The Antecedents of Cyber-Security Implementation: a study of the cyber-preparedness of UK Social Enterprises.

Dr Gareth R.T. White [1*]

gareth.white@southwales.ac.uk

Dr Robert A. Allen [2]

robby.allen@cranfield.ac.uk

Dr Anthony Samuel [3]

samuela3@cardiff.ac.uk

Dr Ahmed Abdullah [1]

ahmed.abdullah@southwales.ac.uk

Dr Robert Thomas [1]

Robert.thomas1@southwales.ac.uk

[*] Corresponding Author

[1] University of South Wales. Pontypridd, CF37 1DL. United Kingdom.

[2] Cranfield University. Shrivenham Campus, Shrivenham. SN6 8TS. United Kingdom.

[3] Cardiff University. Colum Road, Cardiff. CF10 3AT. United Kingdom.

Abstract

The cyber-security of organisations is a subject of perennial concern as they are subject to mounting threats in an increasingly digitalised world. While commercial and charitable organizations have been the objects of cyber security research, Social Enterprises have remained unexplored. As Social Enterprises have become increasingly important features of social and economic development, so their prominence as potential targets of cybercrime also increases.

In order to address this knowledge gap, this study examines the factors that influence the cyber-preparedness of Social Enterprises in the UK. Through the use of semi-structured interviews with Social Enterprise, these factors are found to comprise the characteristics of the enterprise, the characteristics of the enterprise management, resource constraints, experience of cyber attacks, usage of IT, and awareness of cybersecurity schemes and resources. These insights provide valuable guidance for SE owner-managers, SE support agencies and policy-makers when considering the cyber security of SEs.

These findings are of immediate concern to social enterprises but also to other organizations that are engaged in partnerships with them as social enterprises may afford ‘gateway’ opportunities to those with malicious intent.

Managerial Relevance

Social Enterprises are institutions that balance the competing needs of commercial success and the primary objective of delivering social value. The management of cyber security places a further demand upon these resource-constrained organizations, and upon the capacity of individual owner-managers. However, the nature of these enterprises suggests that they present unique opportunities to cyber criminals: their association with vulnerable individuals, use of volunteer resources and links with government systems, and rising

visibility among the business landscape, makes their management of cyber security a pressing issue. This study has identified a general lack of awareness of cyber security reporting requirements, preventive measures and support schemes among social enterprises in the United Kingdom. Organizations that represent social enterprises, and local and national governing bodies, need to review the efficacy of their current methods of communicating with and educating this increasingly important sector. However, social enterprise owner-managers must also take responsibility for raising their own awareness of the current regulations and for effecting appropriate cyber security management within their organizations. This may be aided by the collaborative activity of groups of social enterprises, for instance, among those that operate within defined Social Enterprise Places, or among other collective arrangements.

KEY WORDS: social enterprise, cyber security, cyber crime

Introduction

The continued development and adoption of internet technologies and devices has sparked a concomitant increase in the research and development of methods for detecting and understanding cyber-crime (Chaffey and White, 2011; Stephens, 2005) as well as technological solutions for preventing digital crimes (see for example White, 2017). A significant proportion of the literature on cyber-crime explores the context of commercial organisations but comparatively little of that is of a scholarly nature (Paoli, Visschers and Verstraete, 2018).

To date, no research has been conducted that explores cyber-crime in the context of Social Enterprises (SE). This is significant since SEs are becoming an increasingly important element of modern society. SEs are a form of organisation that aim to fulfil some pertinent social purpose through commercial means (Doherty et al, 2014; Peattie and Morley, 2008). Frequently termed ‘hybrid’ organizations due to their dual social and commercial mission, the majority of profits that they generate are reinvested in order to ‘respond to the need of others’ (Dees, 2012, 321): for example, cafes that provide ‘experience and accredited training’ for homeless people (Café from Crisis, 2020). The number of SEs in the United Kingdom (UK) rose by 33% between 2012 and 2015: 52% of them reported a growth in their turnover while 59% offered a new product or service in the last year (Villeneuve-Smith and Temple, 2015). UK SEs operate in over eighteen different industries, 76% of them break even or make a profit and 41% of them create new jobs, predominantly for disadvantaged people (Villeneuve-Smith and Temple, 2015). Consequently, these organizations are rapidly emerging as an economically as well as socially significant sector of activity.

In addition to their nascent role in social and economic development, SEs exhibit several characteristics that further suggest that their ability to manage cyber-security requires examination -

First, SEs often have a lack of financial and professional resources compared to commercial organisations (White, Samuel, Pickernell, Taylor and Mason-Jones, 2018; Rey-Marti, Ribeiro-Soriano and Palacios-Marques, 2016; Katre and Salipante, 2012). Furthermore, they typically employ individuals with low levels of skills (Rey-Marti et al., 2016; Richards and Reed, 2015; Doherty et al., 2014; Lui, Takeda and Ko, 2014). SEs are therefore unlikely to possess the internal skills and capabilities to manage cyber-security weaknesses, nor are they likely to possess the financial resources to hire such skills (Martin 2015; Lehner and Nicholls, 2014; Reiser and Dean, 2014).

Second, the employment of individuals with low levels of skill makes SEs open to social engineering attacks (Bullee, Montoya, Pieters, Junger and Hartelk, 2018). It may also result in the improper use of data and information technologies, for example, through unintentional disclosure of sensitive data, or the use of information systems in a manner that circumvents policy or security measures (Ani, He and Tiwari, 2019).

Third, SEs are likely to be in possession of the details of the organisations and vulnerable individuals that they serve or employ (Doherty, Haugh and Lyon, 2014; Samuel, White, Jones and Fisher, 2018). This information may be highly detailed and contain sensitive data such as personal histories, criminal records or medical conditions. While the protection of personal data is an issue of concern for all organisations it is evident that the nature of SEs makes them notable targets for the malicious acquisition of data. Furthermore, SEs are frequently employed by local authorities to service the social needs that have become exposed during a period of global austerity: almost half of SEs trade with the public sector (SEUK, 2019). Consequently, SEs may be in possession of sensitive government data and become portals for access to important government systems.

Collectively, SEs represent an influential sector of commerce that are imbued with notable characteristics that make them not only susceptible to cyber-attack but also the organisation and the individuals with whom they engage have the potential to be harmfully impacted by their effect. Their increasing presence as socially and commercially viable and successful organisations, for instance 52% of UK social enterprises grew their turnover in the last year (SEUK, 2019), may also be conspiring to raise awareness of their vulnerabilities to those with malicious intent. Therefore, as their popularity increases this may increase their prominence as subjects of cyber crime: a trajectory that has been witnessed in the growth of cyber crime against larger charitable organizations (Charity Commission, 2019).

This paper therefore aims to understand the factors that influence the cyber-preparedness of social enterprises in the UK. In achieving this goal, the paper systematically unpacks the factors that support and hinder the preparedness of SEs to deal with cybercrime. The paper is structured as follows: first, a review of the cyber-crime literature is presented before the key issues and the characteristics of SEs are formulated as a conceptual framework and research questions. Following this the methods of the study are detailed before the findings of the analyses are presented. The paper closes with statements of contributions and suggestions for future research.

Cyber-crime

Cyber-crime is a difficult term to define accurately, and thereby a difficult act to counter, since it covers a plethora of nefarious behaviours that may be conducted wholly or partly online, by individuals or groups, upon other individuals, groups, organisations or nations (Ngo and Jaishankar, 2017; Afolayan, Plant, White, Jones and Beynon-Davies, 2015; Deibert, 2011; Marcum, Higgins, Freiburger and Ricketts, 2010). Rising academic interest in cybercrime detection and prevention is evidenced by several recent special issues in journals across management, technical and professional disciplines. These include the special issue in which this article is published, the Journal of Crime and Justice (Bossler and Berenblum, 2019), Information Technology & People (Shah, Jones and Choudrie, 2019) and Computers and Security (Choo, Gai, Chiaraviglio and Yang, 2020).

Despite the recent media reports of cyber-attacks, such as the recent 'ransomware' attack on the UK's National Health Service that cost over £90 million and resulted in 19,000 medical appointments being cancelled (Telegraph, 2018), and numerous efforts by governments and expert institutions to improve the cyber-awareness and readiness of organisations, many are still underprepared (O'Rourke, 2018). For instance, a study of Ghanaian corporations showed that while their knowledge of information technology was good their knowledge of cyber issues was poor (Adu, 2018). Similarly, the Cyber Security Breaches Survey (CSBS, 2018), that presents a detailed examination of the cyber-attacks and preventive measures of commercial organisations and charities in the UK, shows that while both types of organisations had suffered from cyber-attacks in the last twelve months (43% of businesses and 19% of charities) less than 30% of either had a formal cyber security system in place.

Some research suggests that cyber-attacks are becoming more frequent, and there is a growing body of literature that proffers instruments for assessing cyber risks (Kure, Islam and Razzaque, 2018; Bartolini, Ahrens and Zascerinska, 2018; Ali, Almogren, Hassan, Rassan and Bhuiyan, 2018). The severity of cyberattacks seems to have plateaued (Xu, Schweitzer, Bateman and Xu, 2018), yet a single cyber-attack is estimated to cost an average of $229,000. The global cost of cyber-attacks is thought to be several hundreds of billions of dollars (RAND, 2018). As a result of this, one third of organisations are planning to take out cyber insurance (O'Rourke, 2018). However, this may not be a viable option for SEs that are frequently beset by considerable financial constraints. Furthermore, it is questionable whether financial compensation for being the subject of cybercrime is a meaningful support for SEs, whose purpose is usually socially motivated rather than driven by purely profit. SEs are measured not only on their financial performance but also on their societal value or benefit. Consequently, just as they find their social value difficult to measure (Ebrahim, et al., 2014; Huybrechts and Nicholls, 2013; Zainon, Ahmad, Atan, Wah, Bakar and Sarman, 2014) so is the totality of the impact of cyber crime difficult for SEs to measure and therefore insure against.

Despite the recent introduction of the General Data Protection Regulations 2016/679 (GDPR) (supplemented in the UK by the Data Protection Act 2018) that mandates the reporting of cyber-attacks, it is believed that many instances remain undisclosed. This can be because organisations do not perceive it necessary to disclose such information, nor are they aware of the legal need to do so, and they are also reluctant to disclose such information since it may be reputationally damaging (Amir, Levi and Livne, 2018; Meisner, 2018). Information about attacks is also rarely used to improve systems against future attack (Alrimawi, Pasquale, Mehta and Nuseibeh, 2018) and this makes it difficult to quantify the precise cost of disruptions (Meisner, 2018).

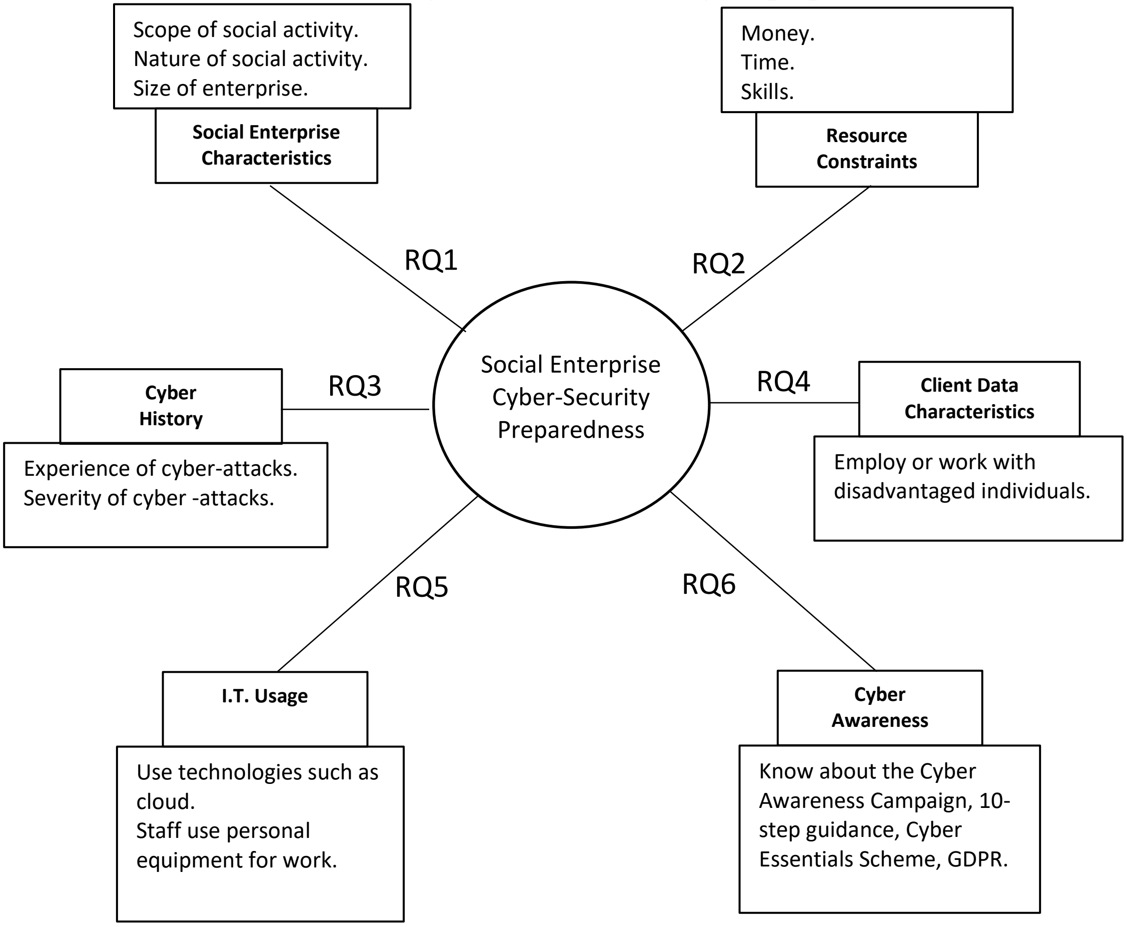
The acquisition of sensitive data via cyber-attack has increased and this has a deleterious effect upon large governmental institutions as well as smaller businesses (Dasgupta, Roy and Ghosh, 2018) and charities (Cook and Bernal, 2018; Charity Commission, 2019). For example, a ransomware attack upon a local council in the UK was estimated to cost between £11m and £18m to repair (Pidd and Robinson, 2020). Small businesses especially, are less likely to have adequate cyber defence capabilities than larger organisations (Berry and Berry, 2018) while 36% of charities are unaware of the types of cybercrime they may be subjected to (Charity Commission, 2019). The healthcare sector is at particular risk of cyber-attack due to the sensitivity of patient data (Meisner, 2018) and this data is also likely to be disclosed by the organisation's staff (Meng, Li, Wand and Au, 2018). The characteristics of individual system users, such as their propensity for risk-taking and gender, are also known to be a determinant in cyber security behaviours (Gratian, Bandi, Cukier, Dykstra and Ginther, 2018). Social engineering attacks, that target individual system users through approaches such as phishing, are not only difficult to protect against but are also exceedingly damaging (Thomas, 2018; Pathan, 2018).

The ability of an organisation to prevent or successfully manage cyber-attacks is dependent upon numerous factors, including resource constraints as well as the characteristics of individual system users. This study assesses SEs 'preparedness' to manage cyber security: 'Preparedness' is conceptualised as consisting of several indicators of the measures that organisations have in place for managing cyber security and cyber-attacks. These indicators are adopted from the CSBS (2018) survey of the cyber-attacks and preventive measures of commercial organisations and charities in the UK, augmented with insights that have been gained from the extant literature, and broadly comprise the adequacy of financial and human resources, possessing policies for cyber security and information technology usage, undertaking system tests, and keeping software and hardware up to date.

Based upon the extant literatures that examine cyber-crime and the characteristics of SEs, the following Research Questions (RQ1-6) are generated and are expressed as the conceptual framework for this study in Figure 1.

SEs are chosen as the focus of this research since they are an increasingly important part of the economy they have not previously been examined for their cyber-readiness (RQ1, RQ3 & RQ6), they are often constrained by their limited financial and expert resources (RQ2 & RQ5), they frequently possess sensitive personal information about their staff and clients (RQ4), they frequently employ low-skilled and volunteer staff (RQ1 & RQ4), many are contracted to deliver local and national government services (RQ4), and their rising success as socially and commercially important organisations may be increasing their visibility among cybercriminals (RQ1).

RQ1: The characteristics of the SE influence cyber preparedness.
RQ2: Resource constraints influence cyber preparedness.
RQ3: A history of cyber-attacks influence cyber preparedness.
RQ4: The characteristics of stored data influence cyber preparedness.
RQ5: The usage of IT equipment influence cyber preparedness.
RQ6: Awareness of cyber risks influence cyber preparedness.



Scope of social activity.
Nature of social activity.
Size of enterprise.
Social Enterprise Characteristics
Money.
Time.
Skills.
Resource Constraints
RQ1
RQ2
Social Enterprise Cyber-Security Preparedness
Cyber History
RQ3
Experience of cyber-attacks.
Severity of cyber -attacks.
RQ4
Client Data Characteristics
Employ or work with disadvantaged individuals.
RQ5
RQ6
I.T. Usage
Use technologies such as cloud.
Staff use personal equipment for work.
Cyber Awareness
Know about the Cyber Awareness Campaign, 10-step guidance, Cyber Essentials Scheme, GDPR.

Figure 1, SE Cyber-Preparedness Conceptual Framework

Methodology

This study employs an interpretive approach in order to understand the factors that influence the cyber-preparedness of SEs in the UK. A wide range of interpretive methods have been used to garner insight into cyber security issues (Fujs, Mihelic and Vrhovec, 2019) and their successful application substantiates the appropriateness of the chosen approach (for example Boroujeni, Tajfer and Parhizgar, 2019; Rivituso, 2014). Semi-structured interviews were utilised for their ability to gain rich insight into SE owner's understanding of cyber security and the challenges that they face in developing and implementing effective cyber security policies and practices (Denscombe, 2010; Fox, 2009; Johnson and Onwuegbuzie, 2004; Seidman, 1998). Maintaining confidentiality and anonymity underpins interpretive research (Duclos, 2017) and this was established by obtaining written consent from each participant (Li, 2008; Burgess, 2007).

Interviews of around one hour duration were conducted with twenty-one owner/managers of SEs by two of the research team. The participant SEs all operated within one of five Social Enterprise UK's 'Social Enterprise Places' (SEP), which are "hotspots of social enterprise activity" (SEUK, 2020). These comprised Alston Moor (a village), Digbeth (a quarter), Oxfordshire (a county), Plymouth (a city) and Wrexham (a town). Five SEs agreed to take part from Oxfordshire, and four from the remaining locations. The nature of the SEs is presented in Table 1: the precise location of each SE is not disclosed in order to ensure anonymity and to encourage candid exchange of views (Stewart, Gill, Chadwick and Treasure, 2008).

I.D.	Type	Company Details
1	Legal Advice	Sole trader, in business for 1 year.
2	Horticulture	Sole trader, in business for 3 years, employing on average 7 volunteer staff, operating in two neighbouring counties.

3	Café and SE Hub	4 permanent members of staff, in business for 3 years, employing over 20 volunteer staff, operating nationally.
4	Food	4 permanent members of staff, in business for 9 years, operating nationwide to hundreds of customers.
5	Music Therapy	Sole trader, in business for 3 years, operating nationwide to hundreds of beneficiaries.
6	Legal Advice	Sole trader, in business for 2 years.
7	Training and Education	Sole trader, in business for 5 years.
8	Mechanical Training	2 permanent members of staff, in business for 3 years, operating nationally.
9	Farm Project.	5 permanent members of staff, in business for 5 years, operating nationally.
10	Media Adviser	Sole trader, in business for 2 years, fifteen local clients.
11	Prisoner Workshop	Sole trader, in business for 6 years, volunteer workforce comprises current offenders and three other staff, serving the local community.
12	Clothes Shop	4 permanent members of staff, in business for 4 years, serving the local community.
13	Bike Repairs	11 permanent members of staff, in business for 6 years, employing 40 volunteer staff, serving the local county.
14	Cleaning Service	2 permanent members of staff, in business for 3 years, serving the local community
15	Advice for SE	3 permanent members of staff, in business for 4 years.
16	Training and Support	4 permanent members of staff, in business for 8 years, serving the local county.
1	Shared Mobility	6 permanent members of staff, in business for 9 years.
18	Food	3 permanent members of staff, in business for 4 years.
19	Sustainability Advice	Sole trader, startup enterprise.
20	Music	2 permanent members of staff, in business for 2 years.
21	Care Services	Sole trader.

Table 1, Participant Social Enterprises

All responses have been anonymised and participants are identified in the analyses using the convention P1, P2…P21 etc. The interview questions were open-ended and operationalized from the six Research Questions that were developed from the literature (Halcomb and Davidson, 2006; Charmaz, 2006). Questions typically took the form "*What do you understand by the term cyber security*" and further questions were developed during the interviews in order to explore salient and emergent themes. Other question were phrased to elicit deeper narratives around the participant's perceptions and experiences and utilised terms such as 'tell me', 'what do you think' and 'could you describe' (Charmaz, 2006; Strauss and Corbin, 1998). Spontaneous interview questions were crafted to explore emergent subjects and this allowed participants the opportunity to express themselves and to illustrate their points with meaningful examples and personal stories (Duffy, Ferguson and Watson, 2002). The interview questions were reviewed and refined after each interview to ensure that theoretical saturation was achieved (Samuel and Peattie, 2016; Guest, MacQueen and Namey, 2006; Glaser and Strauss, 1967).

The data were analysed using thematic analysis (Guest, et al, 2012) following Braun and Clarke's (2006) six-step process (detailed in Table 2): (1) data familiarization, (2) initial interpretation, (3) identification of themes, (4) reviewing and agreeing themes, (5) defining the dominant themes, and (6) construction of the narrative of the analysis. The process began (Step 1) with the interviewers transcribing their interviews verbatim in order to minimise misinterpretation (Opdenakker, 2006). Following this (Step 2), each interviewer thematically analysed and coded every transcript and then (Step 3) collated the codes into themes. The themes were then cross-compared by all four of the researchers in order to reach consensus (Step 4). All four of the researchers were again involved in the final analytical stage (Step 5) where the overarching, dominant themes were identified. Prior to constructing the written narrative of the analyses the thematic interpretation was member validated with two owner-managers of SEs that took part in the study (Sandelowski, 1993).

Determining the robustness of interpretive research has been the subject of considerable debate (Miles, 1979) and terms such as 'reliability' and 'validity' should be avoided (Johnson, Buehring, Cassell and Syman, 2006). Instead, the research process should incorporate a 'declared in advance' process (Gronhaug and Olson, 1999; Whittemore, Chase and Mandle, 2001) and triangulation (Gronhaug and Olson, 1999; Eden and Huxham, 1996; Jick, 1979). The triangulation of interpretive results may be achieved through the utilization of multiple research sites and multiple researchers. The similarity of the interpretations of the investigating team may then be determined through the calculation of 'inter-rater reliability' using measures such as Cohen’s Kappa (for two raters) or Fleiss’s Kappa (for multiple raters (Castano, Fontanil and Garcia-Izquierdo, 2019; Graversen, Pedersen, Carlsen, Bro, Huibers and Christensen, 2019; Hassan, Puteh and Sanusi, 2019; Schwartz, Albin and Gerberich, 2019). Kappa values are interpreted as 0 (no agreement) to 1 (complete agreement). There is some debate over what value constitutes ‘acceptable’ Kappa values. For instance, Landis and Koch (1977) declare that values above 0.6 are ‘substantial’ agreement, whereas Altman (1991) states that values above 0.6 are ‘good’, while Fleiss et al (2003) class values of 0.41-0.75 as ‘good’ and values above 0.75 as ‘very good’. In this study, Fleiss’s Kappa was used to measure the degree of agreement between the investigators at Steps 4 and 5 of the Braun and Clarke (2006) process: at Step 4 Fleiss’s Kappa was 0.65 and at Step 5 was 0.8. These measurements, plus the confirmatory member validation, substantiate the claim of ‘very good’ robustness of the study.

Initial Codes		**Themes**		**Consensus of Themes**	**Final Themes**	**Link to RQ**
Researcher 1	Researcher 2	Researcher 1	Researcher 2			
Threat	Threat	Vulnerability	Threat	Vulnerability	Vulnerability	RQ1/RQ4
Vulnerability	Risk					
	Likelihood of attack					
History of attack	Experience of attack	History	Experience	Experience	Experience	RQ3
Repeated attack						
Social media	Online data	Data	Data	Data (location and type)	Data	RQ5
	Protect volunteers					
Skills	Skills	Skills	Skills & Abilities	Skills	Skills	RQ2
Personal skills	In-house skills					
Volunteers	Abilities					
Overload	Capacity	Overload	Capacity	Overload	Overload	Emergent

Cost	Cost	Cost	Resources	Resources	Resources	RQ2
	Time					
	Fines					
HELP!	Awareness of Assistance	Knowledge	Awareness	Awareness	Cyber Awareness	RQ6

Table 2, Data Coding and Analysis

Findings & Discussion

This section presents the key findings of the study and is structured according to the order for the research questions (RQ1…RQ6). Discussions with the participants around RQ1 and RQ4 were found to be textually rich and thematically interwoven (as indicated in Table 2) and this prompted a revision to the conceptual framework that is finally presented in Figure 2. The modified framework also captures the emergent feature of 'Management Characteristics', discussed within the section on RQ6, that reflects the observations of the limited SE owner-managers' absorptive capacities.

Social Enterprise Characteristics (RQ1 & RQ4)

Many of the respondents in this study emphasised the vulnerabilities of their organisation and of the sector as a whole. While this may be expected to be the response of owner-managers of organisations in almost any sector, many of the owner-managers identified unique aspects of SEs that make them particularly susceptible to cyber attack:

> *I suppose that some of the grant money that we win could be attractive to some people.* P14

Some highlighted the specific challenges that the human resources present to those with malicious intent, and this is clearly linked with RQ4 that explores the nature of the data that is held by the organisation:

> *Some of our members have…how can I put it…a colourful past.* P11

> *That's another big thing about volunteers, you really have to protect these people as well and hold their information safely.* P3

The involvement of volunteers, both as recipients of services and as employees, presents a particular problem. Volunteer resources are often poorly skilled (Bullee, Montoya, Pieters, Junger and Hartelk, 2018; Rey-Marti et al., 2016; Richards and Reed, 2015; Doherty et al., 2014; Lui, Takeda and Ko, 2014) and lack experience of digitally-enabled workplaces, and this makes them particularly susceptible to social-engineering attacks as well as the improper care and use of data and equipment. Additionally, the problem of poor skills is exacerbated by the transient nature of volunteers thereby diluting the effect of any training that may be provided. The close involvement of SEs with often disadvantaged and vulnerable individuals makes them even more susceptible to social engineering attacks, which are inherently hard to protect against (Thomas, 2018; Pathan, 2018). Collectively, this evidences RQ1 by highlighting that owner-managers recognise that the uniqueness of SEs may make them vulnerable to cyber-attack, particularly those that are predicated upon a social-engineering approach.

Resource Constraints (RQ2)

All of the participants raised the issue of the lack of time or resources that impinges upon their ability to take affirmative action to improve their cyber-security, and this is widely recognised as a factor that affects all aspects of SE operation (White, Samuel, Pickernell, Taylor and Mason-Jones, 2018; Rey-Marti, Ribeiro-Soriano and Palacios-Marques, 2016; Katre and Salipante, 2012):

> *The problem is it's just another thing to consider.* P2

> *You haven't got all the resources to be able to look after that.* P3

As a consequence of this, most SEs relied upon the skills of their current staff to deal with cyber-security issues.

> *We have an IT guy…well, we don't employ him but he's a volunteer in our community and he comes in and sorts out our computers and things.* P12

> *I've let other people deal with that mire than myself.* P17

Several SEs have taken the step of hiring cyber security expertise and have:

> *…a consultant coming in and doing that.* P18

It is notable that the reliance upon 'casual' IT skills that may be possessed by human resources may, in itself, be inadequate to provide robust protection from potential cybersecurity threats (Ani, He and Tiwari, 2019). In many instances, the 'IT skills' that are possessed by individuals are limited to personal or 'domestic' experience of IT. The Charities Commission (2019) reports upon the use of trustees that have 'varied knowledge and experience' yet, due to their age profile are likely to have low levels of cyber awareness and therefore make the enterprises 'more vulnerable to cybercrime'. It may be ventured that the utilization of available and volunteer resources imbues SEs and their owner/managers with a false sense of reassurance that risks have been addressed properly. Furthermore, it is not inconceivable to imagine that a person that is tasked with undertaking IT duties for such an organization could become the subject of a cybersecurity attack (Gratian, Bandi, Cukier, Dykstra and Ginther, 2018).

The issue of financial cost was one that frequently arose within discussions and this is widely recognised as a problem for all SEs (Martin 2015; Lehner and Nicholls, 2014; Reiser and Dean, 2014). Consequently, few SEs are in a position to be able to afford expert support, with one owner/manager extolling:

> *Even the smallest of fines, that could tip us over the edge really.* P6

> *Access to money as opposed to support. You can be supported to death, but access to actual money would be great.* P15

One participant identified that the cost of improper cyber-preparedness could result in a fine that would undermine the organisation's financial security. This is a subject of perennial concern for SE scholars and practitioners alike (Martin 2015; Lehner and Nicholls, 2014; Reiser and Dean, 2014). It must therefore be concluded that cost is predominantly a limiting factor in cyber-security, however one can surmise that improved awareness of the financial consequences of poor cyber-security may influence owner-manager behaviours.

The views expressed by the participants substantially evidences RQ2, that resource constraints influence cyber-preparedness. However, it must be noted that this is a multifaceted relationship. In its simplest manifestation, the lack of resources precluded the implementation or development of cyber-security initiatives. For a few organisations however, the need to be cyber-secure prompted the diversion of financial resources in order to secure appropriately skilled IT resources.

Cyber History (RQ3)

Some of the participants recalled instances of cyber-attacks that they, or their organisations, had suffered. However, all of them were relatively minor, but still damaging (Thomas, 2018; Pathan, 2018), comprising phishing or scam emails:

> *I constantly get emails and calls from foreign numbers.* P3

> *My inbox is always full of spurious emails and requests.* P20

Many, including those that had experience of cyber-crime, downplayed or underestimated the risks involved:

> *Cyber security isn't a big concern for us.* P9

> *To be honest, we're not overly worried about it.* P12

This is somewhat surprising given that the owner-managers recognised that their organisations were vulnerable to cyber-attacks. There was no indication within the data that prior experience of cyber-attacks would influence their cyber-preparedness to evidence RQ3 and this contrasts with the majority situation in charitable organizations whereby 69% implemented system revisions following cyber attack (Charity Commission, 2019). This may be due to the young age of the organizations and there being little organizational history to draw upon: almost half of SEs in the UK are less than five years old (SEUK, 2019). It is also possible that those organisations that had experienced minor attacks were those that already had adequate protection in place or that the severity of the attacks were not sufficient to stimulate cyber-security initiatives: for instance, P3 and P20's responses (quoted above) indicated that they were basing their perceptions upon their experience of having their personal email and telephone scammed.

Client Data Characteristics (RQ4 & RQ1)

While many of the owner-managers recognised the sensitive nature of the data that they held (illustrated by the statements of P5, P14 and P19 in RQ1) in accord with the literature (Doherty, Haugh and Lyon, 2014; Samuel, White, Jones and Fisher, 2018), this alone did not seem sufficient to instigate cyber-security initiatives. Many of them pointed toward the lack of commercially valuable data that they possessed:

> *The other reason why it's not really a threat for us is because we don't have a lot of personal data worth stealing.* P17
>
> *We're not a large charity…we don't have people's bank details.* P10

This is important for it indicates that SE owners/managers are aware that some types of data are more valuable than others and thereby may increase the likelihood of them being viable targets for cyber-attacks. However, many did not perceive the sensitive nature of data that they may hold either directly or indirectly about their vulnerable, volunteer resources that have ‘colourful pasts’, or about government agencies to which they may provide vicarious access (Dasgupta, Roy and Ghosh, 2018). It was expected that the SE owner-managers would be aware of the potentially sensitive data that their organizations possess (Doherty, Haugh and Lyon, 2014; Samuel, White, Jones and Fisher, 2018). and thereby directly evidence RQ4. However, the observation that many did not recognise this important facet of their organizations serves to stress the significance of the finding. As was discussed in RQ2, many owner-managers have limited commercial experience and their perceptions of cyber risks are dominated by ‘domestic’ examples such as scam emails and phishing, even though these may still be costly to deal with (Thomas, 2018; Pathan, 2018). This ‘blinkered’ perspective appears to be hindering their recognition of the real risks surrounding the data that their organizations possess, thereby exacerbating the false sense of security that they may have and, along with resource constraints, inhibit their desire and ability to take appropriate action.

IT Usage (RQ5)

The nature of the data that the organisation possesses (RQ4) could be expected to have some relationship to the usage of IT equipment (RQ5). It was expected, or indeed hoped, that SEs would employ IT systems, practices and technologies that would be in accord with the types of data that they possessed. However, as also indicated in the evidence for RQ4, there was scant reference to the types and usage of IT equipment. A few SE owner-managers referred to the use of social media platforms and noted the care that was taken in ensuring that sensitive or personal information was not posted:

> *We use Facebook a lot, if it’s public stuff, pictures and so on, people can get hold of all that, I would never put any information about their lives or addresses on there.* P5

Social media applications are notorious for providing relatively easy access to private and personal data for malicious intent (Alguliyev, Aliguliyev and Abdullayeva, 2019; Singh and Kaur, 2019; Soomro and Hussain, 2019). SE owner-managers need to be aware of these issues and give them due consideration, alongside those of cost and ease-of-use, when determining to utilise social media as part of their business proposition or marketing. However, scholarly examination of the vagaries of social media adoption in SEs is nascent but limited (El-Den, Adhikari and Azam, 2017) and has so far ignored the issue of cybercrime and security.

None of the SE owner-managers highlighted unusual usage of IT in their operations: the majority used standard 'office' software and some used simple backup systems. Consequently, there was little data that evidenced RQ5. This finding may however be constrained by the type of SEs that were involved in the study and the nature of the work that they undertake.

Cyber Awareness (RQ6)

The interpretation of the data in RQ4 suggested that SE owner-managers underplayed the risks presented by cyber-attacks, or thought that they were not at risk because they did not hold any commercially valuable data. However, further investigation revealed that this was not necessarily the case and some SE owner-managers in fact merely considered cyber-security issues as 'just another thing to manage':

> *Cyber security threats – I wouldn't take it particularly any more seriously than I take any other threats.* P10

Although unexpected, this is not entirely surprising since SEs are frequently headed by socially and ideologically-driven individuals that are focussed upon the social mission of the organisation (White et al, 2018). While the commercial dimension of the organisations is important, it is seen as a necessity in order to achieve the social mission, and not as an end in itself. Consequently, these owner-managers have a rather different mindset to managers of predominantly commercial organisations. One may venture that they view all aspects of their business equally and thereby cyber-preparedness does not feature prominently within their discussions as it may with other types of owners or managers.

Other SE owners/managers were cognisant of the consequences of cyber-crime upon their organisation and the need to take action:

> *A data breach would not only harm our reputation but also get us into trouble with the Information Commission.* P6

> *I've actually thought to myself that I need to get a more secure email.* P8

Worryingly, while they aware of the importance of cyber-security and the need to address the issue, many have yet to act:

> *It's on my to do list.* P21

Most SE owners/managers ascribed this to their lack of understanding of key issues. For example:

> *When this whole GDPR thing happened…I don't really know if that's anything to do with cyber security.* P5

> *I went to these GDPR meetings and you get scared to death about this sort of thing.* P8

Many owners/managers commented upon their own personal skills and abilities being inadequate:

> *Fledgling social entrepreneurs – if it's never been your field why would you even know about it.* P21

> *The cyber threat…yeah, we'd have to bring somebody in because I haven't got a clue.* P8

Only one SE owner-manager was aware of the Information Commission, and none volunteered any knowledge of the various schemes that existed to support organisations in developing and implementing cyber-security measures. Even when prompted through targeted questions only a few stated that they had heard of the schemes and none had any knowledge of their purpose or content or availability. Furthermore, none of the respondents knew that formal cyber risk assessment tools existed (see for example: Kure, Islam and Razzaque, 2018; Bartolini, Ahrens and Zascerinska, 2018; Ali, Almogren, Hassan, Rassan and Bhuiyan, 2018). This is an important finding that evidences RQ6 and has significance for those organisations that are responsible for promoting cyber-awareness and preparedness, and also for those organisations that represent SEs and communicate contemporary issues with their members.

Allied to this observation is the theme of 'Overload' that is presented in Table 1 as an emergent issue. 'Overload' refers to the frequent mention that was made of the owner-manager's capacity to handle 'everything at once'. This is related to the preceding discussion of RQ6 and the nature of the owner-managers themselves and to the discussion of RQ2 (resources): in giving equal attention to all issues within the organisation, it may be impossible for SE owner-managers to dedicate themselves to all issues at once, and may also be difficult for them to devolve responsibility for some issues to others, particularly in the presence of limited skills and resources. The issue may be one of what Szulanski (1996, p31) terms the 'absorptive capacity' of the individual, that is, their ability to assimilate new information, or one of 'retentive capacity', that is, their ability to institutionalise new information as new ways of working.

Summary of Analyses & Discussion

The analyses support the assertion that the cyber-preparedness of SEs is in need of dedicated examination and concur with O'Rourke's (2018) observation that many organisations are poorly prepared to manage their cyber-security, particularly smaller organisation such as SEs (Berry and Berry, 2018). While the CSBS (2018) found that around one third of UK organisations had cyber-security systems in place, 44% of charities were not adequately protected despite 50% of them being the subjects of cybercrime within the past year (Charity Digital, 2019). This study suggests that the figure for effective cyber-security systems in SEs in the UK may be far lower. Even though the sector as a whole is in need of further examination for cyber-security activities, capabilities and preparedness, one of the challenges that this sector presents is its inordinate degree of heterogeneity (Samuel et al, 2018; White et al, 2018). Consequently, it is difficult to draw generalizable results for the sector because a 'representative' sample is elusive.

The management and governance structure of SEs is known to be important and problematic (Doherty et al., 2014; Lehner and Nicholls, 2014; Reiser and Dean, 2014) and this study suggests that the magnitude and multitude of management issues is further problematized through the addition of the issues that surround cyber-security. The literature highlights that managerial issues may lead to SEs being unable to achieve their social goals (Cornforth, 2014; Santos et al., 2015; Young and Kim, 2015; Ebrahim et al., 2014) while this study also suggests that a lack of attention to cyber-security issues may result in them being unable to meet their legal and ethical goals. Recognizing the challenges that best individual owner-managers of SEs, and the broader managerial challenges that are identified in the extant literature, Figure 2 proffers a modified conceptual framework of the factors that influence cyber-preparedness in SEs. The pertinent features of each of the antecedents of cyber-security that were highlighted through the research are presented in the descriptions. Notably, RQ1 and RQ4 have been combined within the single factor of 'Social Enterprise Characteristics' in recognition that discussions of data types and characteristics of the organizations were frequently and inextricably intertwined. RQ3 has been modified to read ‘Cyber Experience’ to reflect that the majority of owner-managers focused upon their own personal experiences rather than the historical experience of cyber attacks within the organization.

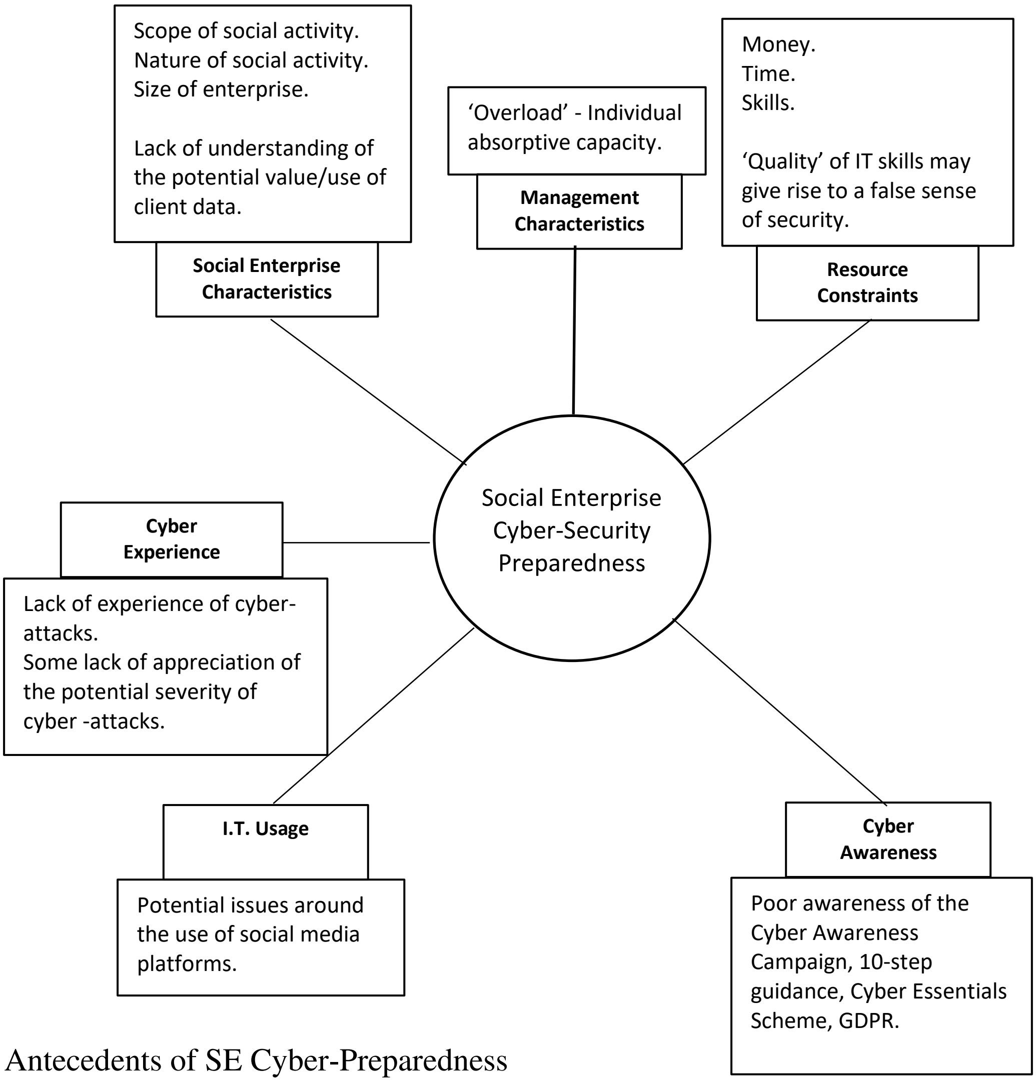

Scope of social activity.
Nature of social activity.
Size of enterprise.
Lack of understanding of the potential value/use of client data.
Social Enterprise Characteristics
‘Overload’ - Individual absorptive capacity.
Management Characteristics
Money.
Time.
Skills.
‘Quality’ of IT skills may give rise to a false sense of security.
Resource Constraints
Cyber Experience
Lack of experience of cyber-attacks.
Some lack of appreciation of the potential severity of cyber -attacks.
Social Enterprise Cyber-Security Preparedness
I.T. Usage
Potential issues around the use of social media platforms.
Cyber Awareness
Poor awareness of the Cyber Awareness Campaign, 10-step guidance, Cyber Essentials Scheme, GDPR.

Figure 2, Antecedents of SE Cyber-Preparedness

Conclusions

Cyber-security has become a subject of great interest in the academic literature and even greater importance for practicing managers worldwide. The science of cyber-security has matured rapidly whereas the practice of managing cyber-security can be perceived to have lagged considerably, particularly in smaller organizations (Berry and Berry, 2018). While some large-scale studies have been made of the cyber-security systems and practices in different types of organisations, none have as yet examined the social enterprise sector. This is problematic since SEs are a rapidly growing sector of the economy and an increasingly important facet of modern society in light of the widespread retraction of state-funded social support systems.

This study aimed to understand the factors that influence the cyber-preparedness of social enterprises. A series of in-depth examinations were undertaken of the cyber awareness, practices and readiness of SE owner-managers in the UK structured around a conceptual model that was developed from the extant cyber-security and SE literatures. The study finds that very few SEs are aware of the initiatives that are designed to support the development and implementation of cyber-security systems and this mirrors findings in other organisation types (O'Rourke, 2018; Amir, Levi and Livne, 2018; Meisner, 2018). This is problematic since owner-managers recognise that SEs are constrained by a lack of skills and finance, and discontinuous staffing that precludes effective cyber training. The use of suboptimal IT resources, that are frequently provide by volunteers, may also lead to a false-sense of security and inhibit adequate cyber-preparedness. Government agencies are known to be likely targets of cybercrime (Dasgupta, Roy and Ghosh, 2018) and security vulnerabilities in SEs may afford a 'gateway' for their perpetration. In addition, the widespread utilization of social media platforms, whilst attractive for their ease-of-use and apparent cost-effectiveness, opens up SEs to a growing wave of cybercrime that is conducted through this media. Consequently, the SE sector appears to be under-prepared to manage cyber-security issues despite appearing to be vulnerable to such an attack. Further efforts are needed to improve the awareness of cyber-security assistance schemes.

The study also indicates the importance of the absorptive capacity of SE owner-managers and thereby extends our understanding of the characteristic of individual system users that can affect the cyber security of an organization (Gratian, Bandi, Cukier, Dykstra and Ginther, 2018). This research therefore proffers a contribution to knowledge by theorising the factors that induce the adoption and implementation of cyber-security measures in SEs, comprising the characteristics of the enterprise, the characteristics of the enterprise management, resource constraints, experience of cyber attacks, usage of IT, and awareness of cybersecurity schemes and resources. This is the first study to examine these factors in the context of Social Enterprise, presented in a conceptual model, and thereby provides a valuable 'first exploration' into the steps that need to be taken in order to make these organisations 'cyber secure'.

Limitations

This study is somewhat limited by its geographic focus upon SEs in the UK, and by virtue of its interpretivist approach. Efforts to establish the robustness of the study have been made through the calculation of inter-rater reliability and subsequent member validation. However, the heterogeneity of the sector insists that generalizations of the findings must be made with caution. The study attempted to improve its generalizability through the construction and distribution of a survey instrument to facilitate a quantitative examination of the relationship between the elements of the conceptual framework. The survey was duly created and distributed, with the assistance of Social Enterprise UK (SEUK) to all SEs that subscribe to their mailing list via their monthly newsletter and via their Twitter feed (circa 5000 SEs in the UK). Despite numerous reminder messages the survey did not return sufficient responses to enable a statistically rigorous analysis to be made. This study therefore affords a methodological warning to future studies that aim to elicit the participation of SEs: whether it is due to a lack of time to devote to requests for participation in surveys, or a lack of awareness of the importance of cyber-security issues, or is yet another burden upon owner-managers' absorptive capacity, the engagement of SEs in future studies requires careful consideration of the methods by which participation may be encouraged and improved.

Future Research

Notwithstanding the methodological hurdle of engaging the participation of organizations that are severely resource constrained, future research should aim to provide quantitative examination of the factors that influence SE cyber-preparedness. The conceptual framework proffered in this study may form the basis of a large-scale survey of SEs. The use of survey technique may also be a means of confirming and refining the findings of this study in SEs outside the UK. Furthermore, useful insight could be gained through case study examination of SEs that have experienced and managed cyber-attacks, or have robust cyber-security systems and practices from which other organisations could learn. Identifying these cases and attracting willing participants may be challenging, but the reports of the Information Commission may be useful starting points. It is also imperative that the lack of SE awareness of the various cyber initiatives that exist in the UK is examined more closely to improve the cyber-preparedness of this valuable and growing sector. Organizations that represent SEs, as well as national and local governing bodies, need to review the ways in which they may individually and collectively address this need.

References

K. K. Adu, "The Phenomenon of Data Loss and Cyber Security Issues in Ghana", *Foresight*, vol. 20, no. 2, pp. 150-161, 2018.

A. Afolayan, E. Plant, G. R. T. White, W. P. Jones and P. Beynon-Davies, “Information Technology Usage in SMEs in a Developing Economy”, *Strategic Change: briefings in entrepreneurial finance*, vol. 24, no. 5, pp. 483-498, 2015.

M. Alali, A. Almogren, M. M. Hassan, L. A. L. Rassan and M Z. A. Bhuiyan, “Improving Risk Assessment Model of Cyber Security Using Fuzzy Logic Inference System”, *Computers & Security*, vol. 74, pp. 323-339, 2018.

R. M. Alguliyev, R. M. Aliguliyev and F. J. Abdullayyeva, “Deep Learning Method for Prediction of DDos Attacks on Social Media”, *Advances in Data Science and Adaptive Analysis*, vol. 11, no. 1 & 2, pp. 1-19, 2019.

F. Alrimawi, L. Pasquale, D. Mehta and B. Nusiebeh, “I’ve Seen This Before: Sharing Cyber-Physical Incident Knowledge”, In *Proceedings of IEEE/ACM 1st International Workshop on Security Awareness from Design to Deployment, Gothenburg, Sweden, May, 2018 (SEAD ‘18)*, pp. 1-8, 2018.

E. Amir, S. Levi and T. Livne, “Do Firms Underreport Information on Cyber-Attacks? Evidence from capital markets”, *Review of Accounting Studies*, pp. 1-30, 2018.

U. D. Ani, H. He and A. Tiwari, “Human Factor Security: evaluating the cybersecurity capacity of the industrial workforce”, *Journal of Systems and Information Technology*, vol. 21, no. 1, pp. 2-35, 2019.

D. N. Bartorini, A. Ahrens and J. Zascerinska, “Instrument Design for Cyber Risk Assessment in Insurability Verification”, *8th International Interdisciplinary PhD Workshop/ I2PhDW 2018*, Swinoujscie, Poland, 2018.

C. T. Berry and R. L. Berry, “An Initial Assessment of Small Business Risk Management Approaches for Cyber Security Threats”, *International Journal of Business Continuity and Risk Management*, vol. 8, no. 1, pp. 1-10, 2018.

S. A. T. Boroujeni, A. H. Tajfar and M. M. Parhizgar, “Prioritizing Obstacles to Industrial Control Systems Security Management Implementation, Using Interpretive Structural Modelling (ISM) Approach”, *Journal of Electronic and Cyber Defence*, vol. 7, no. 2, pp. 109-119, 2019.

A. M. Bossler and T. Berenblum, “Introduction: new directions in cybercrime research”, *Journal of Crime and Justice*, vol. 42, no. 5, pp. 495-499, 2019.

V. Braun and V. Clarke, “Using thematic analysis in psychology”, *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77-101, 2006.

J. Bullee, L. Montoya, W. Pieters, M. Junger and P. Hartel, “On the Anatomy of Social Engineering Attacks – a literature-based dissection of successful attacks”, *Journal of Investigative Psychology and Offender Profiling,* vol. 15, no. 1, pp. 20-45, 2018.

M. M. Burgess, “Proposing modesty for informed consent”, *Social Science & Medicine*, vol. 65, no. 11, pp. 2284–2295, 2007.

Café from Crisis, “Old Fire Station Café”, Available from: https://oldfirestation.org.uk/shop-cafe/cafe/ (Accessed 25th February 2020).

Charity Commission, “Preventing Charity Cybercrime”, Available from: https://www.gov.uk/government/publications/preventing-charity-cyber-crime-insights-and-action (Accessed 25th February 2020).

A. M. Castano, Y. Fontanil and A. L. Garcia-Izquierdo, “Why Can’t I Become a Manager? – a systematic review of gender stereotypes and organizational discrimination”, *International Journal of Environmental Research and Public Health*, vol. 16, no. 10, pp. 1813, 2019.

D. Chaffey and G. R. T. White, *Business Information Management*, Pearson Education: UK, 2011.

Charity Commission, “Preventing Charity Cybercrime: Insights + Action”, Charity Commission for England and Wales, 2019.

Charity Digital, “Charities Affected by Cyber Crime in 2019”, Available from: https://charitydigital.org.uk/topics/charities-affected-by-cyber-crime-in-2019-6526 (Accessed 27th February 2020).

K. Charmaz, *Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis,* London: SAGE Publications, 2006.

K. R. Choo, K. Gai, L. Chiaraviglio and Q. Yang, “Special Issue on A Multidisciplinary Approach to Internet of Things Cybersecurity and Risk Management”, *Computers & Security*, 2020.

J. Cook and N. Bernal, “Russian Hackers Targeted Cancer Research UK and other British Businesses”. Available from: https://www.telegraph.co.uk/technology/2018/10/07/british-airways-hackers-targeted-cancer-research-uk-british/ (Accessed 7th October 2018).

C. Cornforth, “Understanding and combating mission drift in social enterprises”, *Social Enterprise Journal*, vol. 10, no. 1, pp. 3-20, 2014.

CSBS “Cyber Security Breaches Survey”. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf Accessed 10/07/2018

D. Dasgupta, A. Roy and D. Ghosh, “Multi-user Permission Strategy to Access Sensitive Information”, *Information Sciences*, vol. 423, pp. 24-49, 2018.

J. G. Dees, “A tale of two cultures: Charity, problem solving, and the future of social entrepreneurship”, *Journal of Business Ethics*, vol. 111, no. 3, pp. 321–334, 2012.

R. Deibert, "Towards a Cyber Security Strategy for Global Civil Society*?" Global Information Society Watch*, pp. 23-26, 2011.

M. Denscombe, *The good research guide: For small-scale social research projects* (4th edn), Berkshire, UK: McGraw-Hill Education, 2010.

B. Doherty, H. Haugh and F. Lyon, "Social enterprises as hybrid organisations: a review and research agenda", *International Journal of Management Reviews,* vol. 16, no. 4, pp. 417-436, 2014.

D. Duclos, "When ethnography dose not rhyme with anonymity: Reflections on name disclosure, self-censorship and storytelling", *Ethnography*, vol. 20, no. 2., pp. 175-183, 2017.

A. Duffy, C. Ferguson and H. Watson, "Data Collecting in Grounded-Theory – some practical issues", *Nursing Research*, vol. 11, no. 4, pp. 67-78, 2004.

A. Ebrahim, J. Battailana and J. Mair, "The Governance of social enterprises: Mission drift and accountability challenges in hybrid organizations", *Research in Organizational Behavior*, vol. 34, pp. 81-100, 2014.

C. Eden and C. Huxham "Action Research for Management Research", *British Journal of Management*, vol. 7, pp. 75-86, 1996.

J. El-Den, P. Adhikari and S. Azam, "A Model for Social Media Adoption in Social Enterprises: a comparative analysis with existing adoption model", *Journal of Advanced Management Science*, vol. 5, no. 6, pp. 467-473, 2017.

J. Fleiss, B. Levin and M. Paik, *Statistical Methods for Rates & Proportions*, 3rd Ed. Wiley & Sons, New York, 2003.

N. Fox, "Using interview in a research project", Yorkshire, UK: The NIHR Research Design Service.

D. Fujs, A. Mihelic and S. L. R. Vrhovec, “The Power of Interpretation: qualitative methods in cybersecurity research”, *Proceeding of the 14th International Conference on Availability, Reliability and Security*, pp. 1-10, 2019.

B. G. Glaser and A. L. Strauss, *The Discovery of Grounded Theory: Strategies for Qualitative Research*, New York, NY: Aldine Publishing Company, 1967.

M. Gratian, S. Bandi, M. Cukier, J. Dykstra and A. Ginther, “Correlating Human Traits and Cyber Security Behaviour Intentions”. *Computers & Security*, vol. 73, pp. 345-358, 2018.

D. S. Graversen, A. F. Pedersen, A. H. Carlsen, F. Bro, L..Huibers and M. B. Christensen, “Quality of Out-of-Hours Telephone Triage by General Practitioners and Nurses: development and testing of the AQTT – an assessment tool measuring communication, patient safety and efficiency”, *Scandinavian Journal of Primary Health Care*, vol. 37, no. 1, pp. 18-29, 2019.

V. A. Greenfield and L. Paoli, “A Framework to Assess the Harms of Crimes”, *The British Journal of Criminology*, vol. 53, no. 5, pp. 864-885, 2013.

K. Gronhaug and O. Olson, “Action Research and Knowledge Creation: merits and challenges”, *Qualitative Market Research*, vol. 2, no. 1, pp. 6-14, 1999.

G. Guest, K. MacQueen and E. Namey, *Applied thematic analysis*, Thousand Oaks, CA: Sage Publications, 2012.

E. J. Halcomb and P. M. Davidson, “Is verbatim transcription of interview data always necessary?” *Applied Nursing Research*, vol. 19, pp. 38-42, 2006.

N. F. B. Hassan, S. B. Puteh and A. B. M. Sanusi, “Fleiss’s Kappa: assessing the concept of technology enabled active learning (TEAL)”, *Journal of Technical Education and Training*, 2019.

B. Huybrechts, and A. Nicholls, "The role of legitimacy in social enterprise-corporate collaboration", *Social Enterprise Journal,* vol. 9, no. 2, pp. 130-146, 2013.

T. D. Jick, "Mixing qualitative and quantitative methods: Triangulation in action", *Administrative Science Quarterly*, vol. 24, no. 4, pp. 602–611, 1979.

P. Johnson, A. Buehring, C. Cassell and G. Symon, "Evaluating qualitative management research: Towards a contingent criteriology", *International Journal of Management Reviews*, vol. 8, no. 3, pp. 131-156, 2006.

R. B. Johnson and A. J. Onwuegbuzie, "Mixed Methods Research: A Research Paradigm Whose Time Has Come", *Educational Researcher,* vol. 33, no. 7, pp. 14-26, 2004.

A. Katre and P. Salipante "Start-up social ventures: Blending fine-grained behaviors from two institutions for entrepreneurial success", *Entrepreneurship Theory and Practice,* vol. 36, pp. 967–994, 2012.

H. I. Kure, S. Islam and M. A. Razzaque, "An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System", *Applied Sciences*, vol. 8, pp. 1-29, 2018.

J. Landis and G. Koch, "Measurement of Observer Agreement for Categorical Data". *Biometrics*, vol. 22, pp. 159-174, 1977.

O. M. Lehner and A. Nicholls, "Social finance and crowd funding for social enterprise: a public private case study providing legitimacy and leverage", *Venture Capital: An International Journal of Entrepreneurial Finance,* vol. 16, no. 3, pp. 271-286, 2014.

J. Li, "Ethical challenges in participant observation: A reflection on ethnographic fieldwork", *Qualitative Report*, vol. 1, no. 1), pp. 100–115, 2008.

G. Liu, S. Takeda and W. Ko, "Strategic orientation and social enterprise performance", *Nonprofit and Voluntary Sector Quarterly*, vol. 43, no. 3, pp. 480–501, 2014.

C. D. Marcum, G. E. Higgins, T. L. Freiburger and M. L. Ricketts, "Policing Possession of Child Pornography Online: investigating the training and resources dedicated to the investigation of cyber crime*", International Journal of Police Science and Management*, vol. 12, no. 4, pp. 516-525, 2010.

M. Martin, "Building impact business through hybrid financing", *Entrepreneurship Research Journal*, vol. 5 no. 2, pp. 109-126, 2015.

C. Mason and B. Doherty, "A fair trade-off? Paradoxes in the governance of fair-trade social enterprises", *Journal of Business Ethics*, vol. 136, no. 3, pp.451-469, 2016.

M. Meisner, "Financial Consequences of Cyber Attacks Leading to Data Breaches in Healthcare Sector", *Copernican Journal of Finance & Accounting*, vol. 6, no. 3, pp. 63-73, 2018.

W. Meng, W. Li, Y. Wang and M. H. Au, "Detecting Insider Attacks in Medical Cyber-Physical Networks Based on Behavioral Profiling", *Future Generation Computer Systems*, vol. 108, pp. 1258-1266, 2018.

M. B. Miles, "Qualitative Data as an Attractive Nuisance: The Problem of Analysis", *Administrative Science Quarterly*, vol. 24, no. 4, pp. 590-601, 1979.

F. Ngo and K. Jaishankar, "Commemorating a Decade in Existence of the International Journal of Cyber Criminology: a research agenda to advance the scholarship on cyber crime", *International Journal of Cyber Criminology*, vol. 11, no. 1, pp. 1-9, 2017.

R. Opdenakker, "Advantages and disadvantages of four interview techniques in qualitative research", *Open Journal System*, vol. 7, no. 4. Available from http://www.cpc.unc (Accessed 1st July 2019).

M. O'Rourke, "Assessing Cyber Readiness", *Risk Management*, vol. 65, no. 3, pp. 52, 2018.

L. Paoli, J. Visschers and C. Verstraete, “The Impact of Cybercrime on Businesses: a novel conceptual framework and its application to Belgium”, *Crime, Law and Social Change*, vol. 70, pp. 397-420, 2018.

A. K. Pathan, “Defending Against Common Cyber Attacks: phishing and cross-site scripting”. *2018 International Symposium on Programming and Systems*, Algiers, 2018.

K. Peattie and A Morley, “Eight paradoxes of the social enterprise research agenda”, *Social Enterprise Journal*, vol. 4, no. 2, pp. 91-107, 2008.

H. Pidd and G. Robinson, “Ransomware Attack Leaves Council Facing Huge Bill to Restore Services”, Available from: https://www.theguardian.com/technology/2020/feb/27/redcar-and-cleveland-council-hit-by-cyber-attack (Accessed 28th February 2020).

RAND *Estimating the Global Cost of Cyber Risk: methodology and examples.* RAND Corporation, Santa Monica, California, 2018.

D. B. Reiser and S. A. Dean, “Creative financing for social enterprise”, *Stanford Social Innovation Review,* pp. 50-54, 2014.

A. Rey-Marti, D. Ribeiro-Soriano and J. L.Sanchez-Garcia, ”Giving back to society: Job creation through social entrepreneurship”, *Journal of Business Research,* vol. 69, pp. 2067–2072, 2016.

A. Richards and J. Reed, “Social capital’s role in the development of volunteer led cooperatives”, *Social Enterprise Journal*, vol. 11, no. 1, pp. 4-23, 2015.

J. Rivituso, “Cyberbullying Victimization Among College Students: an interpretive phenomenological analysis”, *Journal of Information Systems Education*, vol. 25, no. 1, pp. 71-75, 2014.

A. Samuel, G. R. T. White, P. Jones and R. Fisher, “Social Enterprises Operating in the South Wales Valleys: a Delphi study of persistent tensions”. *Social Enterprise Journal*, vol. 14, no. 1, pp. 1750-8614, 2018.

A. Samuel and K. Peattie, “Grounded theory as a macromarketing methodology: critical insights from researching the marketing dynamics of Fairtrade Towns”. *Journal of Macromarketing* vol. 36, no. 1, pp. 11-26, 2016.

M. Sandelowski, “Rigor or rigor mortis: the problem of rigor in qualitative research revisited”, *Advances in Nursing Science*, vol. 16, no. 2, pp. 1-81, 1993.

F. Santos, A. C. Pache and C. Birkholz, “Making hybrids work: aligning business models and organisational design for social enterprise”, *California Management Review*, vol. 57, no. 3, pp. 36-58, 2015.

A. H. Schwartz, T. J. Albin and S. G. Gerberich, “Intra-rater and Inter-rater Reliability of the Rapid Entire Body Assessment (REBA) Tool”, *International Journal of Industrial Ergonomics*, vol. 71, pp. 111-116, 2019.

I. Seidman, *Interviewing as Qualitative Research: A Guide for Researchers in Education and the Social Sciences.* Teachers College Press, 1998.

SEUK, “Capitalism in Crisis? Transforming our Economy for People and Planet”. State of Social Enterprise Survey, 2019.

SEUK, “About Places”, Available from: https://www.socialenterprise.org.uk/social-enterprise-places/about-places/. (Accessed 23rd April 2020).

M. H. Shah, P. Jones and J. Choudrie, “Cybercrimes Prevention: promising organisational practices”, *Information Technology & People*, vol. 32, no. 5, pp. 1125-1129, 2019.

A. Singh and M. Kaur, “Intelligent Content-Based Cybercrime Detection in Online Social Networks Using Cuckoo Search Metaheuristic Approach”, *The Journal of Supercomputing*, 2019.

W. K. Smith, M. Gonin and M. L. Besharov, “Managing social-business tensions: A review and research agenda for social enterprise”, *Business Ethics Quarterly*, vol. 23, no. 3, pp. 407-442, 2013.

T. R. Soomor and M. Huusain, “Social Media-Related Cybercrimes and Tecniques for their Prevention”, *Applied Computer Systems*, vol. 24, no. 1, pp. 9-17, 2019.

K. Stewart, P. Gill, B. Chadwick and E. Treasure, “Qualitative research in dentistry”, *British Dental Journal*, vol. 204, no. 5, pp. 235–9, 2008.

D. W. Straub, S. Goodman and R. L. Baskerville, “Information Security: policy, processes and practices”, *Advances in Management Information Systems*, Armonk: England, 2008.

A. Strauss and J. Corbin, *Basics of Qualitative Research*. Thousand Oaks, CA: Sage Publications Inc., 1998.

G. Stephens, “Policing the Future: Law enforcement’s new challenges”, *The Futurist*, pp. 51-57, 2005.

G. Szulanski, “Exploring Internal Stickiness: Impediments to the Transfer of Best Practice Within the Firm”, *Strategic Management Journal*, vol. 17, pp. 27-43, 1996.

Telegraph, “WannaCry Cyber Attack Cost the NHS £92m as 19,000 Appointments Cancelled”, Available from: https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/. (Accessed 25th February 2020).

J. E. Thomas, “Individual Cyber Security: empowering employees to resist spear phishing to prevent identity theft and ransomware attacks”, *International Journal of Business Management*, vol. 12, no. 3, pp. 1-23, 2018.

F. Villeneuve-Smith and N. Temple, *State of Social Enterprise Survey, Leading the World in Social Enterprise’*. Social Enterprise UK. Available: Socialenterprise.org.uk, accessed 2nd March 2017.

Y. Wang and X. Shi, “E-business assimilation in SMEs of China”, *International Journal of Electronic Business,* vol. 7, no. 5, pp. 512-535, 2009.

G. R. T. White, “Future Applications of Blockchain in Business and Management: a Delphi study”. *Strategic Change: briefings in entrepreneurial finance*, vol. 26, no. 5, pp. 439-451, 2017.

G. R. T. White, A. Samuel, D. Pickernell, D. Taylor and R. Mason-Jones, “Social Entrepreneurs in Challenging Places: a Delphi study of experiences and perspectives”, *Local Economy*, pp. 1-24, 2018.

R. Whittemore, S. K. Chase and C. L.Mandle, “Validity in Qualitative Research”, *Qualitative Health Research*, vol. 111, pp. 522-537, 2001.

M. Xu, K. M. Schwetizer, R. M. Bateman and S. Xu, “Modeling and Predicting Cyber Hacking Breaches”, *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2856-2871, 2018.

D. R. Young and C. Kim, “Can social enterprise remain sustainable and mission focused? Applying resilience theory”, *Social Enterprise Journal*, vol. 11, no. 3, pp. 233-259, 2015.

S. Zainon, S. A. Ahmad, R. Atan, Y. B. Wah, Z. A. Bakar and S. R. Sarman, “Legitimacy and Sustainability of Social Enterprise: Governance and Accountability”, *Procedia - Social and Behavioral Sciences*, vol. 145, pp. 152-157, 2014.