Available online at https://ijikm.uitm.edu.my/

e-ISSN: 2289-5337

Journal of Information and Knowledge Management (2024) Vol. 14, No. 2

Journal of Information and Knowledge Management

Corporate Computer Forensics Investigation Adoption Antecedents in Malaysia's Critical Information Infrastructure Agencies

Wan Abdul Malek Wan Abdullah[1], Nurussobah Hussin[2]*, Mohd Nazir Ahmad[3], Ahmad Zam Hariro Samsudin[4], Abdurrahman Jalil[5]

[1,2,3,4,5]*School of Information Studies, College of Computing, Informatics and Mathematics, Universiti Teknologi MARA*

ARTICLE INFO

Article history:
Received 1 July 2024
Revised 15 August 2024
Accepted 1 September 2024
Online first
Published 1 October 2024

Keywords:
computer forensic investigation
digital information management
criminal evidence
computer crime
information management

ABSTRACT

To counteract computer-related crimes that have affected many companies, Computer Forensics, which involves obtaining and analyzing digital information for use as evidence in civil, criminal, or administrative cases, has become a focal point of attention for top management. The objective of this study is to assess Tornatzky's TOE innovation adoption model in relation to the Information Assurance of Corporate Computer Forensics Investigation's Action Plan among 210 respondents from Malaysia's Critical Information Infrastructure agencies. The research results demonstrate a strong relationship between the TOE model and the Information Assurance of Corporate Computer Forensics Investigation, specifically in anticipatory, process, and post-incident measures, with the exception of Tornatzky's organizational factor.

INTRODUCTION

Computer technology has become an integral part of daily life, rapidly advancing alongside the increase in computer-related crimes such as financial fraud, unauthorized access, identity theft, and intellectual property theft. To counteract these crimes, computer forensics plays a crucial role. In general, computer forensics involves obtaining and analyzing digital information to be used as evidence in civil,

[2*] Corresponding author. *E-mail address*: nurussobah@uitm.edu.my

criminal, or administrative cases. Digital evidence is time-sensitive by nature, and the faster the evidence is identified and collected, the more information can potentially be gathered to build a stronger case for presentation in the courtroom.

Computer forensic investigation should now be considered an integral part of enterprise-wide operations, especially in organizations that handle critical and sensitive data. Major regions, such as the United States and Europe, have identified and categorized National Critical Information Infrastructure (NCII) to safeguard the national interest inherent in these agencies' functions and processes. NCII is not unique to any one country; the United States, South Africa, the United Kingdom, Malaysia, and many other countries have their own identified critical agencies. Protecting these national critical infrastructure agencies with proactive countermeasures against cyber threats allows onboard staff to conduct cyber forensics, thereby maximizing the potential for identifying and collecting fragile evidence. Should an incident lead to a court case, an organization with computer forensics capabilities will have a distinct advantage.

Therefore, it is crucial for national critical infrastructure to implement swift and decisive mitigating actions to prevent national disasters (R. McCreight, 2022). Despite the introduction of numerous computer forensic models almost every year, most seem to be tailored primarily for Law Enforcement Agencies (LEAs) and are filled with technical jargon, making them difficult for non-LEA organizations to understand. Additionally, very little empirical research has explored the adoption of these models in collaboration with industries. As a result, the objective of this study is to assess Tornatzky's Technology-Organization-Environment (TOE) innovation adoption model in relation to the Information Assurance of Corporate Computer Forensics Investigation Action Plans, based on responses from 210 participants within Malaysia’s Critical Information Infrastructure agencies.

LITERATURE REVIEW

Computer Forensic Models

The model development has taken place almost every year since the very first model was in 1995 by Pollit, Casey (2000), Kruse (2002), Carrier & Stafford, Stephenson (2003), Lee, Palmer (2011), Stephenson (2003), Ciardhuain, Baryamureeba & Tushabe (2004)[28] and Beebe & Clark (2004), Kent (2006), Freiling (2007), NIJ (2008), Perumal & Cohen (2009), Pilli (2010), Agarwal (2011), Martini et al (2012), Wen et al & Kohn(2013), Quick et al (2014), Hitchcock & Chahira (2016). The evolution of the emerging computer forensic investigation is expected to be continuous alongside the breakthrough of the advanced mechanism to maximize the data recovery, analysis, and security protocols necessary to combat increasingly sophisticated cyber threats. The ongoing evolution of computer forensic models highlights the field's adaptability to advancing technologies and rising cyber threats. From Pollit's 1995 model to Hitchcock & Chahira's 2016 advancements, the focus remains on improving data recovery, analysis, and security, emphasizing the need for continual innovation in digital forensics.

The others are Trustworthiness, Computer Forensics in Networked Environments, Detection Recovery and Acquisition. The model development has taken place in almost every years since the very first model was in 1995 by Pollit, Casey (2000), Kruse (2002), Carrier & Stafford, Stephenson (2003), Lee, Palmer (2011), Stephenson (2003), Ciardhuain, Baryamureeba & Tushabe (2004) and Beebe & Clark (2004), Kent (2006), Freiling (2007), NIJ (2008), Perumal & Cohen (2009), Pilli (2010), Agarwal (2011), Martini et al (2012), Wen et al & Kohn(2013), Quick et al (2014), Hitchcock & Chahira (2016). The evolution of the emerging computer forensic investigation is expected to be continuous alongside with the

breakthrough of the advance mechanism to maximize the data finding. The computer forensic framework or model has been identified by Selimun et al (2008) as one of the major five (5) important scopes for future research. (PWC, 2016)

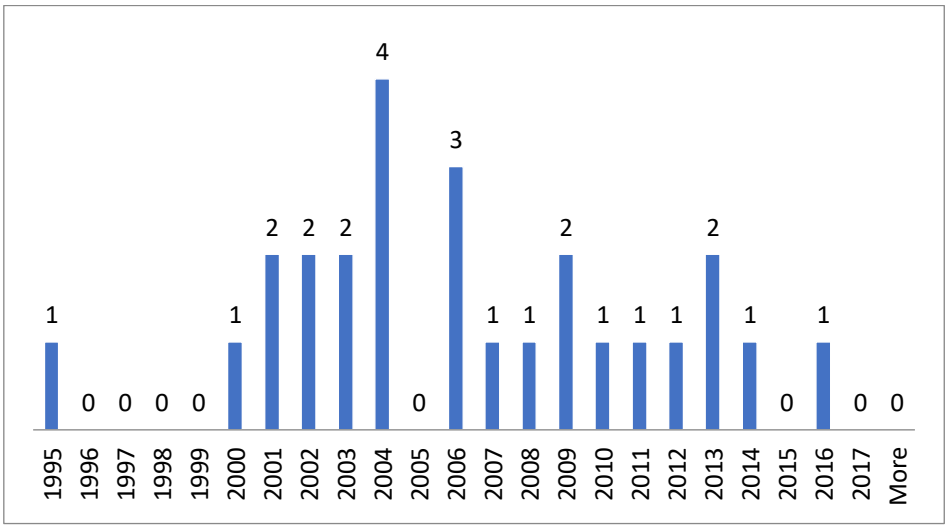

Figure 1: Computer Forensic Model Evolution

Most of the models seemed to be only suitable for Legal Enforcement Agencies (LEA) which were too technical-jargon terminologies hard and beyond the non-LEA organization could comprehend. The choice models for the research adoption model of the Corporate Computer Forensics Investigation should be appropriate for Non-Legal Enforcement Agencies (LEA) in terms of Practicality process for non-LEA in carrying out investigation, and the model that has strong industrial linkages with industry. These factors are important to choose an appropriate and working model for the Corporate Computer Forensics Investigation.

Table 1: Selected Models are those which have collaborated with Industries

No	Model name	Phase for Non-Legal Enforcement Agency factor	Collaboration with industry
1	The Integrated Digital Investigation Process (IDIP) by Carrier & Spafford (2003)	Readiness Phase	No
2	Enhanced Integrated Digital Investigation Process (EIDIP) Baryamureeba (2004)	Readiness Phase	No
3	Scientific Crime Scene Investigation Model by Ciardhuain (2004)	Awareness	No
4	Casey 2004	Incident Recognition	No
5	Computer Forensics Field Triage Process Model (CFFTPM) Rogers (2006)	Triage	No

6	Enhanced Integrated Digital Investigation Process(EIDIP) by Baryamureeba (2004)	Traceback	No
7	CPMICF by Freiling et al 2007	Pre-Incident	No
8	A Guide to Forensic Readiness for Organizations, Security Advisers and Lawyers. 2nd Edition 2008. By Information Assurance Advisory Council (IAAC), UK.	Anticipatory Measurement, Investigation Process, and Post Incident.	Yes

The company, has collaborated with the Information Assurance Advisory Council (IAAC) on the *Guide to Forensic Readiness for Organizations, Security Advisers, and Lawyers* (2nd Edition, 2008), as well as with industry leaders behind frameworks such as CPMICF by Freiling et al. (2007), Enhanced Integrated Digital Investigation Process (EIDIP), and The Integrated Digital Investigation Process (IDIP) by Carrier & Spafford (2003), has established itself as a key player in digital forensics. This collaboration has solidified its reputation and credibility, making it a trusted resource for organizations seeking comprehensive forensic readiness strategies. The integration of diverse methodologies has enabled the company to develop cutting-edge forensic tools and processes, effectively addressing modern cyber threats and positioning it as a preferred partner for those aiming to strengthen their digital security posture.

With the development of proprietary solutions that set it apart from competitors, the company attracts a broad spectrum of clients, from governmental agencies to private enterprises. Looking to the future, the company is poised to adapt and innovate as the digital landscape evolves with advancements like AI, IoT, and quantum computing. This adaptability, combined with its collaboration with international frameworks and standards, positions the company for global expansion, particularly in regions where digital forensic capabilities are still developing. By continuing its partnership with industry and academic leaders, the company has the potential to influence the future direction of digital forensics, shaping the industry's evolution and maintaining its role as a thought leader. Additionally, the company can offer comprehensive forensic readiness services that not only focus on investigation and response but also on proactive measures to prepare organizations for potential cyber incidents, ensuring its continued relevance and leadership in the ever-changing field of digital forensics.

Information Assurance Advisory Council (IAAC)

The Information Assurance Advisory Council (IAAC) is a private sector-led, cross-industry forum dedicated to promoting a safe and secure Information Society. IAAC brings together corporate leaders, public policy makers, law enforcement, and the research community to address the security challenges of the Information Age. The IAAC is involved with giant international companies range from different business in nature, such as global aerospace, defence, security, and advanced technologies company, Lockheed Martin[2], a multinational professional services network such as auditing, Price Water Cooper[3]), an aerospace and defence technology company, Northrop Grumman[4], a telecommunications company, Vodaphone[5], an information technology company based in Blue Bell, Pennsylvania, that provides a portfolio of IT services, software, and technology, Unisys, a service company to safeguard government, defence and critical national infrastructure computer systems, Nexor, a software company that

provides software for security, storage, backup and availability, Symantec, a multinational information technology company, HP, a multinational network security company, RSA and an electronics and information technology business, Selex Elsag.

The Corporate Computer Forensic Investigation's Action plan consists of three distinct stages: Anticipatory Measurement, Investigation Process, and Long-Term Measure/Post Incident. Below is the stage of IAAC's Corporate Computer Forensics Investigation action Plan.[6] The adoption of the IAAC's Action Plan of the Corporate Computer Forensic is empirically supported by the fact that the lack of cooperative research between academia and industry, where only 10% of the research studies examined where a collaborative effort between industry and academia.

METHODOLOGY

This study employed a quantitative research approach. A structured questionnaire was distributed to IT staff within the IT departments resulting in a total of 201 respondents. The collected data were then analyzed using SPSS, where they underwent validation, descriptive analysis, and hypothesis testing, culminating in actionable recommendation.

The sampling selection is purposively chosen due to the nature of the research subject matter is a sub-set of the Computer Security field from is the National Critical Information Infrastructure of Malaysia as outlined by the Malaysia's Cyber Security agency, CyberSecurity, in which consists of ten (10) main government agencies and seven (7) their sub-agencies. A total of 210 questionnaire which consists of 56 items were distributed and 201 were useable. The Cronbach Alpha value for the Technology, Environment and Organization stood at .854, 953, and .974 respectively while the Factor analysis with Kaiser-Meyer-Olkin's produced 0.771, and 0.886 for the Information Assurance Factors respectively. Organizational factor appeared to have no significant relationship with Early Measure and Investigation Process.

Table 2: Results of the Reliability and Correlation Analysis

Correlations

		Organizational Factor	Technology _Factor	IV_Enronment _Factor
IV_Organizational	Pearson Correlation	1	.380**	.184**
	Sig. (2-tailed)		0	0.009
	N	200	196	200
IV_Technology	Pearson Correlation	.380**	1	.143*
	Sig. (2-tailed)	0		0.045
	N	196	197	197

IV_Environment	Pearson Correlation	.184**	.143*	1
	Sig. (2-tailed)	0.009	0.045	
	N	200	197	201
DV_Anticipatory Measure	Pearson Correlation	.198**	.355**	.362**
	Sig. (2-tailed)	0.005	0	0
	N	200	197	201
DV_Investigation Process	Pearson Correlation	.211**	.395**	.355**
	Sig. (2-tailed)	0.003	0	0
	N	200	197	201
DV_Post Incident	Pearson Correlation	.293**	.255**	.278**
	Sig. (2-tailed)	0	0	0
	N	200	197	201

DISCUSSION

There are several journal research on the TOE's and Critical Infrastructure Agency. Anthony (2014) used TOE's framework to study barriers to government cloud adoption and found that over 80% of our respondents mentioned the issue of security and privacy as the major concern for government cloud adoption of the Critical Infrastructure agency in addition to the Records Management with plays an important role in defining and protecting agencies' critical infrastructure. (Kuan, K.K.Y. and Chau, P.Y.K, 2001). The rationale for choosing the TOE over the above theories is based on several considerations. First, the TOE framework considers various contexts, not only focusing on technological contexts (such as IDT), but also considering organizational and environmental contexts. It is recognized that a model that covers many dimensions can provide better explanatory power than a model that only covers one dimension and assumes that changes in an organizations are determined not only by individuals in the organization but also by the characteristics organization in which they operate (Oliveira, T and Martins, M, F, 2011).

T-O-E specifically targets technology acceptance and popularly underpins many IS studies that explain end-user adoption at the organizational level. T-O-E framework is more holistic and size and industry friendly and robust empirical support in IS field more than other adoption frameworks (e.g. TAM, IDT, TRA, SM, and TPB) predicts predict the likelihood of innovation/technology adoption. The framework proposes three bits of enterprise contexts that influence the adoption and/or implementation of innovations. It suggests three aspects of an enterprise's context that influence the process by which it adopts and implements a technological innovation: technological context, organizational context, and environmental context. Technological context describes both the internal and external technologies relevant to the firm. Organizational context refers to descriptive measures about the organization such as scope, size, and managerial structure Environmental context is the arena in which a firm conducts its business—its industry, competitors, and dealings with the government.

Technological Factor

The technological context includes all the technologies that are relevant to the firm. It may also include those which are available in the marketplace but not been bought by the organization. The firm's existing technologies are important in the adoption process because the set a broad limit on the scope and pace of technological change that firm can undertake (Nicolas et.al, 2020). Technological context also describes that adoption depends on the pool of technologies inside and outside the firm as well as the application's perceived relative advantage (gains), compatibility (both technical and organizational), complexity (learning curve), trialability (pilot test/experimentation), and observability (visibility/imagination).

Organizational Factor

The organizational factor is the second variable in TOE's Tornatzky adoption model at organization-level measurement. Organizational context captures firm's business scope, top management support, organizational culture, complexity of managerial structure measured in terms of centralization, formalization, and vertical differentiation, the quality of human resource, and size and size related issues such as internal slack resources and specialization (Jeyaraj et. al., 2006).

Environmental Factor

Environment context refers to facilitating and inhibiting factors in areas of operations. Significant amongst them are competitive pressure, trading partners' readiness, socio-cultural issues, government encouragement, and technology support infrastructures such as access to quality ICT consulting services Zhu, K., & Kraemer, K. (2002). Customer expectation is seen as the external support as the next candidate refers to the availability of support and pressure for implementing and using an innovation (Awa et al., 2016). External competitor or Competitive Zhu, K., & Kraemer, K. (2002). Pressure that may come from new vigorous business company (Kinuthia, John Njenga, 2015). Government Policy factors are also considered as the adoption factors for IT innovation as well as in addition to Tornatzky and Fleischer.

While most of the studies embarked on the TOE's model, lies the fact that it conducted regarding IT adoption at the organizational level (Tsetse, Anthony (2014), Khairina, Yeow, Siew (2012), and Kuan, K.K.Y. and Chau, P.Y.K (2001)), in fact there are multiple social units who participate in the process of innovation. The decision in being made by individuals, group and organization, collectively. A review of the literature on Information Technology (IT) adoption indicates that there are several studies at the individual level.

In summary, while the Technological Factor focuses on the availability and attributes of technology, the Organizational Factor examines internal capabilities and readiness, and the Environmental Factor looks at external pressures and supports that influence the adoption of new technologies within a firm.

CONCLUSION

The study on the scope of Malaysia Critical Information Infrastructure (NCII), the use of Tornatzky's TOE adoption model, and the Action Plan model of Corporate Computer Forensics Investigation by UK's Information Assurance Advisory Council (IAAC) has never been done before by any academic researchers or any research group. This modest research effort was driven by a strong inclination to investigate the lacking factors of research on the both Independent and Dependent Variables despite the NCII and IAAC

are two critical category of government agencies and the former is an established council that has many giant international companies behind the council in the effort to combat the issue of information security, information assurance and responsive action plan for corporate with computer forensic investigation.

The inclusion of an additional independent variable of Information Management to measure the innovative adoption of Corporate Computer Forensic Investigation's Action Plan offers new insight to the field of Information and Records Management. None of the two variables, Information Processing and Storage yielded significant scores of factor analysis. The result shows the fact that the two Information Management variables require more extensive exploration to make them compatible and have strong relationship with seem-to-be compatible discipline of the computer forensic field. The positive side of knowledge contribution to the field of Information & Records Management is the battles to become pioneer in finding the link between those two disciplines which theoretically have some connection between them in providing evidence and discovering evidence.

REFERENCES

Accenture. (2003). *Web services: IT efficiency today...powerful business solutions tomorrow*. Retrieved from http://rvww-306.ibm.com/software/solutions/webservices/pdf/RTS_AB_hires.pdf

Agarwal, A., Gupta, M., Gupta, S., & Gupta, S.C. (2011). Systematic digital forensic investigation model. *International Journal of Computer Science and Security (IJCSS)*, 5(1), 118–131.

Awa, H.O., Ojiabo, U., & Emecheta, B.C. (2016). *Exploring the trend towards cloud computing: Literature review and current research. Cogent Business & Management*. [Ibid].

Barske, D., Stander, A., & Jordan, J. (2010). A digital forensic readiness framework for South African SMEs. *Information Security for South Africa (ISSA)*, 1-6. Sandton, Johannesburg: IEEE.

Beebe, N.L. (2005). A hierarchical, objectives-based framework for the digital investigations process. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.98.2406&rep=rep1&type=pdf

Carrier, B.D. (2003). *Open source computer forensic manual*. Available from: http://www.digital-evidence.org/

Casey, E. (2004). *Digital evidence and computer crime: Forensic science, computers, and the Internet*. Academic Press.

Ciardhuain, S. (2004). An extended model of cybercrime investigation. *International Journal of Digital Evidence*, 3(1), 1-22.

Coburn, N. (2006). Corporate investigations. *Journal of Financial Crime*. Retrieved from www.emerald.com/insight/content/doi/10.1108/13590790610678422/full/html?mobileUi=0&fullSc=1

Cohen, F.B. (2012). *Digital forensic evidence examination*. Fred Cohen & Associates.

Dong, L., Neufeld, D., & Higgins, C. (2009). Top management support of enterprise systems implementation. *Journal of Information Technology*, 24, 55-80. https://doi.org/10.1057/jit.2008.21

Duranti, L., & Endicott-Popovsky, B. (2010). Digital records forensics: A new science and academic program for forensic readiness. *Scholarly Commons*. Retrieved from commons.erau.edu/jdfsl/vol5/iss2/4/

Dzomira, S. (2014). Digital forensic technologies as e-fraud risk mitigation tools in the banking industry: Evidence from Zimbabwe. *Risk Governance & Control: Financial Markets & Institutions*, 4(2).

Fahmid, I. (2006). Enterprise computer forensics: A defensive and offensive strategy to fight computer crime. *Australian Digital Forensics Conference*. Retrieved from https://ro.ecu.edu.au/adf/

Freiling, F.C., & Schwittay, B. (2007). Common process model for incident and computer forensics. *Proceedings of Conference on IT Incident Management and IT Forensics, Stuttgart*.

Frost & Sullivan. (2015, February 18). Cybersecurity risks threaten digital integration in key process industries. LinkedIn SlideShare. Retrieved from www.slideshare.net/FrostandSullivan/cybersecurity-risks-threaten-digital-integration-in-key-process-industries

Grobler, C.P., & Louwrens, C.P. (2007). Digital forensic readiness as a component of information security best practice. In *New approaches for security, privacy and trust in complex environments* (pp. 13–24). Springer, Boston, MA.

Hameed, T., Counsell, S., & Swift, S. (2012). *Technology adoption in organizations: A review of the literature*. [Ibid].

Henriksen, H.Z. (2006). Motivators for IOS adoption in Denmark. *Journal of Electronic Commerce in Organizations*, 4, 25–39. https://doi.org/10.4018/JECO

Hitchcock, B., Le-Khac, N.-A., & Scanlon, M. (2016). Tiered forensic methodology model for digital field triage by non-digital evidence specialists. *Digital Investigation*, 16, S75–S85.

Imtiaz, F. (2006). Forensic computer crime investigation. In *Taylor & Francis Group*.

ISO/IEC 17799:2005. (2010, June 3). Retrieved from www.iso.org/standard/39612.html

Jeyaraj, A., Rottman, J., & Lacity, M. (2006). A review of the predictors, linkages, and biases in IT innovation adoption research. *Journal of Information Technology*, 21, 1–23. https://doi.org/10.1057/palgrave.jit.2000056

Johnson, R. (2006). Forensic computer crime investigation. *Taylor & Francis Group*.

Kauffman, R.J., & Walden, E.A. (2001). Economics and electronic commerce: Survey and directions for research. *International Journal of Electronic Commerce*, 5, 5–116.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response. *NIST Special Publication*, 10(800), 886.

Khairina, Y., Siew, E.G., & Yeow, P.H.P. (2012). Investigating the technological, organizational, and environmental influence on the adoption of audit technology among Malaysian audit firms. Retrieved July 3, 2014, from www.buseco.monash.edu.my

Kinuthia, J.N. (2015). Technological, organizational, and environmental factors affecting the adoption of cloud enterprise resource planning (ERP) systems. *Semantic Scholar*. Retrieved from https://pdfs.semanticscholar.org/fb6c/9f4d8648a9e39791694d9536d34af0aab2d2.pdf

Kohn, M.D., Eloff, M.M., & Eloff, J.H.P. (2013). Integrated digital forensic process model. *Computers & Security*, 38, 103–115.

Kruse, W., & Heiser, J.G. (2001). *Computer forensics: Incident response essentials* (1st ed.). Addison Wesley Professional.

Kruse, W., & Heiser, J.G. (2002). *Computer forensics: Incident response essentials*. Addison Wesley Professional.

Li, P., & Xie, W. (2012). A strategic framework for determining e-commerce adoption. *Journal of Technology Management in China*, 7(1), 22-35.

Martini, B., & Choo, K.-K.R. (2012). An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation*, 9(2), 71–80.

Mbugua Chahira, J., KinanuKiruki, J., & KipronoKemei, P. (2016). A proactive approach in network forensic investigation process. *International Journal of Computer Applications Technology and Research*, 5, 304-311. https://doi.org/10.7753/IJCATR0505.1012

McCreight, R. (2022). Reconceptualizing security vulnerabilities. In *Handbook of Security Science*. Springer, UK.

National Institute of Justice. (2008). *Electronic crime scene investigation: A guide for first responders* (2nd ed.). U.S. Department of Justice Office of Justice Programs. Retrieved from https://www.ncjrs.gov/pdffiles1/nij/219941.pdf

Nicolas, M., et al. (2020). Advanced technologies adoption and use by U.S. firms: Evidence from the annual business survey. *NBER Working Paper No. 28290*. Retrieved from https://www.nber.org/system/files/working_papers/w28290/w28290.pdf

Oliveira, T., & Martins, M.F. (2011). Literature review of information technology adoption models at firm level. *The Electronic Journal Information Systems Evaluation*, 14(1), 110-121. Retrieved from www.ejise.com

Palmer, G. (2001). A road map for digital forensic research. In *First Digital Forensic Research Workshop, Utica, New York* (pp. 27–30).

Pangalos, G. (2010). The importance of corporate forensic readiness in the information security framework. Retrieved from www.researchgate.net/publication/221015022_The_Importance_of_Corporate_Forensic_Readiness_in_the_Information_Security_Framework

Perumal, S. (2009). Digital forensic model based on Malaysian investigation process. *International Journal of Computer Science and Network Security*, 9, 38–44.

Pilli, E.S., Joshi, R.C., & Niyogi, R. (2010). A framework for network forensic analysis. *SpringerLink*. Retrieved from https://link.springer.com/chapter/10.1007/978-3-642-15766-0_21

PWC. (2016). *Forensic investigations and fraud risk management*. Retrieved from https://www.pwc.pl/en/services/forensic.html