the terms "computer crime" and "computer abuse", seem to describe the same problem, there is a subtle difference between them. The type of computer crime with which most professional accountants are familiar with, is financial fraud. Statements on the Auditing Standards No. 99, identify two types of fraud; fraudulent financial reporting and misappropriation of assets. Although, data on computer crimes and fraud are limited, at least three reputable organizations conduct surveys that help us understand the breadth and depth of these crimes.

In addition to the typical accounting services rendered by accountants, the profession is rapidly moving into other value-added services known as fraud investigation litigation support or the broader comprehensive term of forensic accounting. The terms forensic accounting and litigation support, generally imply the use of accounting in a court of law. Thus, the services of an accountant in a fraud investigation or court cases are often referred to as forensic accounting or litigation support services.

The Accountant and Cyber Crime

The growth of information technology has been a positive force in business; but, as in the case with all innovations, it has a downside risk as well. Organizations, both large and small, have come to rely heavily on information technology to provide timely information used in making critical business decisions. As reliance on information technology grows, so do the risks which the organization faces. Thus, anyone involved in decision making, should understand those risks and how they can impact on the organization. Cyber-crime is one of the business risks. A cyber-crime just like fraud is a dishonest act by an employee or an external party that results in personal benefit to the employee at the expense of the employer or the company. The three main factors that contribute to fraudulent activity are depicted by the fraud triangle: opportunity,

financial pressure, and rationalization (Weygandt et al., 2010). Fundamentally, computer fraud is people fraud; no computer system can perpetrate fraud without at least some human interventions. The required computer skills will vary greatly depending on the type of fraud being perpetrated.

What can be done to prevent or to detect fraud? After numerous corporate scandals came to light in the early 2000. The Congress addressed this issue by passing the Sarbanes- Oxley Act of 2002 (SOX). Under SOX, all publicly traded U.S. corporations, are required to maintain an adequate system of internal control. Corporate executives and boards of directors must ensure that these controls are reliable and effective. In addition, independent outside auditors must attest to the adequacy of the internal control system. Companies that fail to comply are subjected to fines, and their officers can be imprisoned. SOX also, created the Public Company Accounting Oversight Board (PCAOB), to establish auditing standards and regulate auditor activity (Bawaneh, 2011)

Nick (2018), prescribed the following measures for the protection of cyber-crime:

Do a review: List everything in your business that could be at risk from cyber attack such as money, IT equipment, pricing information and product designs. Then work out what form these threats could take. Review your cyber security procedures and technology regularly.

Back up data: The loss of data critical to the running of your business can have serious consequences. This need not necessarily be from a cyber-attack; it could also be from hardware or software failure. Identify data you need to back up. Most network or cloud storage products can automatically back data up.

Get malware protection: Malicious software (malware) infects legitimate software. The main defence against it is anti-virus software. Install and turn on anti-virus software for all computers and devices. Install licensed anti-virus programs only.

Prevent users from unauthorised third-party downloading apps: Make sure you keep IT systems up to date by applying patches from software and hardware suppliers. Most security software will have an option to automatically apply a patch whenever a new one is released. Remember to replace software and hardware that's not supported by suppliers because it's too old. You must ensure that you switch on your firewall (the security device that monitors incoming and outgoing traffic in your organisation's computer network and decides whether to allow or block traffic based on a defined set of security rules). Most operating systems incorporate firewalls.

Protect smartphones: Businesses are increasingly reliant on mobile technology. However, mobile devices and systems can be your organisation's weak link. Make sure you switch on password protection and be smart with the password.

Prepare for phishers: Phishing is a type of fraud in which criminals send emails claiming to be from reputable organisations such as banks. Phishing fraud is becoming more devious as well as more common.

Make sure that you do the following: (1) Configure accounts to reduce the impact of successful attacks by giving your employees the lowest possible level of IT privilege (the information they can access and change) for them to do their job. (2) Educate staff to spot requests that are unusual. Example is sending a large one-off payment to a supplier, or providing their passwords or credit card details. (3) Be aware of what to look out for. Although, phishing emails are becoming more sophisticated, there are usually still signs that they are dodgy. Example is incorrect or inappropriate email addresses and poorly worded messages.

Train your staff: Encourage staff to report all cyber attacks. Knowing that you have been attacked, enables you to manage the recovery. If you are unsure about any aspect of cybersecurity, consult an expert. Do not leave it to chance.

Get certified: The ISO/IEC 27032:2012, is an international standard for cybersecurity. It is a set of guidelines that cover information security, network security, internet security and the protection of 'critical information infrastructure'. Make sure your business complies with it.

Take out insurance: First-party insurance covers your business's assets. It may include:

- loss or damage to digital assets such as data or software programs, business interruption
- cyber extortion, where third parties threaten to damage or release data if money is not paid.
- Third-party insurance covers the assets of others typically, your customers. It may include:

Security and privacy breaches, investigation, defence costs and civil damages associated with multimedia liability to cover investigation, defence costs and civil damages arising from defamation and breach of private loss of third-party data, including compensating customers.

Plan for an emergency: Have a plan for responding to a serious cybersecurity attack. It should include verifying the extent of damage caused by the attack and mitigating it, reporting the incident to the relevant national authority, and testing your data backup and business continuity systems.

Theoretical Framework

Technology Acceptance Model

The Technology Acceptance Model (TAM) was developed in 1986 and aims to explain individuals' acceptance and beliefs towards new technology. It is still a widely used model in recent research (e.g. Abroud et al., 2015; Bach et al., 2016; Priyadarshinee et al., 2017). TAM relies on two factors that are affecting individuals' attitude towards new technology, namely perceived usefulness and perceived ease of use. Perceived usefulness is described as the degree which individuals think the new system will increase one's performance, while perceived ease of use, is defined as the degree which the individuals believe that using the system will be free from interference (Davies et al., 1989). Davies and Venkatesh (2000), later extended the perspective perceived usefulness, where several social impacts were added; subjective norms, voluntariness and image.

The purpose of using TAM in this study, is because of its prominent applicability on attitudes toward technology, and in the widely usage of the theory in previous researches. The model has been able to explain the phenomena during a significant time. Thereof, since the extended usage among scholars, and where the model has been proven useful, it will fit in this paper because attitudes among the accountant firms' consultants towards automated accounting, and the prevention of organisation from cyber-crimes, can be addressed. With the named model, we will be able to explain attitude from a technology perspective.

Path Dependency Theory

Path Dependency Theory (PDT), has its foundation in institutions which inspires organizations and their actors and activities. A normal conceptualization of the theory is that, the past reflects the present actions (Mahoney, 2000). There is no agreed unified definition of institutions but normally one refers to the established ways of acting, cultural assumptions, or conscious or subconscious actions (Eriksson-Zetterquist, 2009). Hence, institutions also described as social constructions that affect organizations' actions and at the same time restraining them, could have an impact on how firms and individuals are influenced by technologies and their chain reactions (Krell et al., 2016). Path dependency can be found in several

articles put in different contexts such as institutional paths or organizational paths (Bergek & Onufrey, 2013). But in this paper, it will focus on the technological perspective. Organizations and their actors have their inherent behaviour and actions in entrenched paths, where the paths are a construction of institutions and societal policies rooted in previous decisions. The paths taken in a historical context is difficult to change because the institutions are grown into one's processes and becomes costly in terms of investing, learning, coordination and anticipation, where it is cheaper to continue in the same manner as previously (Trouvé et al., 2010). In our understanding, the reasoning behind PDT, is that, one continues to act in one alway, e.g. continue to use a specific system due to one's historical preferences even though, there comes new innovative and more efficient approaches to the problem. Hence, it is costlier in the terms mentioned above to change one's preferences even though there are more efficient solutions.

The purpose of using PDT in this study, is to be able to assess the need for organisation in e-commerce to be pro-active in following the technological dynamism in order to ensure the protection and prevention of cyber-crime.

RESEARCH METHODOLOGY

The paper uses secondary data in its exploration. The collected data from published books, journals, research papers, magazines, daily newspaper, internet and official statistical documents. The study is qualitative in nature.

CONCLUSION

Cyber security is an umbrella concept that encompasses information security and information assurance. Fafinski (2013), opined that future regulation on computer misuse should go beyond criminal and civil laws. It includes non-legal means of governance including internet users and user-groups, internet service providers, corporations, the law enforcement agency and other non-governmental organizations. Some individuals commit crimes even with no intent to profit from their actions.

Federal, state, and international accounting standards are regularly amended to keep up with the new and creative crimes being committed. Shukan & Erdogan (2013), concluded that the current legal regulations in many countries are not sufficient no matter how many laws the federal or state government passes. The most anticrime strategy is one of self-protection; a strategy of securing one's digital assets. Auditors, individuals, businesses, and government must be vigilant in their efforts to secure information, computer and networks against criminal activities.

REFERENCES

Abroud, A, Choong, Y, Muthaiyah, S, & Fie, D. (2015). Adopting e-finance: Decomposing the Technology Acceptance Model for Investors. *Service Business*, 9 (1).

Bach, M. P, Celjob, A, & Zorojaa, J. (2016). Technology Acceptance Model for Business Intelligence Systems: Preliminary Research. *Procedia Computer Science*, 100.

Bagranoff, N., Simkin, M. & Norman, C. (2010). *Core Concepts of Accounting Information Systems.* Singapore: John Wiley & Sons, Inc.

Bawaneh, S. (2011b). The Effects of Corporate Governance Requirements on Jordan Banking Sector. *International Journal of Business and Social Science*, 2(9)

Bergek, A., & Onufrey, K. (2013). Is One Path Enough?: Multiple Paths and Path Interaction as an Extension of Path Dependency Theory. *Industrial and Corporate Change*, 23 (5)

Brandas, C., Megan, O. & Didraga, O. (2015). Global Perspectives on Accounting Information Systems: Mobile and Cloud Approach. *Procedia Economics and Finance, 20.*

Bruce, R. G. & John C. L. (2004). Codes of Ethics with Impact. *The CPA Journal*, May.

Davies, F. D. & Venkatesh, V. (2000). Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation and Emotion into the Technology Acceptance Model. *Information systems Research, 11*.

Davies, F. D., Bagozzi, R. P. & Warshaw, P. R. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science*, 35 (8).

Edwin J. K. (2003). The Need for Old-Fashioned Ethics. *The CPA Journal, December*.

Elmaghraby, A., & Lasavio, M. (2014). Cyber Security Challenge in Smart Cities: Safety, Security and Privacy. *Journal of Advanced Research, 5*.

Eriksson-Zetterquist, U. (2009). *Institutionell Teori - Ideer, Moden, Förändring*. 1st ed. Malmo: Liber.

Fafinski, S. (2013). Computer Misuse: Response, Regulation, and the Law. *Routledge*.

Ghasemi, M., Shafeiepour, V., Aslani, M., & Barvayeh, E. (2011). The Impact of Information Technology (IT) on Modern Accounting Systems. *Procedia- Social and Behavioural Sciences, 8*.

Jang-Jaccard, J., & Nepal, S. (2014). A Survey of Emerging Threats in Cyber security. *Journal of Computer and System Sciences, 80*.

Kelly, R. & Cegielski, C. G. (2013). *Introduction to Information Systems,* 4th Ed. Singapore: John Wiley & Sons.

Krell, K., Matook, S., & Rohde, F. (2016). The Impact of Legitimacy-Based Motives on Information System Adoption Success: An Institutional Theory Perspective. *Information & Management*, 53 (6).

Laudon, D. P., & Laudon, J. P. (2010). *Management Information System: Managing the Digital Firm,* 11th ed. London: Pearson Education Ltd.

Mahoney, J. (2000). Path Dependence in Historical Sociology. *Theory and Society*, 29 (4).

Malik, F. (2013). Application of Data Mining in Changing Times and its Role in Future. *Indian Journal of Commerce and Management Studies*, *4*(1).

Narayanan, A. S., & Ashik, M. M. (2012). Computer Forensic First Responder Tools. Advances in Mobile Network, Communication and its Applications (MNCAPPS): International Conference.

Nick, H. (2018). Has Your Business Been Hacked or Lost Your Clients' Personal Data? If the answer is Yes, You are Far from Alone. *Association of Certified Chartered Accountants*: www.accaglobal.com/gb/en/member/discover/cpd-articles/business management/cybercrimejul-cpd.html

Nicolaou, A. (2000). Contingency Model of Perceived Effectiveness in Accounting Information Systems: Organizational Coordination and Control Effects. *International Journal of Accounting Information Systems, 1*.

Ohidujjaman, N. (2013). E-commerce Challenges, Solutions and Effectiveness Perspective in Bangladesh". International Journal of Computer Applications, 70(9).

Paul, M. C. (2003). Education for the Public Trust. *CPA Journal*, August.

Priyadarshinee, P., Raut, R.D., Jha, M.K., & Gardas, B. B. (2017). Understanding and Predicting the Determinants of Cloud Computing Adoption: A two Staged Hybrid SEM - Neural Networks Approach. *Computers in Human Behaviour*, 76.

Rabai, L. B. A., Jouini, M., Aissa, A. B., & Mili, A. (2013). A Cyber Security Model in Cloud Computing Environments. *Journal of King Saud University-Computer and Information Sciences, 25.*

Rezaee, Z. (2004). Restoring Public Trust in the Accounting Profession by Developing Anti-Fraud Education, Programs, and Auditing. *Managerial Auditing Journal, 19(1).*

Romney, M. B., & Steinbart, P. J. (2009). *Accounting Information System.* New Jersey: Pearson Prentice Hall.

Saini, H., Rao, Y. S. & Panda, T. C. (2015). Cyber-Crimes and their Impacts: A Review. *International Journal of Engineering Research and Applications, 2(2*).

Shukan, A., & Erdogan, Y. (2013). Criminal Law Problems of IT-Crimes in Kazakhstan and Turkey. *Middle-East Journal of Scientific Research*, 17(12).

Trouve, H., Couturier, Y., Etheridge, F., Saint-Jean, O., & Somme, D. (2010). The Path Dependency Theory: Analytical Framework to Study Institutional Integration: The Case of France. *International Journal of Integrated Care*, 10.

Weirich, T., Thomas, P. & and Churyk, N. (2010). *Accounting & Auditing Research Tools and Strategies.* Singapore: John Wiley & Sons, Inc.

Weygandt, J., Kimmel, P., & and Kieso, D. (2010). *Accounting Principles.* Singapore: John Wiley & Sons, Inc.