

Cybercrimes prevention: promising organisational practices

Contextualising the special issue

The growth of e-commerce worldwide has enabled many organisations to deliver products and services using innovative, efficient, fast and cost effective business models. The digital economy continues to grow and makes a considerable contribution to the world economy. However, this relatively rapid growth has also caused even faster growth in cybercrimes, mainly due to the ease of committing these crimes, lucrative returns and the slowness of prevention efforts. Cybercrimes represent an existential threat to e-commerce and the need to effectively control their growth is urgent. As the relevant legislation and capabilities of law enforcement agencies is failing to catch up with the fast changing nature of crimes, businesses need to adopt innovative preventative strategies. This special issue focuses on how both large organisations and SMEs are making effective use of cybercrime prevention strategies. It also presents new research approaches and methodologies contributing to the theory and practice in this important emerging research domain.

Bera (2019) gave worldwide figures for cybercrimes for the year 2018, stating that almost 700m people were victims of some type of cybercrime. Cybercriminals generate revenues of \$1.5tn annually and cybercrime is estimated to cost \$6tnn businesses annually by 2021. Generally, when calculating cybercrimes losses, only reported direct losses are accounted for. The indirect losses such as reduction in sales, a reduction in market share, share price drop and other legal costs have a significant adverse impact on organisations; however, they are often overlooked. Many cybercrimes are not reported or are under reported by organisations because of possible reputational damage. Therefore, the figures given here could be under estimated below the real number of cybercrimes or the extent of damage. Nevertheless, these figures demonstrate how widespread these crimes are, with the resulting damages to the world economy in the trillions.

Doargajudhur and Dell (2019) identify that enhanced awareness of cybercrimes and alarming media reports about losses resulting from these crimes have intensified interest and attracted the attention of consumers, organisations, governments and researchers. Moreover, Vahdati and Yasini (2015) stressed that cybercrimes are the biggest threat to the survival of e-tailing. Whereas cybercrimes are a fast-evolving problem, prevention strategies and implementation have been slow amongst businesses. The losses caused by cybercrimes can damage both the finances and reputation of businesses (Vahdati and Yasini, 2015). These crimes and resulting fears also discourage many customers from buying goods online. Spanaki *et al.* (2019) and Tsohou and Holtkamp (2018) identified major challenges faced by consumers when they become victims of cybercrimes. These consumers faced issues such as credit problems (including rejection of loan applications), disruption to normal life routines and psychological difficulty in providing personal data to organisations and banks during an investigation.

Previous studies focused on issues related to the development and management of identity fraud policies (Njenga and Osiero, 2013; Coulson-Thomas, 2017). Syed (2018) investigated the effects of data breaches on the reputation of organisations on social media. Moreover, Doherty and Tajuddin (2018) researched prevention approaches including identifying risks and sharing knowledge about information security with other organisations. The majority of these studies are, however, directed at internal fraud in banking and other public and private sectors; there is very limited literature available in terms of theories on cybercrime management.



Njenga and Osiemo (2013) focused on fraud management policies and asserted that organisations should consider all stages in fraud management when developing an anti-fraud policy. Coulson-Thomas (2017) and Chen *et al.* (2015) suggested the importance of employees' participation in fraud management plans, whereas Soomro *et al.* (2016) focused on identity fraud prevention. Jalali *et al.* (2019) suggested that organisations need to synchronise their fraud management plans and protocols with other partners in their value chain to ensure that there are no weak links for fraudsters to exploit. Furthermore, Yoon and Kim (2013) investigated information security behavioural intention and suggested that learning opportunities for IT users helps achieve improved security by eliminating previous mistakes and addressing user-related weaknesses in organisations.

Chen *et al.* (2015) and Kolkowska *et al.* (2017) researched the effectiveness of internal audits and recommended that organisations should develop regular audit processes for improved fraud detection and prevention. Some studies have suggested providing training that can create awareness of cybercrime-related problems (Singh *et al.*, 2013; Chen *et al.*, 2015). Al-Khouri (2014) focused on cybercrime-related difficulties and how these are having an impact on investments in online retailing. Khajouei *et al.* (2017) and Alsmadi and Prybutok (2018) researched frauds in mobile commerce which they claim are different compared to traditional e-commerce-related frauds in terms of methods used by the fraudsters.

The extant literature covered above investigated various organisational practices related to fraud which is encouraging; however, the fact that the cyber frauds are still growing in terms of number and resulting financial losses suggests that existing approaches are still inadequate, hence the need for further research. This special issue aims to serve this need. With the rest of this editorial, we consider the papers included in this special issue which are presented in the following order.

The study by Campbell investigated the three most significant issues related to social engineering and security approaches for counteracting social engineering attacks. The three most significant issues produced three target areas for implementing best practices in countering social engineering attacks. The findings offer fresh insights into blending security processes, practices and programmes, and aim to provide leaders with increased understanding in implementing counteractions.

Chatterjee, Kar, Dwivedi and Kizgin's study identifies the factors influencing the citizens of India to prevent cybercrimes in the proposed smart cities of India. The study proposes a conceptual model identifying factors preventing cybercrimes. The study reveals that "awareness of cybercrimes" significantly influences actual usage of technology to prevent cybercrimes in the smart cities of India. The authors suggest that government initiatives and legal awareness have less impact towards the spreading of awareness of cybercrimes to the citizens of proposed smart cities.

Maitlo, Ameen, Peikari and Shah's study considers barriers to effective knowledge sharing in preventing identity fraud in online retail organisations using a case study approach. The study proposes a framework based on a reconceptualization and extension of the knowledge sharing enablers framework. The findings suggest the major barriers to effective knowledge sharing for preventing identity fraud are poor leadership support, limited employee willingness to share knowledge, lack of employee awareness of knowledge sharing, inadequate learning/training opportunities, insufficient trust in colleagues, poor information-sourcing opportunities and information and communications technology infrastructure, inferior knowledge sharing culture, insufficient evaluation on performance and inadequate job rotation. The research offers solutions for removing existing barriers to knowledge sharing in preventing identity fraud.

Asongu, Nwachukwu, Orim and Pyke's study complements the limited macroeconomic literature on the development outcomes of social media by examining the relationship between Facebook penetration and violent crime levels in a study of 148 countries using a

quantitative analysis. The study noted a negative relationship between Facebook penetration and crime. Furthermore, when the data set is decomposed into regions and income levels, the negative relationship is evident in the Middle East and North Africa, whereas a positive relationship is confirmed for Sub-Saharan Africa. Studies on the development outcomes of social media are sparse because of a lack of reliable macroeconomic data on social media.

Aloysius, Arora and Venkatesh's study found that, in a smartphone checkout setting, intention to shoplift was driven by experiential beliefs and peer influence. Experiential beliefs and peer influence was recognised as having a stronger effect for prospective shoplifters when compared to experienced shoplifters. The findings also indicated that in an employee-assisted mobile checkout setting intention to shoplift was driven by experiential beliefs. Moreover, peer influence and experiential beliefs had a stronger effect for prospective shoplifters when compared to experienced shoplifters.

Pérez-González, Trigueros Preciado and Solana-Gonzalez's study expanded current knowledge regarding security organisational practices and analysed its effects on information security management performance. The authors propose a theoretical research model together with hypotheses. The results validate that information security knowledge sharing, information security education/training and information security visibility and security organisational practices have a positive effect on management performance. The consideration of organisational aspects of information security should be taken into account by academics, practitioners and policymakers in SMEs. The study further recognises the need to develop empirical research on information security focused on SMEs and the need to identify organisational practices that improve information security.

Ikhaliya, Serrano, Bell and Louvieris employ mixed methods to evaluate a Facebook application including surveys, laboratory experiments and semi-structured interviews. The escalation of social engineering malware encourages a demand for end-user security awareness measures. Online social network (OSN) users have a higher propensity to malware threats due to the trust and persuasive factors that underpin OSN models. A Facebook video animation application (e.g. Social Network Criminal) creates security awareness and improves the threat avoidance behaviour of OSN users. Results validate the effectiveness of OSNs applications utilising a TTAT-MIP model – specifically the mass interpersonal persuasive (MIP) attributes. Practitioners are able to develop security awareness systems that more effectively leverage the intra-relationship model of OSNs. SNC enable persuasive security behaviour amongst employees and avoid potential malware threats. SNC support consistent security awareness practices by identification of new threats which may inspire creation of new security awareness videos. The structure of OSNs is making it easier for malicious users to undertake their activities without the possibility of detection. Thus, building a security awareness programme, using the TTAT-MIP model, organisations can proactively manage security awareness.

Ratten's study examines the impact of open innovation on cybercrime in technology firms using semi-structured in-depth interviews. The study seeks to understand the role of open innovation in terms of technology scouting, horizontal collaboration and vertical collaboration on cybercrime activity. The study found that there is a dilemma most technology firm's face in having a open innovation strategy and how to manage cybercrime. This means that a cooptation strategy is utilised that helps to balance the need to have open innovation but also protect intellectual property. Thus, managers of technology firms need to encourage open innovation as a strategy but manage the cybercrime that comes from sharing too much information in an online context.

Ekelund and Iskoujina demonstrate how to find the optimal investment level in protecting an organisations asset. This study integrates a case study of an international financial organisation with various methods and theories in security economics and mathematics. It combines theory and empirical findings to establish a new approach to

determining optimal security investment levels. The results indicate that optimal security investment levels can be found through computer simulation with historical incident data to find value at risk. By combining various scenarios, the convex graph of the risk cost function has been plotted, where the minimum of the graph represents the optimal invest level for an asset. The results can be used by business practitioners to assist them with decision making on investment to the increased protection of an asset. The originality of this research is in its novel way of combining theories with historical data to create methods to measure theoretical and empirical strength of a control (or set of controls) and translating it to loss probabilities and loss sizes.

In conclusion, the manuscripts collected here confirms the complexity of cybercrime threat with its implications for citizens, consumers, firms and their employees, public sector entities, cities, states, governments, technology and social media providers. Cybercrime represents an ongoing and significant threat driven by multiple agents. Several of the studies presented here offer recommendations and best practice frameworks to combat cybercrime. However, it is apparent that the cybercrime literature remains nascent and the academic community must endeavour to work with all parties to offer ongoing best practice.

Mahmood Hussain Shah

School of Strategy and Leadership, Coventry University, Coventry, UK

Paul Jones

School of Management, Swansea University, Swansea, UK, and

Jyoti Choudrie

Hertfordshire Business School, University of Hertfordshire, Hatfield, UK

References

- Al-Khouri, A.M. (2014), "Identity management in the retail industry: the ladder to move to the next level in the internet economy", *Journal of Finance & Investment Analysis*, Vol. 3 No. 1, pp. 51-67.
- Alsmadi, D. and Prybutok, V. (2018), "Sharing and storage behavior via cloud computing: security and privacy in research and practice", *Computers in Human Behavior*, Vol. 85, August, pp. 218-226.
- Bera, A. (2019), "Terrifying cybercrime statistics", March 12, available at: <https://safeatlast.co/blog/cybercrime-statistics/> (accessed 2 May 2019).
- Chen, Y., Ramamurthy, K. and Wen, K. (2015), "Impacts of comprehensive information security programs on information security culture", *The Journal of Computer Information Systems*, Vol. 55 No. 3, pp. 11-19.
- Coulson-Thomas, C. (2017), "Fraud, security risks and corporate responses", in Ahluwalia, J.S. (Ed.), *Corporate Ethics & Risk Management in an Uncertain World*, IOD Publishing, Mumbai, pp. 67-76.
- Doargajudhur, M.S. and Dell, P. (2019), "Impact of BYOD on organizational commitment: an empirical investigation", *Information Technology & People*, Vol. 32 No. 2, pp. 246-268.
- Doherty, N.F. and Tajuddin, S.T. (2018), "Towards a user-centric theory of value-driven information security compliance", *Information Technology & People*, Vol. 31 No. 2, pp. 348-367.
- Jalali, M.S., Siegel, M. and Madnick, S. (2019), "Decision-making and biases in cybersecurity capability development: evidence from a simulation game experiment", *The Journal of Strategic Information Systems*, Vol. 28 No. 1, pp. 66-82.
- Khajouei, H., Kazemi, M. and Moosavirad, S.H. (2017), "Ranking information security controls by using fuzzy analytic hierarchy process", *Information Systems and e-Business Management*, Vol. 15 No. 1, pp. 1-19.
- Kolkowska, E., Karlsson, F. and Hedström, K. (2017), "Towards analysing the rationale of information security non-compliance: devising a value-based compliance analysis method", *Journal of Strategic Information Systems*, Vol. 26 No. 1, pp. 39-57.

- Njenga, N. and Osiemo, P. (2013), "Effect of fraud risk management on organization performance: a case of deposit-taking microfinance institutions in Kenya", *International Journal of Social Sciences and Entrepreneurship*, Vol. 1 No. 7, pp. 490-507.
- Singh, A.N., Picot, A., Kranz, J., Gupta, M.P. and Ojha, A. (2013), "Information Security Management (ISM) practices: lessons from select cases from India and Germany", *Global Journal of Flexible Systems Management*, Vol. 4 No. 4, pp. 225-239.
- Soomro, Z.A., Shah, M.H. and Ahmed, J. (2016), "Information security management needs a more holistic approach: A literature review", *International Journal of Information Management*, Vol. 36 No. 2, pp. 215-225.
- Spanaki, K., Gürgüç, Z., Mulligan, C. and Lupu, E. (2019), "Organizational cloud security and control: a proactive approach", *Information Technology & People*, Vol. 32 No. 3, pp. 516-537.
- Syed, R. (2018), "Enterprise reputation threats on social media: a case of data breach framing", *The Journal of Strategic Information Systems*, Vol. 28 No. 3, pp. 257-274, available at: <https://doi.org/10.1016/j.jsis.2018.12.001>
- Tsohou, A. and Holtkamp, P. (2018), "Are users competent to comply with information security policies? An analysis of professional competence models", *Information Technology & People*, Vol. 31 No. 5, pp. 1047-1068.
- Vahdati, S. and Yasini, N. (2015), "Factors affecting internet frauds in private sector: a case study in cyberspace surveillance and scam monitoring agency of Iran", *Computers in Human Behavior*, Vol. 51, Part A, pp. 180-187.
- Yoon, C. and Kim, H. (2013), "Understanding computer security behavioural intention in the workplace: an empirical study of Korean firms", *Information Technology & People*, Vol. 26 No. 4, pp. 401-419.

About the Guest editors

Dr Mahmood Hussain Shah is Senior Lecturer in e-business within the School of Strategy and Leadership, Coventry University, UK. Previously he has held academic posts at the University of Central Lancashire, Cranfield University and the University of Hertfordshire. He is acting as Consultant to several UK banks and online retailers on information security and e-banking management-related issues. His present research interests include identify theft prevention in online retailing and e-banking as well as in health information systems and IS strategy. He has published several books in the area of information security, e-banking and mobile technologies. He has also published many papers in high quality journals such as the *Computer and Human Behaviour*, *European Journal of Information Systems*, *International Journal of Simulation Modelling*, *Health Informatics* and the *International Journal of Information Management*.

Paul Jones is Professor of Entrepreneurship and Innovation at Swansea University and Head of the Business Department. He is currently Editor of the *International Journal of Entrepreneurial Behaviour and Research* and Associate Editor of the *International Journal of Management Education*. Professor Jones is an active Researcher and publishes widely on issues related to entrepreneurial behaviour and small business management. Paul Jones is the corresponding author and can be contacted at: W.P.Jones@Swansea.ac.uk

Jyoti Choudrie is Professor of Information Systems in Hertfordshire Business School. Professor Choudrie has maintained an active media profile in issues such as the digital divide, social inclusion, entrepreneurship, innovation and broadband development. She has also attained expertise in the non-adopters and adopters research area that has led her to understand the digital divide where her research influence lies. Professor Choudrie has published widely in international journals such as *Information Systems Frontiers*, *Journal of Business Research* and *Government Information Quarterly*, where her work is well cited. Professor Choudrie is presently researching older adults and information communication technologies where her interest is on the adoption and diffusion of technologies, with an emphasis on entrepreneurship for older adults. Professor Choudrie is also focused on examining and understanding the digital divide by considering internet access for older adults.