Are small medium enterprises cyber aware?

Homan Forouzan1, Amin Hosseinian-Far2, Dilshad Sarwar3

1, 2, 3Department of Business Systems & Operations, University of Northampton, NN1 5PH, UK

{Homan.Forouzan; Dilshad.Sarwar;Amin,Hosseinianfar}@northampton.ac.uk

**Abstract.** Technology has become a pivotal point in our society, this dependency is becoming increasingly more critical on a daily basis. . This ranges from people to businesses and on a larger scale government organisations who are now increasingly focusing on becoming more cyber resilient. This paper intends to provide an overview as to why a comprehensive knowledge management framework is necessity for SMEs on tackling cyber and cyber-enabled crimes. The paper explores new sources of data to reliably understand the importance as to why such a framework is required. This type of system can pave the way for SME’s to devise their cyber strategy and to be able to respond efficiently to cyber-related incidents. One of the cyber weakness and vulnerabilities for the SME’s are through their interactivity and or engagement with their suppliers and customers. Namely the interactions which take place via their respective internet sites, email communications, ports (using external devices, USB, CD drive, SD cards etc...) or the router (The use of their WIFI systems). The benefits of this framework model will be primarily to educate SME’s in becoming more cyber resilient and provide them with the knowledge, awareness and techniques to identify weaknesses and vulnerabilities in their computer networks, devices and internet usage.

**Keywords:** Cybercrime, Cyber, Crime, Conceptual Framework, Design Science Research, Small and Medium Sized Enterprises

1 INTRODUCTION

The term SME’s can be defined as any business being a small and or medium sized enterprises (SMEs) with fewer than 250 employees and a turnover of less than £50 million. Three different categories come under the SME umbrella; micro, small and medium size businesses (Sainidis et. al, 2016). Micro businesses are those employed with nine or less employees, according to the statistics from figure four that accounts for ninety-six percent of all the operating businesses within the UK. Small businesses employ just under forty-nine employees and medium businesses employ just under two hundred and forty nine employees, which makes up three percent of the total businesses operating in the UK. In total, there are only 8,000 large businesses that employee over the 250 employees and this in comparison to all the businesses operating in the UK is only 0.1 percent (FSB, 2018).

There are millions of people within the UK employed by the SMEs, and as such the SMEs are one of the main driving factors of the UK economy in creating more employments then larger organizations. As the SMEs dependency of technology is rapidly advancing so are the opportunities of cyber criminals to carry out increasingly complex and sophisticated crimes. This could also have a ripple effect on larger businesses and organisations who are in business relationship with those SMEs. As cyber criminals could either attack the intended SMEs or even use those as proxies to launch an attack on the lager businesses or organizations.

According to Federation of Small Businesses (FSB, 2018) there are two main vulnerability factors why businesses increasingly face cyber threat challenges they are technological and organizational vulnerabilities.

* Technological vulnerabilities: the weaknesses of networks, devices, hardware, software and programmes, which may be exploited for breaches and attacks.
* Organisational vulnerabilities: the weaknesses within the staff (who either knowingly or unknowingly divulge information), the processes and procedures within that SME. Limited staff knowledge and understanding of the technological vulnerabilities.

For SMEs, such vulnerabilities could be the supplier’s data, customer’s information, and financial details held on their devices. One could argue that the Internet is one of the most important assets for SMEs as through the Internet they will build upon their reputation, advertise and sale their products / services. If the integrity of such assets are breached that would mean significant financial and reputational consequences to the SME’s. If SME’s are not cyber resilient then such attacks and breaches could push the company towards liquidation.

In conjunction with these vulnerabilities, most SME’s also function with limited resource and knowledge constrains, for example lesser assets base, due to their seize the limitations of the bargaining power, limited access to finance capital, and limited internal resource capacity (Hayes, et al. 2013). Consequently, most SME’s will have limited access to resources and knowledge to be able to grow their cyber resilience. As a result of these limitations alongside the organisational and technological vulnerabilities, generally SME’s are not well positioned to be able to tackle their own internal cyber-attacks and exposures (FSB, 2018).

There are currently a number of different products, guidance and approaches available on the market for SME’s to be able to increase their cyber resilience, however due to the limited resources SME’s have the capacity and their lack of awareness allows for a wider intelligence gap around cyber resilience. One of the key arguments is that larger organisations are more robust when encountering cyber-attacks as they are more adequately equipped and prepared with more financial and human resources; on the other hand, SME’s are more vulnerable in the approach to attacks due to their poorer resilience capability (Valli, et al. 2014). What is apparent is that the need for SME’s who form ninety nine percent of all the UK businesses to have cyber resilience embedded as part of their core business functions. In order to raise the profile and the importance of embedding cyber security within SMEs it is imperative that larger organisations, government, and law enforcement agencies share the burden of resilience to support SME’s for a successful economy.

This paper is organised as follows: Section 2 provides a succinct overview of the methods used for the development of a conceptual framework that can inform a pertinent knowledge management system for preparing small and medium sized enterprises additionally improving their cyber resilience. Section 3 outlines the developed conceptual models. A critical discussion of results is provided in Section 4. The paper is concluded in Section 5.

2 METHODS

Methodology is at the heart of any research and plays a pivotal point in providing a structure for that research. Within this research the researcher intends to use Design Science Research (DSR) qualitative approach to capture the information through iterative interviews.

Design Science Research can be described as a road map that focuses on a set of procedures or guidelines for evaluation and repetition within research development. Design Science Research Methodology results in the development of a system and/or an artefact and has gained pace in the information technology and engineering subject areas. However, the methodology has been applied in other subject disciplines where there is no tangible artefact. For instance, Montasari (2021) has applied the methodology to develop a framework for magistrate and crown court judges to assess and evaluate cybercrime cases.

Such an approach emphasises the performance and development of the implemented artefacts with the clear purpose in mind to improve the well-designed performance of that artefact. DSR is aimed at developing a new approach in tackling the said problem through understanding the behavioral aspects attributed to that research by improving or considering new approaches, techniques and methods. Van Aken (2005) describes DSR as an instrument in developing knowledge to assist experts of that particular field to design and implement a solution to tackle the said problem. Such an approach works on three main factors which are to describe, explain and forecast the problem with an element of providing a solution for that problem. According to Hevner (2004) the purpose of DSR is accomplishing knowledge and obtaining a bigger understanding of the said problem by developing a designed artefact.

DSR is applied to a number of artefacts namely human / computer interfaces, algorithms, languages and design methodology. There are numerous variants to the Design Science Methodology (DSRM) for example computer science (Takeda, 1990) and engineering (Fulcher and Hills, 1996).

According to Peffers (2018) research in such fields are seen as a mission in understanding the concept of the current problem and ways to improve and develop human performance. Design science research has had its footprints in many fields and disciplines, more notably in information technology and engineering. What is apparent is that DSR is not confined to one set of guidelines or rules; there are a number of different methods, approaches and techniques used by Design Science Research (Peffers, 2007 and 2018).

****2.1 Interviewees Profiles****

One of the main aspects of this research is heavily reliant on a range of different interviews being completed, in order to gain a better understanding of the issues and to be able to work towards implementing a knowledge management framework to support SMEs. Interviews will provide a platform to the researcher to support in building the framework of this project. In order to get a detailed understanding of the problem the researcher intends to conduct ten interviews from different sources namely:

• SMEs and start-ups - their understanding of cybercrime and the adequate provision provided to them by support agencies, insurance companies and the law enforcement agencies.

• The law enforcement agencies – to understand the police and government approach towards cybercrime and the current measures in place in supporting SMEs. In addition, to understanding the current crime trends, methods, and approaches that affect SMEs.

• Companies Supporting SMEs - It is essential for the researcher to be aware on products currently available in supporting SMEs, in order to gain an in depth understanding of what they provide and to avoid duplications.

• Academics – liaising with subject matter experts to understanding the areas of vulnerabilities and weaknesses that SMEs encounter.

The purpose of the interviews was to obtain comments and feedbacks from the interviewers around their experience and knowledge on the developed framework. Although there will be ten participants within this research, the number of interviews conducted were far higher than the number of participants. During this research thirty interviews were carried out this resulted to three interviews per participant. The comments and feedback provided by the interviewee enables the research team to identify any shortcomings or missed variables within the developed framework. Such feedback proved to be a crucial contributor to the process of developing a fit for purpose knowledge management framework.

3 RESULTS

After conducting thirty interviews the output from the comments and feedback provided on the proposed conceptual modelling framework model was embraced within Figure 1 to Figure 6. The modelling tool used to develop this framework is called a Systemigram. Systemigram was used to create a structured approach as such visualisation would be more effective in demonstrating what the framework is actually trying to illustrate.

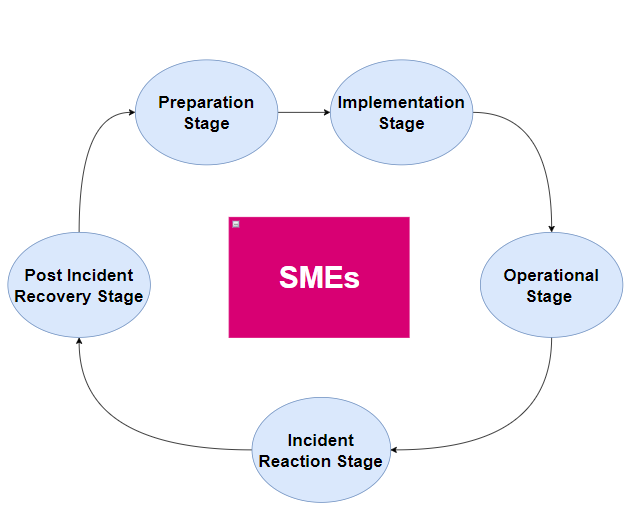


Figure 1: The conceptual framework cycle Iteration Three.

Figure 1 illustrates the conceptual model framework cycle that forms the foundation of the knowledge management framework to support SMEs in protecting their business from cyber-attack. The conceptual model consist of five stages, the preparation stage, implementation stage, operational stage, incident reaction stage and post incident recovery stage.

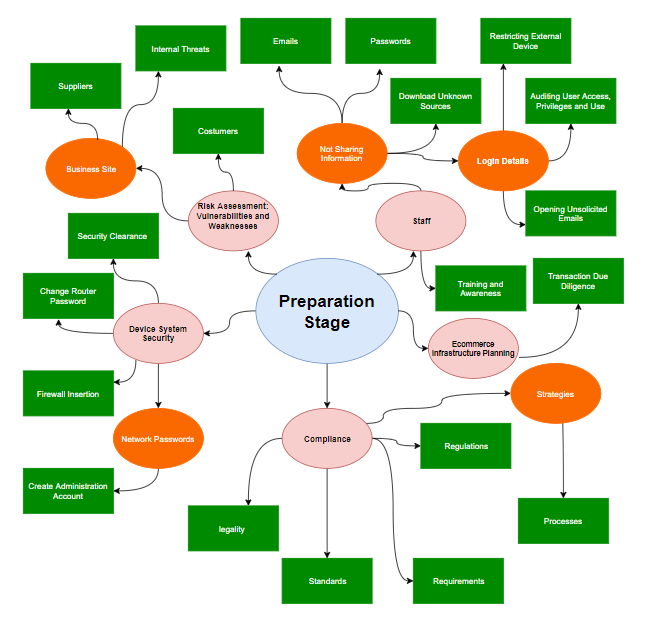


Figure 2: Illustrates the first stage of the framework - The Preparation Stage

The preparation stage is the most important stage of the conceptual framework as this will alert SMEs to identify and explore their businesses weaknesses and vulnerabilities. As highlighted within Figure 2, SMEs shall navigate through each of the strands (staff, ecommerce infrastructure planning, compliances, device system security and risk assessment strand) to ensure that each processes and actions are considered.

The staff strand highlights periodical staff learning and development processes to ensure that SME staff are adequately trained and more importantly aware of the recent threats, risk, harm and social engineering methods that staff could fall foul of as victims. If these are not addressed there could be significant business damage both in terms of reputational and financial. The ecommerce infrastructure planning strand demonstrates the necessity for SMEs to ensure that they have a transaction and due diligence process in place preventing spear phishing or any other forms of breaches on their invoices or receipts. The compliance strand alerts the SME to contemplate and follow some of the regulations, standards and requirements relevant to their business. Complying with the appropriate social and ethical factors to prevent the latter, significantly impacts the business. Consideration needs to be given to the legality of the business and the work that is intended to be carried out to prevent any criminal proceedings attributed to the business.

The device system security strand highlights the importance of periodical system security measures to be considered for the business. The following considerations are provided;

* Having firewalls and Anti-virus installed on networks and devices to monitor and control incoming and outgoing network traffics. Such barriers will work in preventing malware, breaches or other forms of attack penetrating the network and devices within the business.
* Having mandatory passwords for all devices and networks within the business, creating an administration account to restrict employee’s access to certain important accounts, folders and files.
* The use of a two-factor authentication (2FA) system in place for those more important accounts, folders and files.

The risk assessment strand highlights the importance to businesses in having secure systems in place to protect their ICT (information communication technologies). Therefore the need to identify and address their ICT vulnerabilities and weaknesses. These could consist of communications from suppliers, customers and staff interactions with the ICT (FSB, 2018). Fundamentally it is imperative that these potential risks are identified before a business is started as such risks if not mitigated could cause financial, reputational damage and can lead the businesses becoming bankrupt.

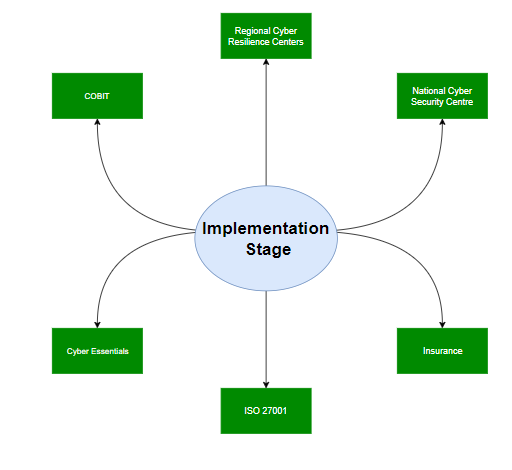


Figure 3: Illustrates the second stage of the framework - The Implementation Stage.

The implementation stage as illustrated in Figure 3 allows business to consider the use of available business support services (such as NSCS, RSRC, Cyber Essentials, COBIT, ISO 27001, and insurances companies) to be up-to-date with topical cyber trends, threats, methods and techniques which will assist SMEs in raising their cyber security awareness.

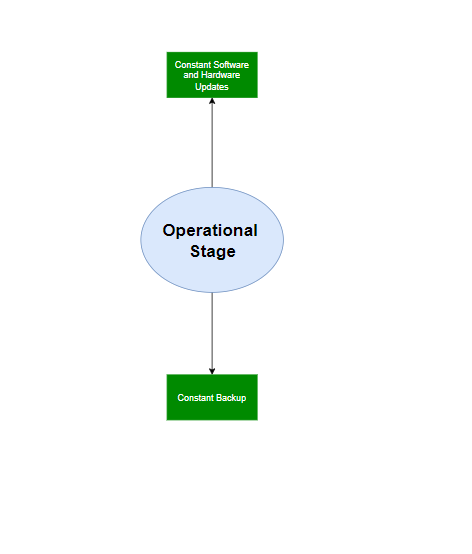


Figure 4: Illustrates the third stage of the framework - The Operational Stage.

The operational stage as illustrated in figure 4 highlights the necessity for businesses to have periodical software and Hardware device updates and frequent data backups. Data security is extremely critical to any business or organisation. As such, leakages or breaches of information could have significant impact on the business financially, the functionality and reputation.



Figure 5: Illustrates the fourth stage of the framework - The Incident Reaction Stage.

The incident recovery stage as illustrated in Figure five highlights the consideration that needs to be given In light of a breach, hacking and or a cyber-attack. To make contact with Action Fraud, insurance company, in an emergency to call 999 and none emergency to call 101.

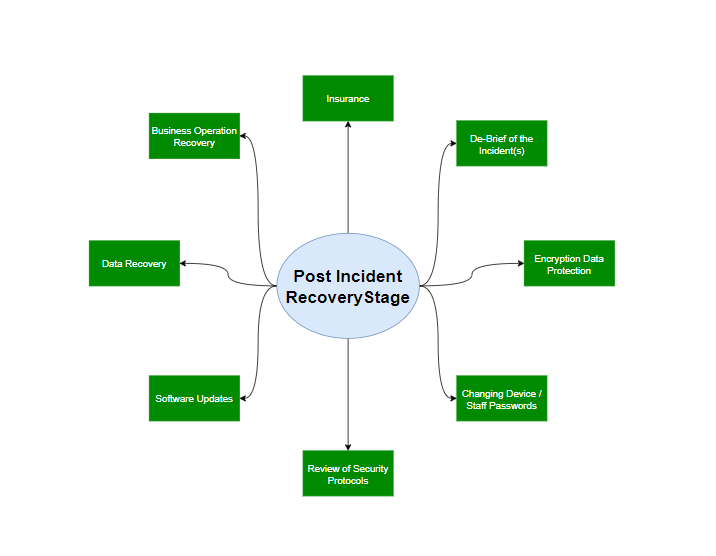


Figure 6: Illustrates the last stage of the framework - The Post Incident Recovery Stage.

The Post Incident Recovery Stage as illustrated in figure 6 highlights what SMEs should do after they have been victims of a cyber-attack. Considerations needs to be given to the following:

* Providing encrypted data protection for devices and staff to protect loss of data.
* Reviewing the business recovery plan, having contingencies in place to run the business on the backup when the Information communication technologies, systems and devices are all cleared of any malware.
* Recovering data through utilising accredited agencies,
* Software updates,
* Review of security Protocols and Identifying where the weakness and vulnerabilities where and putting contingencies in place to address them,
* Reporting the attack to insurance company for compensation and further assistance for business recovery,
* Changing Device / Staff Passwords,
* It is extremely important that debrief is held to identify knowledge gap and learning.

4 DISCUSSION

Over previous decades, the UK Economy has moved towards a very complex communications infrastructure within the digital environment. As a result of this, there are tremendous opportunities now available for small to medium sized enterprises. This digital economy information age started quite innocently with the introduction of the personal computer, mobile telephone, the Internet and email. Technology has advanced considerably resulting in the introduction of tablets, smart phones and social media. Although the emergence of such technological advancements has helped to reduce cost considerably for businesses, this has helped to increase the overall efficiency and provide global reach for small to medium enterprises (Attaran, et al. 2019, Porter, et al. 2019). The Internet thus far has offered phenomenal opportunities for SMEs, with these opportunities there are also additional risks.

With the adoption of the Internet and development of various digital business models, small to medium enterprises must have a web presence to remain competitive. Most people are now using the Internet to order and purchase their desirable products and services therefore business are more internet dependent than ever (Okamoto, et al. 2017). Although, many benefits are made available to these types of businesses through their cyber presence, there have also been numerous consequential challenges. Businesses are now facing complex dilemmas such as the ensuring privacy and security of consumer data, as well as enhancing the customers’ trust. The digital and online business models have been evolving since the first Business to Consumer (B2C) instance in 1997, and so as adversaries’ techniques targeting such online platforms (Timmers, 1998, Webb, 2001). The rise in the adoption of cyber platforms has also seen a larger increase in related cyber, and cyber-enabled crimes. This research paper has focused on how to support SMEs from falling fowl of cyber criminals and more importantly highlights how organisations can be resilient to cyber attacks.

The findings of the results identified within this research highlighted that despite the increases in cyber-attack year on year on SMEs there is a lack of investment on cyber security within the business infrastructures. This was supported with one of the interview participants who stated that cybersecurity was not at the forefront of their business strategy, as their main focus was on making revenue. Such false beliefs highlighted not just through the literature review but also through interviews conducted with a number of SMEs during this research that their business would not be targeted as they were of an opinion that they had nothing of value for cyber criminals was rather concerning that such lack of knowledge and awareness was still apparent in the current ever dependant digital society. There may be a number of factors as to why such misconceptions are still apparent within SMEs;

• Lack of awareness campaigns from government sectors, organisations, their party providers,

• Lack of a one stop shop platforms so that SMEs could be sign posted in identifying cyber related advice when setting up or running a business,

• Lack of mandatory enforcements by governing bodies on making cyber compliance compulsory for SMEs.

There are at times misconceptions by SME’s that staff are adequately trained and educated relating to basic cyber-security awareness. Clearly as highlighted within this paper such assumptions could be costly to a business or an organisation. One of the interview participant’s touched upon the fact that that some of the elementary process were not being carried out for example staff were not aware that passwords needed to be changed periodically. Such findings were alarming as assumptions of this nature would be detrimental to SMEs whom without the adequate cyber security measures could be left with no option but to terminate their business in light of an attack as there could be exposures of significant financial and reputational damage to the business.

The results from the interviews further highlighted that there are increasing needs for a knowledge management framework for SMEs to consider implementing as the purpose of this framework would be essential in raising understanding, awareness and knowledge of the significance of cyber security within SMEs. The benefits of such a framework would be invaluable in forewarning SME’s in considering risk factors that need to be well-thought-out before a business is started, whilst the business is functioning and in light of an attack being resilient in keeping the business operational. This does not mean that the framework is the ‘be-all and end-all’ but more of a tool to support SMEs in preventing cyber-attacks or in light of an attack to be resilient.

The proposed conceptual model intends to reduce technological vulnerability, organisational vulnerability, improve policing of cybercrime and cyber criminals. Where there is a reduced level of pliability across digital networks, cost imposed on businesses can be phenomenal. These costs can be detrimental to SMEs both reputationally and financially. The costs of these vulnerabilities are not limited to the attacks directly influencing the SME but rather the day to day functioning of the business. For instance, the SME’s ability to meet customer needs, meet order requests, obtain new customers and the digital reputation of the SME. As SME’s main concern is to focus on developing and sustaining their businesses, SMEs tend not to have the skills base or the resources to adequately match cyber threats and vulnerabilities as highlighted within this paper. Therefore, it is imperative that cyber resilience is adequately and appropriately directed to support SMEs.

Further benefits of such a framework were highlighted by another interview participant, that the conceptual model mitigates start-ups and SMEs falling fowl of becoming victims of a cyber-attack as through early involvement in raising awareness. Furthermore, being mindful of the information contained within the proposed conceptual model can help mitigate risks and identify digital vulnerabilities.

5 CONCLUSION

The findings of the results identified within this paper highlighted that despite the increases in cyber-attack year on year on SMEs there is a lack of investment on cyber security within the business infrastructures. This was supported by one of the interviewee participants who stated that cybersecurity was not at the forefront of their business strategy, as their main focus was on making revenue. Such false beliefs highlighted not just through the literature review but also through the interviews conducted that some SMEs believed that their businesses would not be targeted as they had nothing of value for cyber criminals, was rather concerning that such lack of knowledge and awareness was still apparent in the current ever depended digital society. There could be a number of factors as to why such misconceptions are still apparent within SMEs;

* Lack of awareness campaigns from government sectors, organisations, third party providers,
* Lack of a one stop shop platforms so that SMEs could be sign posted in identifying cyber related advice when setting up or running a business,
* Lack of mandatory enforcements by governing bodies on making cyber compliance compulsory for SMEs.

The conceptual framework has many benefits one in particular is that it mitigates start-ups and SMEs from falling fowl of becoming victims of a cyber-attack as through early involvement in raising awareness, being mindful of the information contained within the proposed conceptual model can help mitigate risks and identify digital vulnerabilities.

6 REFERENCES

Attaran, M. and Woods, J., 2019. Cloud computing technology: improving small business performance using the Internet. *Journal of Small Business & Entrepreneurship*, *31*(6), pp.495-519.

FSB, 2018. Cyber Resilience: How to Protect Small Firms in the Digital Economy, FSB, UK. Available at https://www.fsb.org.uk/docs/default-source/fsb-org-uk/FSB-Cyber-Resilience-report-2016.pdf?sfvrsn=0 [Accessed 13th July 2019].

Forouzan, H., Jahankhani, H. and McCarthy, J., 2018. An Examination into the Level of Training, Education and Awareness Among Frontline Police Officers in Tackling Cybercrime Within the Metropolitan Police Service. In *Cyber Criminology* (pp. 307-323). Springer, Cham.

Fulcher, A.J. and Hills, P., 1996. Towards a strategic framework for design research. Journal of Engeering Design, 7(2), pp.183-193.

Hayes, J. and Bodhani, A., 2013. Cyber security: small firms under fire [Information Technology Professionalism]. *Engineering & Technology*, *8*(6), pp.80-83.

Hevner, A. R.; March, S. T.; Park, J. & Ram, S. Design Science in Information Systems Research. MIS Quarterly, 2004, 28, 75-106. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.103.1725&rep=rep1&type=pdf

Montasari, R., 2021. *The comprehensive digital forensic investigation process model (CDFIPM) for digital forensic practice*. University of Derby (United Kingdom).

Okamoto, T., Yatsuhashi, J. and Mizutani, N., 2017. Priorities of Smartphone Online Shopping Applications for Young People.

Peffers, K., Tuunanen, T., Rothenberger, M.A. and Chatterjee, S., 2007. A design science research methodology for information systems research. Journal of management information systems, 24(3), pp.45-77.

Peffers, K., Tuunanen, T. and Niehaves, B., 2018. Design science research genres: introduction to the special issue on exemplars and criteria for applicable design science research. *European Journal of Information Systems*, *27*(2), pp.129-139.

Porter, M.E. and Kramer, M.R., 2019. Creating shared value. In *Managing sustainable business* (pp. 323-346). Springer, Dordrecht.

Sainidis, E. and Robson, A., 2016. Environmental turbulence: impact on UK SMEs’ manufacturing priorities. Management Research Review, 39(10), pp.1239-1264.

Takeda, H., Veerkamp, P. and Yoshikawa, H., 1990. Modelling design process. AI magazine, 11(4), pp.37-37.

Timmers, P., 1998. Business models for electronic markets. *Electronic markets*, *8*(2), pp.3-8.

Valli, C., Martinus, I.C. and Johnstone, M.N., 2014. Small to medium enterprise cyber security awareness: an initial survey of Western Australian business.

Van Aken, J.E., 2005. Management research as a design science: Articulating the research products of mode 2 knowledge production in management. *British journal of management*, *16*(1), pp.19-36.

Webb, H. and Webb, L., 2001. Business to consumer electronic commerce Website quality: integrating information and service dimensions. *AMCIS 2001 Proceedings*, p.111.