A Research Report on Cyber Resilience and the Scottish Third Sector: Risks, Challenges and Opportunities

September 2023

Scottish Government
Riaghaltas na h-Alba

A Research Report on Cyber Resilience and the Scottish Third Sector: Risks, Challenges and Opportunities

December 2022

Author:
Dr Robert S. Dewar
Director and Founder
Dewar Cyber Consulting Ltd.

E: robert@dewarcyberconsulting.com
T. 0131 210 0178
www.dewarcyberconsulting.com

Contents

1. Executive Summary

In 2021 the Scottish Government published its revised Strategic Framework for A Cyber Resilient Scotland. Instead of addressing cyber security separately by sector, the Scottish Government sought to create a unified approach to cyber resilience and promote the understanding that cyber resilience requires holistic solutions, not silos. The Strategy therefore contains not just strategic objectives for policy and legislation, but measures and recommendations for the public, private and Third Sectors in a series of collated action plans[1]. For the Third Sector, the Framework set out 20 actions divided into seven overarching aims to improve, increase and promote cyber resilience.

The charitable, social and not-for-profit enterprises comprising the Third Sector provide highly specialised services in Scotland, and the UK in general. As such it is a vital part of society. However, it is not immune to cyber risk. Due to the rapid digitalisation brought on by the Covid-19 pandemic, all sectors of society have become increasingly vulnerable to cyber risk. The Third Sector in Scotland has experienced its fair share of malicious cyber activity, one of the most prominent being the SAMH incident of 2022[2].

In autumn 2022 the Scottish Government commissioned Dewar Cyber Consulting Ltd (DCC), an independent Edinburgh-based cyber security consultancy, to conduct applied policy research to examine the challenges faced by the Third Sector in Scotland, examine the impact of the Strategic Framework and to provide practical, specific steps for action to develop cyber resilience in the third sector. On completion of the fieldwork for this project, DCC has identified the following five overarching challenges and makes 10 recommendations:

<u>Challenges</u>

1. Lack of consistency in messaging from regulators and government, as well as lack of consistency in regulatory frameworks
2. Variable degrees of board-level experience and understanding of cyber risks
3. Current UK and international cyber resilience certification systems not fit for many Third Sector purposes
4. Use of cyber-industry terminology and jargon is a counterproductive barrier
5. Funding to support cyber resilience across the third sector

<u>Recommendations</u>

1. Streamline cyber security/resilience communication for the Third Sector
2. Streamline terminology and reduce jargon
3. Consolidate and coordinate local authority cyber security requirements
4. Establish an integrated “cyber assistance office” at the Office of the Scottish Charities Regulator or similar
5. Formalise the Third Sector Catalyst Group as an information exchange and reporting authority
6. Implement a Single Supplier or Trusted Partner Framework for digital and cyber tools for the Third Sector
7. Create a new Third Sector-specific accreditation for minimum levels of security with manageable expectations
8. In any government funding processes stipulate the requirement for embedding cyber resilience measures, and fund this stipulation accordingly.
9. Develop free or reduced cost cyber resilience e-learning resources for Third Sector organisations
10. Share lessons learned from cyber security incidents.

[1] ‘Cyber Resilient Scotland’.

[2] ‘SAMH Announcement’.

2. Introduction

Social enterprises represent an influential sector of commerce that are imbued with notable characteristics that make them not only susceptible to cyberattack but also the organization and the individuals with whom they engage have the potential to be harmfully impacted by their effect[3]

In 2022, it is recognised that we live in a highly digital and digitalised world. While changes were taking place to the way people lived their lives, with more and more interactions taking place on digital devices, the Covid-19 pandemic sped up that change. Many people had to work or study from home, or to live their lives at home due to furlough and lockdown requirements. Cyber security and cyber resilience, already a strategic priority for Scotland, were pushed further up the policy ladder with the publication of the *Strategic Framework for a Cyber Resilient Scotland*[4]. More and more people needed to be aware of cyber security risks and opportunities.

It is already acknowledged that the Third Sector in Scotland not only plays a vital role in providing crucial services to society, but that the Sector is just as vulnerable to cyber risks and threats as the public or private sectors. According to figures from the IASME corporation, nearly a quarter of charities reported breaches of one form or another on a weekly basis[5].

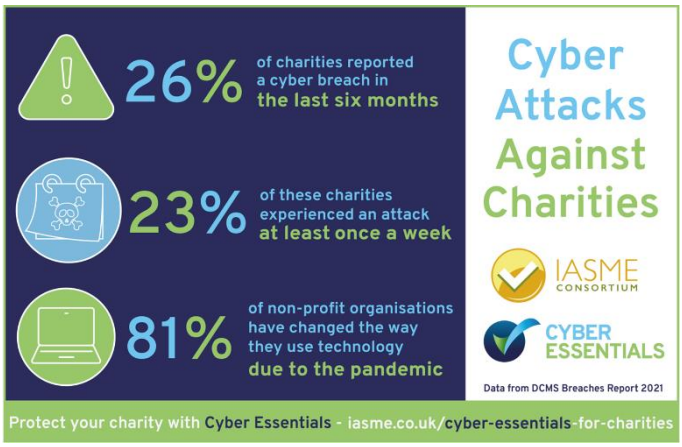

Image Source: IASME

Despite this explicit acknowledgement, however, the Third Sector in Scotland has faced a number of challenges to developing and improving it's cyber resilience posture. The Scottish Government and other agencies promoting a cyber resilient Scotland have conducted a range of activities in recent years, including workshops, seminars, pubic information campaigns and focus groups in attempts to raise awareness of cyber risks in Third Sector organisations, and to increase sector resilience. To date, these activities have met with mixed success.

Dewar Cyber Consulting Ltd. (DCC) has been tasked with conducting research on behalf of the Scottish Government's Cyber Resilience Unit on cyber resilience challenges within Scotland's Third Sector. The objective of this research is to identify what practical steps can be taken to assist the Third Sector in Scotland to increase its cyber resilience. Analysis and research have been conducted before, and Third Sector entities have been surveyed in the past. The purpose of this present research is to collate these previous activities and distil practical and actionable solutions, augmented by further engagement with Third Sector representatives, rather than propose abstract or esoteric policy guidelines.

[3] White et al., 'Antecedents of Cybersecurity Implementation'.
[4] 'Cyber Resilient Scotland'.
[5] 'Cyber Security Challenges for the Charity Sector – How Can Cyber Essentials Help?'

To that end, the project has three key deliverables:

1. an initial standalone workshop at the third sector catalyst group hosted by the Scottish Government and DCC. This was conducted on 31 May 2022 in Edinburgh
2. a publication comprising academic-quality research (this present report)
3. a closing seminar/workshop for the launch of the publication in 2023

As stated above, the main objectives of this project are to provide the Scottish Government with a piece of applied policy research examining the current state of cyber resilience in the Scottish Third Sector and to identify key opportunities and challenges for development. This includes identifying the needs of the sector as a whole and its constituents and providing effective, practicable and reasonable recommendations for actions to improve the cyber resilience posture of the Third Sector in Scotland.

A series of semi-structured interviews identified five prominent challenges facing the Third Sector in Scotland. Chief amongst these was a lack of consistency in messaging and regulatory compliance requirements which hampered even the best efforts of Third Sector organisations. Respondents reported feeling overwhelmed by the amount of information being provided to them and being inundated with threat analyses from numerous different agencies. In addition, different local authorities across Scotland have different cyber resilience requirements in terms of certifications or infrastructure, which causes problems for those Third Sector organisations operating in numerous authorities. What is required in one region is not required in another. This makes ensuring compliance very difficult and is a costly process to achieve. One of the most prominent recommendations in this report is the establishment of a central “voice” for cyber security in Scotland – ideally for all sectors, but in the first instance particularly for hard-to-reach demographics such as the Third Sector. As will be explored later in this repor, the cyber Scotland partnership already has third sector representation, so could potentially take this role.

Additional challenges arise when cyber security agencies publish guidance, advice and information which utilises significant amounts of technical jargon. With the best will in the world, many organisations simply have not had enough training and education to assimilate this technical detail. This is particularly the case for those organisations with service-user board members. Ensuring cyber security remains a board- or C-suite level policy concern is a strategic goal for Scottish authorities and cyber security agencies but is a challenge for board members who are also Third Sector service users. One of the core recommendations presented here is to simplify the language of cyber security, not to dumb it down, but to make it more accessible. This improvement in language combined with a single voice for cyber security information would alleviate many of the challenges of comprehension and accessibility.

Another significant barrier to increasing cyber security and resilience in the sector is the perception in that sector that policy-makers, legislators and national cyber security agencies do not take enough account of the *context* of the Scottish Third Sector. The sector is not homogenous, and different organisations, even those operating in the same service user space, have often very different operational requirements and digital needs. A significant issue is funding. While a lack of income, particularly during the 2022 cost of living crisis, affects all aspects of Third Sector operations requiring often brutal spending choices, a number of mechanisms being promoted by national agencies, such as accreditations, require ancillary costs for implementation Third Sector organisations simply are not in a position to meet. Making certification and compliance fit for Third Sector purposes would go a long way to recognising the specific contexts of the Third Sector.

This report sets out a number of specific recommended actions policymakers and legislators should implement in order to take account of that context. One size does not fit all when it

comes to achieving cyber security or cyber resilience, and nowhere is this more true than in the case of the Third Sector. Accreditation and certification regimes must be made fit for purpose or made anew with specific reference to Third Sector organisations. The terminology used must be relatable and comprehensible, particularly for service user board members tasked with taking important decisions for the organisations they represent. This recognition of context goes both ways, however. Funding is being made available for core activities. One recommendation in this report is that any funding allocations include a portion being set aside for digital or cyber tasks. This would ensure that the message that all societal aspects in 2022 have a digital or cyber component would be heard, and a fraction of funding be set aside to ensure that.

This report is constructed as follows. Chapter three out the research methodology employed to gather data for analysis. While chapter four includes a list of the Third Sector entities interviewed demonstrating the cross-sectional analysis required to make effective recommendations.

Chapter five of the report examines the current literature and publications relating to cyber security in the third sector. While not a literature review in the traditional academic sense of the term, it makes the point that there is a great deal of academic study of the problem being published but not captured in policy. This is something decision-makers may wish to consider.

Chapter six of the report sets out five specific challenges facing the improvement of cyber resilience in the Third Sector in Scotland:

1. Lack of consistency in key areas of operation
2. Board level experience and knowledge
3. Current UK and international certification requirements not suitable for the Scottish Third Sector
4. Language and terminology must be adapted
5. Funding needs to be more creatively allocated

Chapter seven sets out ten practical actions for decision makers to implement in order to meet those challenges.

1. Streamline cyber security/resilience communication for the Third Sector
2. Streamline terminology and reduce jargon
3. Consolidated and coordinated local authority cybersecurity requirements
4. Establish an integrated “cyber assistance office” at the Office of the Scottish Charities Regulator, or similar umbrella organisation
5. Formalise the Third Sector Catalyst Group as an information exchange and reporting authority
6. Implement a Single Supplier or Trusted Partner Framework for digital and cyber tools for the Third Sector
7. Create a new Third Sector-specific accreditation with manageable expectations
8. In any funding grant, stipulate a portion or provide additional funding for cyber-related measures.
9. Develop a free or reduced cost e-learning portal for Third Sector organisations
10. Learn lessons from the NHS digital and cyber security departments.

2.1. Methodology

This project was conducted using recognised academic research principles and tools. Following initial and project-launch discussions with the Cyber Resilience Unit of the Scottish Government (SG CRU), a project scope was agreed which enabled research tools and techniques appropriate to this level of analysis to be deployed.

Following project initiation, the most important aspect of the research was fieldwork. This comprised a series of semi-structured interviews with senior staff and decision-makers in Scottish Third Sector service providers, umbrella organisations, compliance auditors and regulators. The objective, agreed with the SG CRU, was to conduct and achieve a cross-sectional analysis of cyber resilience issues, challenges, and requirements across the whole of the Scottish Third Sector, including regulatory bodies, not just front-line entities.

Once an initial respondent list was agreed with the SG CRU, DCC Ltd reached out to Third Sector entities to secure interviews with introductions from the CRU. These were conducted online using MS Teams. Once interviews were secured and conducted, a snowball process was utilised to encourage and gain further meetings.

The interviews themselves were conducted using "semi-structured" techniques. Semi-structured interviews are conducted in a formal environment with a set of pre-determined questions, but which allow additional or supplemental questions to arise during the conversation[6].

Where permission was given the interviews were recorded. On completion of the interview a transcript was produced, and the text uploaded into NVivo computer-assisted qualitative data analysis software. This enabled common themes and views to be identified and correlated. This research process was developed by Dr Robert Dewar for conducting large scale policy analysis while at the University of Glasgow[7].

2.2. Organisations interviewed

The project parameters required a minimum of 10 Third Sector organisations be interviewed for the project. This total was to include membership and umbrella organisations, and those entities with a direct interest or mandate for operating with front line Third Sector entities.

On completion of the fieldwork component of the project, a total of twelve organisations were successfully interviewed. These were:

- Scottish Federation of Housing Associations (SFHA)
- Scottish Social Services Council (SSSC)
- Association of Chief Officers of Scottish Voluntary Organisations (ACOSVO)
- Lead Scotland
- The UK National Cyber Security Centre (NCSC)
- Scottish Council for Voluntary Organisations (SCVO)
- Office of the Scottish Charities Regulator (OSCR)
- Glasgow Council for the Voluntary Sector (GCVS)
- Turning Point
- Coalition of Care and Support Providers in Scotland (CCPS)
- Aberlour Children's Charity
- Sight Scotland

[6] Bryman, *Social Research Methods*.
[7] Dewar, 'Cyber Security in the European Union'.

Interview subjects were drawn from C-suite decision makers and directors of IT or operations, indicating a high level of interest and engagement with the project, the seriousness with which cyber security is taken in the Third Sector and the level of engagement and decision making at the entities surveyed.

3. Review of current publications and research in the field

This present report is not the first examination and analysis of cyber security and the Scottish Third Sector. There are several industry-specific publications which explore and explain key cyber risks such as data breaches and ransomware, and their impact on social enterprises, charities and other organisations. A challenge identified by several respondents for this report is making those publications relevant and accessible to the Scottish Third Sector – in terms of raising awareness AND issues of jargon – for some of the smaller yet critical Scottish Third Sector service providers.

There are four prominent publications which fall into this category.

1. 2022 ACOSVO report, “Not if, But When”
2. Cyber Scotland’s Incident Response Plan booklet and accompanying PPT presentation
3. The SFHA’s invitation to a learning programme on cyber security for housing associations
4. The Scottish Government's Third Sector Action Plan, part of its larger Strategic Framework for a Cyber Resilient Scotland.

These four documents provide invaluable advice and suggestions for improving the cyber resilience of Third Sector organisations in Scotland. However, a recurring comment in the Cyber Catalyst project launch meeting and in approximately 75% of respondent interviews is that these documents did not “speak the language” of its target audience. Common phrases such as “multifactor authentication”, “AV software” (meaning antivirus software), “incident triage” and “proxies” are important terms for cyber security in any sector, but create barriers to implementation for those not familiar with these concepts. The language and terminology used to engage the Third Sector in Scotland with cyber resilience tools, solutions and techniques must be made sector appropriate. This is particularly important for those organisations with high levels of service user management, such as care homes. This is not to say that the information contained in these, and other publications is not useful. On the contrary. It simply must be made more accessible and more effort undertaken to ensure understanding.

A second challenge evident in the current literature is repetition and replication. The publications highlighted above all provide good advice and solutions (jargon notwithstanding). However, a sizeable proportion of that advice is replicated across them. Examples include the importance of staff knowing where incident response plans are stored, having clear communications processes and reporting mechanisms. While these are important enough to emphasise, repetition and replication implies time taken by each publishing organisation separately to produce and achieve the same results. This is inefficient and speaks to Challenge 4.1 of this Report – an overwhelming amount of information being published and pushed on the Third Sector. Greater effort to streamline and consolidate publications and communication processes would avoid replication and duplication, as well as avoiding information overload, thus ensuring messages are heard.

A final point evident in the current literature around cyber security and the Third Sector relates to academic publications. These are journal articles and books which examine the cyber challenges faced by the Third Sector in general, its position in wider cyber security responses, and its impact on digital society. It is not appropriate to undertake a traditional academic review of these publications; however, it is beneficial to point out that a great deal of academic work is being undertaken in this field. In 2022 alone well over 20 journal articles were published around the world. While the majority of these examined the percentage of charities reporting incidents, or the use of fake charities in phishing operations, it would

nevertheless be useful to policy makers to work with academic institutions to convert these published findings into practical policy solutions. This is a potential future project the SG and the Cyber Catalyst Group may wish to consider.

4. Findings: Challenges facing the Third Sector

4.1. Lack of consistency in key areas of operation causing significant bottlenecks

There are several areas where a lack of consistent approach is causing significant bottlenecks for the Third Sector to achieve or improve cyber resilience. Several respondents reported feeling overwhelmed with the amount of information with which they are being provided, as well as receiving that information from a range of sources. Regulatory bodies, government entities, local, regional, and national cyber security, and resilience entities all routinely publish material, advice and guidance, much of which does not speak to the specific contexts in which the Third Sector operates. Sifting through this wealth of information is, as some of the respondents noted, almost a full-time job.

While the respondents note that the information is often useful and always well-intended, it is counter-productive, particularly for the smallest Third Sector entities. The message that cyber security and resilience in Scotland is something we must all be a part of is being lost, not due to malice or unwillingness to play their part, but simply due to lack of capacity on the part of these smallest entities to engage in any meaningful manner with the subject: they simply have other more pressing and pertinent priorities. As a result, cyber, digital, information or computer security is an afterthought. This is not to say that there are no risks, or that staff are ignorant or burying their heads in the sand. It is simply that there are other more pressing concerns.

One of those concerns is juggling the complex web of regulatory compliance and local authority requirements in Scotland. Many Third Sector organisations operate nationally across Scotland. While this has an impact, it requires these organisations to navigate different local authority regulatory frameworks. Respondents noted that this is particularly problematic when it comes to cyber security certification requirements, such as Cyber Essentials or ISO 27001. One respondent noted that in one local authority in which they operate, Cyber Essentials is desirable but not mandatory for that organisation to provide their service. However, in another area, the same organisation is required to have verifiable Cyber Essentials certification to provide the same service. This inconsistency provides barriers not only to the engagement of Third Sector organisations with particular local authorities, but prevents them from expanding their services.

This lack of consistent frameworks of operation is also reflected in internal processes, particularly as regards regulatory compliance. One umbrella organisation surveyed for this report noted that, due to their members providing a range of care services, they are legally required to comply and be audited by two if not three national regulatory bodies depending on the service being provided. This has the result that two sometimes three regulatory compliance frameworks clash when it comes to data, digital and information security. Work carried out to ensure compliance with one regulator must sometimes be repeated or undone in order to comply with another regulator. Streamlining regulatory compliance would significantly improve Third Sector organisations' capacity to provide their services by reducing red tape.

4.2. Varying levels of board level experience and knowledge in Third Sector

An unexpected finding came about when discussing senior and board-level decision making in Scottish Third Sector organisations. Cyber security needs to be a priority at board level across the public, private and Third Sectors. However, many Third Sector organisations, particularly social care providers, have tenant or service user board members and leadership. This is a challenge for pushing *internal* policy due to lack of awareness and knowledge of external threats and internal infrastructure or prioritisation when faced with more pressing social challenges. Survey respondents and the authors of this report are at pains to point out that this is not meant to be a judgement of the understanding and capability of board members. Rather, it reflects the fact that many if not most are not cyber security specialists and have a vested interest in ensuring basic services are provided and supported, rather than digital infrastructure. One respondent elaborated that in board meetings with service users, it is challenging to explain the global cyber resilience risk landscape in a way which conveys the importance of protecting against those risks, without fearmongering or providing lectures on the technicalities of cyber and digital security solutions.

This report hypothesises that this may be another reason for the perceived lack of uptake of cyber resilience and cyber security measures and advice in the Third Sector: board-level decision makers are choosing to prioritise other aspects of Third Sector service provision over cyber issues, not just because of funding (see Challenge 4.5 below) but because this is a completely new and different way of living and thinking, with new and different challenges of which they were never aware in their personal lives.

4.3. Current UK and international certification regimes do not suit Third Sector

Cyber Essentials and ISO 27001 are increasingly becoming required certifications for a range of entities operating in Scotland. For private and public sector projects and contracts, these programmes are becoming standard attainment targets for contractors. According to a number of respondents, the same is true for Third Sector organisations. This is a significant challenge and hurdle for these organisations, particularly the smallest entities which provide the most niche services.

The concept of cyber security and cyber resilience certification as a proof of compliance or adherence to a minimum standard is not one with which respondents disagreed. Issues with certification arose during discussions about the level of technical knowledge and understanding required before an organisation attempts assessment. ISO 27001 is out of reach for almost all Third Sector organisations operating in Scotland save the largest, primarily due to cost (See Challenge 4.5 and Recommendation 5.7 below).

However in some areas of the third sector even Cyber Essentials is an almost insurmountable challenge when completing self-assessment. Many smaller organisations, which in turn are often the most vulnerable to cyber incidents, are simply not technically able to engage with the questions and provide answers which would pass assessment; the certification is too advanced for the organisation. This would be less of challenge if certification were not becoming a requirement for many organisations to bid for or provide service contracts. Because Cyber Essentials is being seen as the minimum standard for cyber resilience capability, many contract clients are insisting on service providers demonstrating they have the certification.

Many small organisations are simply unable to meet these criteria but are nevertheless expected, encouraged and in some cases required to achieve these certifications without any support for meeting assessment criteria from a technical or staff capability perspective. Both are costly, require a significant amount of *a priori* knowledge of computer and digital systems, and there are significant ancillary costs associated with installing systems and infrastructure which meet the basic criteria.

While Cyber Essentials is therefore suitable for the private and public sectors, it does not fit the idiosyncratic contexts of the Third Sector and is proving to be a barrier to improving the level and understanding of cyber resilience in this sector.

4.4. Language and terminology a barrier to the Third Sector achieving cyber resilience

One important recurring theme in the research is the problem of jargon and the (over)use of the prefix “cyber”. The overall consensus is that reducing the amount of jargon in current messaging, changing the terminology and simplifying messaging would greatly improve communication to and within the sector. While the prefix “cyber” is a commonly used term in policy, research, the private and public sectors and the media, it is a counter-productive term when used both in the context of the Third Sector itself and in measures intended to raise awareness of cyber challenges in the sector.

The basic challenge is one of comprehension. There is a substantial body of literature, and an entire academic sub-field, devoted to answering the question “what does ‘cyber’ mean?” The problem is amplified in the Third Sector in Scotland with a number of respondents asking that same question. Because there is a lack of consistent understanding of what cyber security actually is, many messages and recommendations for, e.g., good cyber hygiene are not hitting their mark. This leads to confusion around what is expected of the sector from regulators and the Scottish Government.

This absence of consistent understanding is exacerbated by the fact that “cyber” has become a fear-laden term. The prevailing narrative from official and news-media channels provokes and promotes a climate of fear of imminent digital disaster (cyber Pearl Harbour) or of cyber criminals constantly trying new and innovative techniques to steal things. The term “cyber attack” is routinely used to refer to any malicious incident, large or small, with little to no context provided. As a result, the message being sent out and received is that we are all about to be victims of a cyber attack of apocalyptic levels, when in reality we may be targets for theft or abuse this is not meant to belittle these threats. The point here is at there are many steps that can be taken to avoid or mitigate them, but this message is not being heard.

The final challenge highlighted through the use of “cyber” is that it leads to assumptions that cyber security/resilience is solely an IT issue rather than a social issue. This results in smaller organisations and those without in-house IT teams assuming that it’s not a problem for them. The message that cyber security/resilience is vital for everyone using the internet is not getting through.

4.5. Funding

Third Sector organisations are often short of funds to achieve their aims. This means that tough decisions have to be made about where to allocate finite financial resources. 11 of the 12 interviews specifically mentioned funding as a barrier to the Third Sector improving, achieving or working towards better cyber resilience. This challenge came in many guises. The most common comment was around prioritisation. Third Sector entities have only a finite

amount of money to spend on all their activities, including staff, infrastructure and the services for which they were established.

Setting aside the question of budget priorities however, there were a number of important points made when the conversations turned to finances and funding. Due to the semi-permanent changes in working practices caused by the Covid-19 pandemic many organisations are instituting home or hybrid working as standard.

The public and private sector have a level of capacity to finance this societal shift. However many if not most Third Sector organisations across Scotland struggle. Not only do organisations not have the resources to provide all staff with the latest secure laptops or mobile phones, many employees and staff do not own high-spec devices of their own. While Bring-Your-Own-Device (BYOD) is becoming more and more prevalent, those devices are themselves often insecure, in part due to a lack of understanding on the part of the staff members themselves, but also due to the staff not being able to afford a new laptop or secure internet connection.

The hidden additional costs of secure digital working extend to certification regimes such as Cyber Essentials or ISO 27001. Both Cyber Essentials and ISO 27001 are expensive processes to undertake. The cheapest rate for Cyber Essentials is that for micro-organisations (0-9 employees) and is £300+VAT. For some Third Sector organisations this is insurmountable when set alongside standard running costs or the costs of providing the services for which they were established. Furthermore, should an organisation undertake the Cyber Essentials certification, pay the fee but fail the assessment, they have 48 hours in which to carry out any remedial actions before being required to pay the fee again for an additional assessment, with no guarantee of passing. The certification must also be annually renewed. For ISO 27001, costs start at around £3750 for an organisation of 1-45 employees. These costs are *in addition* to the costs involved in acquiring, upgrading, and installing the technological and digital solutions necessary to pass the assessments. For obvious reasons, certification is therefore not a priority for many small and medium-sized Third Sector entities.

The final frequently occurring comment around funding is that many of the sources of assistance are grant-based. While this is welcome, many of these schemes are one-off, with little to no continuity of support. As one respondent pointed out, if society wants the Third Sector to be cyber resilient, then it must invest in this as an ongoing process, with continuous support, not a fire-and-forget mentality of one-off grants.

5. Recommendations

5.1. Streamline cyber security communication

One of the most prominent and frequently occurring comments relating to cyber security in the Scottish Third Sector is that the sector feels overwhelmed by the range, breadth and scale of messaging it receives on cyber security and resilience threats, good practice and countermeasures. There is a vast array of regulatory, policy and governance publications from various entities of which Third Sector organisations are expected to note. In addition to the governance and compliance measures from regulators and auditors and the legal frameworks (particularly data protection) within which these entities operate.

While all of the organisations surveyed for this report acknowledged both the importance of digital and cyber security to their and Scotland's wellbeing, a constant refrain was that it was as great a challenge to identify which pieces of advice to pursue, or which regulatory framework with which to comply. Having a single or at least streamlined but reputable communication channel for all or as much information as possible would reduce the information overload currently experienced by many Third Sector organisations. This would also ensure that important information is not lost in the noise.

This report recommends that a single entity be selected as the "voice" of cyber security in Scotland generally, including for the Third Sector. This could be the Third Sector Catalyst Group (see Recommendation 5.5 below) or the Cyber Scotland Partnership which already has third sector representation. Further discussions would be needed to determine the most suitable representative body.

5.2. Streamline terminology

Another repeated comment in the respondent interviews was the need to use clearer and more succinct terminology, especially for the smallest Third Sector organisations. Term such as "cyber security" become progressively less meaningful, and there is a certain level of fatigue amongst many of the respondents when they hear the term. One of the main comments from the launch meeting for this project was that policy-makers and practitioners in general, and those working with the Third Sector in particular, should try to focus on the issues they are dealing with, rather than employ catch-all terms such as "cyber security" or "cyber resilience" that require a degree of technical understanding before progress can be made.

There are two parts to this Recommendation. First, a project should be undertaken to remove jargon from the field and identify how best and most effectively to refer to the various cyber challenges present. Terms such as "cyber security" are not effective when communicating threats, risks, and opportunities to the Third Sector in Scotland. Work is needed to identify what plain English terms would be most effective.

Second, once plain English for the sector is achieved, a central, trusted, verifiable and reliable conduit for messages, announcements, policy changes and recommendations should be established to streamline communications to the sector. This second point is elaborated upon in Recommendation 5.1 above.

5.3. Consolidate Scottish local authority tender requirements

One of the most challenging aspects of operating in the Scottish Third Sector is the variance between local authority digital requirements. As set out in Challenge 4.1 above, Third Sector

entities operating in multiple local authority jurisdictions are required to meet different regulatory and compliance criteria for each area. This creates confusion and inconsistency.

It is therefore recommended that the Scottish Government, the Third Sector Catalyst Group and COSLA work together to create a single coordinated metric for the digital aspect of Third Sector service provision. Different regions will have different social needs, but the digital and cyber element of meeting those needs can be made consistent.

5.4. Establish an integrated "cyber assistance office" at the OSCR

The Office of the Scottish Charities Regulator already monitors and manages the activities of the c.25,000 registered charities in Scotland. Regulation of cyber resilience has been identified as an important benefit to the sector, to maintain consistency and improve/increase the resilience of the sector as a whole. Formalising the regulation of cyber resilience in the sector may centralise these efforts.

However, the role and function of this recommended entity should not be one of regulation in the traditional sense. Regulators examine the organisations under their aegis, and then provide recommendations for action/change, sometimes under threat of sanctions. A sanctions regime would not benefit the Third Sector in Scotland.

This report recommends changing the framework of regulation to be one of provision of practical assistance once issues have been identified. This would include not only advice on how to resolve a particular digital vulnerability but involve working with the organisations on a quasi-consultancy bases to take active steps to facilitate and action that resolution. The office should therefore not be labelled as a "cyber regulator", but "cyber assistance office".

There should be two specific areas of work for this office. First, an essential element of this assistance- and incentive-based regulatory regime would be the creation of off-the-shelf templates for policies, tools and procedures. Because it is often not clear what is expected of particular organisations, the OSCR should collaborate with other stakeholders such as the SG CRU (inter alia) to support the development of a baseline measure of resilience across the whole Third Sector and produce templates to achieve this. Current tools and metrics provided by organisations such as the NCSC are known, but not seen as relevant to the Sector. Sector-specific tools, potentially as simple as forms to complete outlining what to do in a particular, generic cyber situation, may be more beneficial. This would achieve a number of cyber resilience goals: a metric would be produced as well as specific practical steps to achieving that metric, and the Third Sector would benefit from practical guidance and activities in achieving those baseline security posture.

Second, the proposed "Cyber Assistance Office" (CAO) of the OSCR could also be the central point from which communications regarding cyber resilience in the Third Sector should be published (see Recommendation 5.1 above). This would resolve many of the communications and messaging challenges evidenced in the research for this report. This is not to say that the OSCR should be the sole creator of those messages. Instead, it should function as a conduit and moderator for those organisations such as the Cyber Scotland Partnership (CSP) who are routinely publishing on cyber issues.

It should be noted at this point that the CSP is a collaborative initiative dedicated to increasing and improving Scotland-wide cyber resilience. Its stated aim is to act as "a

collaboration of key strategic stakeholders, brought together to focus efforts on improving cyber resilience across Scotland in a coordinated and coherent way[8]

5.5. Formalise the Third Sector Catalyst Group for leadership and oversight, as well as incident reporting.

While the OSCR can provide a regulation-by-assistance service, leadership and oversight is needed for the sector in cyber resilience. It is recommended that the Third Sector Catalyst group be formally instituted as the entity for that leadership and oversight. Membership is currently informal, but many organisations from across the spectrum of Third Sector services take part. This makes the Catalyst Group an ideal entity for policy development, information-sharing, and leadership.

Communication of messages has been identified as a key challenge for the Sector. This incorporates both communication TO organisations FROM regulators, the Scottish Government and other entities, but also communication FROM the Third Sector TO these entities. A trusted mechanism for reporting cyber incidents affecting the Third Sector would bring greater clarity of the threats and risks faced, as well as (potentially) provide an incident response service. Currently, the Cyber and Fraud Centre Scotland (CFCS) provides an incident triage service that is open to all Scottish entities. However, within some third sector organisations it is unclear whether the CFCS provide a service solely to the private and public sectors. Additional research is required to examine whether there is an assumption that the CFCS service is for the private and public sectors only, or whether there are other barriers. Whatever the findings, this report currently recommends tasking a formalised catalyst group with being the incident reporting and response entity for the sector. This would ensure that important incident information is recorded, as well as providing response tools and suggestions from individuals aware of the nuances of the Third Sector.

That being said one of the key responsibilities of the proposed Scottish Cyber Coordination Centre (SC3) is to improve early warning and intelligence coordination. It is anticipated and expected that the SC3 would have a core role in supporting the Third Sector. A way to achieve this could be by the SC3 sharing information and intelligence summaries with the Third Sector Catalyst Group or other Third Sector representative network so that sensible, informed policy decisions can be made for the sector on the basis of sound evidence.

5.6. Implement a Single Supplier Framework or Trusted Partner programme for provision of digital assets

Where organisations are aware of their responsibilities and are in a position to implement internal cyber resilience or data protection policies, they are required to go to the open market for any tools platforms, software or other solutions to meet their requirements and those of their regulatory bodies. This is the case for several business areas including business development, cloud security, multifactor authentication or secure devices.

It is worth pointing out that this situation – the need to go to the open market for solutions – is not restricted to the Third Sector in Scotland. All sectors around the world rely on third party providers of key infrastructure solutions, whether those are device manufacturers, antivirus developers or office tools platforms. For this reason, this situation is not listed as a challenge facing the Third Sector, as it is universal.

[8] https://www.cyberscotland.com/about/ More information on the CSP and its membership is included in Appendix 1 of this report.

That being said, Third Sector entities are often not able to afford the recommended or industry leading solutions. This leads to entities relying on free, open-source tools with limited functionality and little recourse should security issues arise.

This challenge is also not only restricted to security solutions, but to staff training and education. In one of the interviews conducted for this report, three diverse, separate entities were surveyed. When the semi-structured discussion turned to questions of internal staff training, all three organisations stated that they had used online platforms for this purpose. However, they had used three different platforms to achieve largely the same ends.

While this reflects poorly on the overlap and duplication in the open cyber security market, the systemic issue facing Third Sector entities in Scotland is “which provider to trust?”. Without prejudice to the quality and comprehensiveness of the three third-party providers, the organisations surveyed all agreed that it was not an ideal situation, that each organisation had independently carried out reviews, for which there was a cost, to select a platform for internal training.

What was missing from this process was a) communication between the three entities to share experiences and b) a single trusted supplier which could potentially provide preferential rates to Scottish Third Sector organisations. An example of this exists already. One of the organisations surveyed stated that they had entered into a single supplier contract with a mobile phone network to supply devices and connectivity to all their workers. The network in question provides preferential rates to Third Sector organisations. However, this was not widely advertised, and the survey respondent advised that they had heard of this promotion during an industry online conference call and had decided to follow it up.

Third Sector organisations are often paralysed by choice and unsure which platform to choose over another. This report therefore recommends compiling a list of vetted third-party providers which Third Sector entities in Scotland would recommend for particular digital or cyber purposes. If possible, preferential rates for third sector organisations could be negotiated. The list could and should be maintained centrally for all organisations to access. If a single supplier is found to be a preferred provider, then a single supplier framework could conceivably by created, thereby removing questions of trust and reliability from the procurement processes of Third Sector organisations, be already cleared by regulators as a provider of services which meet compliance requirements and be potentially low-cost or subsidised by regulators and/or the Scottish Government. An example of such partnerships is the procurement of Microsoft 365 by the Digital Office for Scottish Local Government[9].

It must be pointed out, that such a process does not eliminate cyber risks. It is a process for managing that risk that may be cost-effective as well as cyber effective.

5.7. Create new Third Sector specific accreditation

Throughout the research for this project, the concept of Cyber Essentials and ISO 27001, the UK and international certifications for achieving a base standard of cyber security, were routinely discussed. The general consensus was that having a certification was a positive measure. It allows organisations to advertise their skills and expertise, while at the same time providing a standardised structure for achieving a base-level of security in an organisation.

As set out in Challenge 4.3 and 4.5 above, the current system of certification is unsustainable and unaffordable for many Third Sector organisations in Scotland. The

[9] Digital Office, ‘Cyber Security’.

challenge is further exacerbated because, according to a number of Respondents, many contract clients now require either Cyber Essentials or ISO 27001 before awarding contracts for services. Additionally, as stated above, some organisations provide services in different Scottish local authorities with differing accreditation requirements, creating inconsistencies.

That being the case, a system of accreditation for Third Sector organisations, associated training and support, is perceived as a positive benefit for Scotland. This report therefore recommends the initiation of a Scottish Third Sector cyber security accreditation system based on a sliding scale of cyber security requirements and achievements. Precise details would require a separate consultation, but an example would be as follows (for illustrative purposes only):

- Bronze level – organisation meets basic legal requirements including GDPR compliance and using recognised free antivirus software
- Silver level – Bronze plus multifactor authentication on BYOD systems
- Gold level – Bronze and Silver plus air-gapped servers, encrypted cloud storage and paid-for antivirus

Bronze level would be free to all applicants. Silver and Gold could be achieved for a fee.

The sliding scale would be accredited not just by an independent verifying organisation but be accepted by the various regulatory bodies overseeing the various fields of the Third Sector, such as the SFHA, OSCR and the Care Commission.

5.8. Greater specificity when allocating funding

As society recovers from the Covid 19 pandemic, the Third Sector in Scotland and the UK is struggling to fulfil its mandates given the cost-of-living crisis. As a result, income and funding are chronic issues for these entities. Many organisations do not have enough funds to carry out the services and functions for which they were established. This was a common refrain across the majority of respondent surveys. It is all very well for the Scottish Government, regulators and cyber security agencies in Scotland and the UK to push for more resilience in the sector, but without making funding available achieving this is a slim possibility.

While funding will always be an issue for Third Sector organisations, a requirement could be made in funding grants that a small percentage of any total be put towards cyber or digital security measures related to the activities the grant in intended to fund. Almost all activities conducted in any sector, not just the Third Sector, have some sort of digital component and so there would always be a role for increased cyber resilience measures.

Allocating funds with this proviso would have the effect of ensuring some money goes towards cyber security but would also highlight the fact that all activities have some sort of cyber or digital component to them.

5.9. Develop a single e-learning portal for Third Sector organisations and make it free at point of use.

Related to Recommendation 5.5 above is the recommendation to create and support an online platform for training Third Sector organisation staff and board members in cyber and digital resilience. This would negate the need for charities to go to expensive and inconsistent third-party providers, as was the case for three of the respondents. Topics covered would include issues such as cloud storage, recognising phishing, or multifactor authentication. What would separate this from some of the other offerings available in terms of training and executive education is that the topics and module content would be

specifically geared to Third Sector experiences, priorities and goals. Throughout the entire research project, the different context in which the Third Sector operates as opposed to the private or public sector creates specific challenges not present elsewhere.

A number of organisations have service user board members, thereby necessitating specific training on the use of digital tools from a C-suite perspective, but without the pressure of a C-suite training workshop. Most Third Sector organisations cannot afford to supply their staff with dedicated laptops or mobile phones, so they are required to institute BYOD systems. There are a number of security risks associated with this which would be elaborated upon and mitigated in the training.

Crucially, any platform would require the input of Scottish regulatory bodies to ensure relevance and could have sections for general cyber security requirements based on legal requirements (GDPR, reporting e.g.) and then have separatee sector specific sections (housing, mental health etc.). this would mean that ALL Third Sector organisations in Scotland would have the same base line learning, and then be able to branch off to learn things relevant for them.

This e-learning platform could also be tied into the sliding scale of certification at point 5.7 above or even be the learning and teaching requirement for a single basic certification ("Digital Thistle Mark – Bronze").

Finally, the platform should be provided free of charge, but made a core component of regulatory audit and compliance such as cloud storage, recognising phishing or multi factor authentication.

5.10. Learn lessons from the NHS Scotland and NHS National Services Scotland Digital and Security experience

The NHS across all parts of the UK is routinely targeted by operators of malicious cyber incidents. The WannaCry operation of 2017[10] and the Adastra ransomware operation of 2022[11] indicate that complex, national digital infrastructures are an almost constant target for large-scale operations.

While there are a number of lessons to be learned from these incidents for the whole of Scottish (digital) society, one specific aspect is germane for the Third Sector in Scotland. Throughout the research carried out for this report, fully 100% of the respondents reported some level of concern, action or set of solutions for managing personal or private data, or a consideration for the requirements of data protection. A number of organisations stated that they or their members were acutely conscious of the need to ensure the security, confidentiality and integrity of highly personal, sensitive information on very vulnerable service users. The rapid switch to working-from-home and use of digital communications to conduct business pushed this issue even higher up the priority level.

As a result of the need to ensure compliance around data management and ensuring the confidentiality and integrity of often highly sensitive personal data, it would be of benefit for current and future policy makers to look at the examples set by large-scale national infrastructures such as the NHS, and examine the tools, processes, procedures and incident responses undertaken to mitigate cyber risk. Even where breaches occurred (WannaCry

[10] Ghafur et al., 'The Challenges of Cybersecurity in Health Care'; Gibbs, 'WannaCry Hackers Still Trying to Revive Attack Says Accidental Hero'.

[11] Rodger, 'Cyber Attacks "crippled Scots NHS Systems" with Patient Records Stored on Paper'; Sephton, 'Ministers Coordinating "resilience Response" after "Major" Cyber Attack Hits NHS Systems across UK'.

2017 and Adastra 2022) there are lessons to be learned and positive messages for all entities entrusted with sensitive data. The NHS NSS Digital and Security department should be approached, if it has not been already, to provide guidance, mentorship or support to Third Sector organisations.

Appendix 1 – The Cyber Scotland Partnership

- The CyberScotland Partnership (CSP) is a collaboration of key strategic stakeholders, brought together to focus efforts on improving cyber resilience across Scotland in a coordinated and coherent way. The 11 partners has expanded to 18 with the inclusion of UK partners including the National Cyber Security Centre, IASME (NCSC sole Cyber Essentials Partner) and the UK Cyber Security Council (self regulating body for the cyber security profession).
- The Partnership represents a commitment from partners to work together to drive the delivery of activities that will help achieve the outcomes of The Strategic Framework for a Cyber Resilient Scotland.
- Partners come together regularly as a networking group to share ideas and identify collaboration opportunities. The UK national cyber security centre (NCSC) serves a technical advisor.
- CyberScotland.com is the web portal of the CyberScortland Partnership designed to be a one stop shop for accessing a range of advice guidance and resources on cyber.
- Included in the resources is a monthly Bulletin provides the most up-to-date information about the latest threats, scams, news and updates covering cyber security and cyber resilience topics. It includes links to authoritative sources, guidance and steps you can take to protect yourself from online threats.

Founding partners of the CSP are:

- **Scottish Government** (via the Cyber Resilience Unit)
- **Police Scotland**
  - Police Scotland's purpose is to improve the safety and wellbeing of people, places and communities in Scotland, focusing on Keeping People Safe in line with values of Integrity, Fairness and Respect.
- **Cyber and Fraud Centre Scotland (CFCS)-**
  - Bringing together the Scottish business community, the CFCS aims to become the catalyst that makes Scotland one of the safest and most resilient places to live, work, and do business, both on and offline, especially during these times of economic recovery. Historically supporting businesses with raising their physical resilience by working with Police Scotland and Fire and Rescue, CFCS now focuses on providing the advice and resources to increase cyber resilience.
- **Highlands and Islands Enterprise (HIE)**
  - HIE is the economic and development agency for the North and West of Scotland, helping build a prosperous, inclusive and sustainable economy across the Highlands and Islands, attracting more people to live, work, study, invest and visit. In addition to their continued investment in digital infrastructure and support, HIE raises awareness of cyber security to businesses, social enterprises and community organisations.
- **Scottish Enterprise**
  - Scottish Enterprise is the main economic development agency for Scotland with a remit to deliver a significant lasting effect on the Scottish economy. It works with partners in the public and private sectors to find and exploit the best opportunities and to help companies to grow. Their expert advisors help businesses understand internal and external information security risks as well as to determine where vulnerabilities might exist within their systems and how they can put in place appropriate technical, administrative and procedural controls to protect themselves. They advise businesses on how they can implement the industry-recognised standards (such as Cyber Essentials/Plus,

ISO27001 and NIST) to improve data governance, reduce cyber risk and to help them respond to a cyber security incident.

- **ScotlandIS**
  - ScotlandIS is the membership and cluster organisation for the digital technologies industry in Scotland, representing over 1000 companies through the cluster ecosystem. Through the Scottish Cyber Cluster, ScotlandIS focuses on strengthening and growing the cyber security sector in Scotland. It works with members and partners to support the wider digital transformation of business and society, acts as a voice for the industry to policy makers, and provides our members with connections throughout our network in Scotland, in addition to relevant research and market intelligence.
- **Scottish Council for Voluntary Organisations (SCVO)**
  - The SCVO is the national membership body for Scotland's voluntary sector. As part of its digital skills work, it provides education and support to Third Sector organisations to improve their cyber resilience. It empowers them with knowledge and simple actions they can take to ensure that their organisation is well placed to defend itself against a cyber attack. Cyber resilience within the SCVO is supported by 17 cyber catalyst organisations who have committed at the Board level to act as cyber ambassadors for the Third Sector.
- **Young Scot**
  - Young Scot is the national youth information and citizenship charity for 11-26-year-olds in Scotland. Since 2017 and with the Scottish Government's support, Young Scot has delivered several cyber resilience and skills projects for young people. Their work includes the *Digi Know?* programme that engages young people in cybersecurity learning and skills opportunities. It also provides information on cyber resilience, security and careers in the cyber sector across a wide range of digital and social media platforms that young people spend their time, including TikTok. *Digi Know?* is available for all young people, but Young Scot targets the programme at those who wouldn't typically access opportunities, are overlooked by the system or are unsure about their future career pathways.
- **Skills Development Scotland (SDS)**
  - SDS contributes to Scotland's sustainable economic growth by supporting people and businesses to develop and apply their skills to deliver the best outcomes for our economy. Through *Digital World*, it promotes the importance of digital skills to help Scotland grow and prosper, and cyber education, training and resilience are seen as a key part of that to protect us all while we work and play online.
- **Education Scotland**
  - Education Scotland works in partnership with local authorities to ensure that learners and educators are aware of the cyber security risks associated with using technology and to help them become more cyber resilient. It supported the development of the Digital Schools Award and continues to provide schools and early learning and childcare settings with support to self-evaluate their practice and ensure that they are providing a strategic approach to cyber resilience and internet safety. Its digital officers work with a range of partners to support practitioners in schools and early learning and childcare settings to engage confidently with cyber resilience and internet safety experiences and outcomes. Through a range of professional development opportunities delivered by the digital officers, practitioners can explore how they can support young people from the early level to navigate their online life, the risks they may face, how to overcome these and develop resilience.

Since its launch, **the** CSP has expanded to include:

- **Scottish Social Security Council (SSSC)** in September 2021
    - The Scottish Social Services Council (SSSC) are the regulator for the social work, social care and early years workforce in Scotland. Its work means the people of Scotland can count on social work, social care and early years services being provided by a trusted, skilled and confident workforce. The SSSC provides resources that support the practice and learning in social and health services.
- **College Development Network (CDN)** in October 2021
    - CDN supports the college and skills system in driving success for students, their wider communities and regional economies. It engages with thousands of members of staff working in colleges across Scotland through training and network events supporting the learning workforce to develop excellent digital skills, to ultimately raise awareness of cyber resilience within the wider student body and contribute to developing the country's future workforce.
- **Youthlink Scotland** in October 2021
    - As the national agency for youth work, YouthLink Scotland aims for all young people and their families to be able to make the most of online opportunities, safely and equipped with knowledge and skills to protect themselves and be resilient to challenges. Helping young people to grow their cyber resilience is a key part of the digital youth work offer so that they can be connected and confident in their online lives, and develop vital digital skills for future employment. Its recent projects focused on embedding cyber resilience into youth work and professional learning offers. On 8 February YouthLink Scotland held a Digital Youth Work conference to mark the Safer Internet Day and celebrate the successes of practitioners in working digitally. Mr Hepburn provided a key note address to the delegates.
- **CENSIS** in December 2021
    - CENSIS is the Innovation Centre for sensor and imaging systems and Internet of Things (IoT) technologies. It helps organisations explore innovation and overcome technology barriers to achieve business transformation, acting as independent trusted advisers, allowing organisations to implement quality, efficiency and performance improvements and fast-track the development of new products and services for global markets. CENSIS helps companies integrate security features during the design stages of IoT products and services, making them 'secure by design' and without impacting their functionality. It works with organisations across Scotland to raise awareness, provide education, demonstrate best practice, and improve access to the best IoT cyber security expertise.
- **IASME Consortium** in April 2022
    - IASME is the National Cyber Security Centre's Cyber Essentials Delivery Partner. IASME offers a range of effective and affordable cyber security and counter fraud certifications.
- **UK Cyber Security Council** in October 2022.
    - The UK Cyber Security Council is the self-regulatory body for the UK's cyber security profession. It develops, promotes and stewards nationally recognised standards for cyber security in support of the UK Government's National Cyber Security Strategy to make the UK the safest place to live and work online. Working across 5 pillars – Professional Standards, Ethics, Careers & Qualifications, Outreach & Diversity, and Thought Leadership, the Council is the only body to award the title of Chartered Cybersecurity professional to individuals, alongside Associate and Principal titles.

- The Council works to standardise the sector, encourage and implement ethical practise, support more people into and through a career in cyber, and increase diversity within the profession.

References

Bryman, Alan. *Social Research Methods*. 3rd ed. Oxford: Oxford University Press, 2008.

'Cyber Resilient Scotland: Strategic Framework'. Accessed 17 November 2022. http://www.gov.scot/publications/strategic-framework-cyber-resilient-scotland/.

'Cyber Security Challenges for the Charity Sector – How Can Cyber Essentials Help?' Accessed 6 December 2022. https://www.cyberscotland.com/cyber-security-challenges-for-the-charity-sector-how-can-cyber-essentials-help/.

Dewar, Robert Scott. 'Cyber Security in the European Union', 2017, 276.

Digital Office. 'Cyber Security'. Accessed 5 December 2022. https://www.digitaloffice.scot/digital-foundation/cyber-security-9.

Ghafur, Saira, Emilia Grass, Nick R. Jennings, and Ara Darzi. 'The Challenges of Cybersecurity in Health Care: The UK National Health Service as a Case Study'. *The Lancet Digital Health* 1, no. 1 (1 May 2019): e10–12. https://doi.org/10.1016/S2589-7500(19)30005-6.

Gibbs, Samuel. 'WannaCry Hackers Still Trying to Revive Attack Says Accidental Hero'. Newspaper. The Guardian, 22 May 2017. https://www.theguardian.com/technology/2017/may/22/wannacry-hackers-ransomware-attack-kill-switch-windows-xp-7-nhs-accidental-hero-marcus-hutchins.

Rodger, Hannah. 'Cyber Attacks "crippled Scots NHS Systems" with Patient Records Stored on Paper'. Daily Record, 27 November 2022. https://www.dailyrecord.co.uk/news/scottish-news/cyber-attacks-cripple-scots-nhs-28592989.

SAMH. 'SAMH Announcement: Cybersecurity Attack'. Accessed 5 December 2022. https://www.samh.org.uk/about-us/news-and-blogs/samh-annoucenment-cybersecurity-attack.

Sephton, Connor. 'Ministers Coordinating "resilience Response" after "Major" Cyber Attack Hits NHS Systems across UK'. Sky News. Accessed 4 December 2022. https://news.sky.com/story/ministers-coordinating-resilience-response-after-major-cyber-attack-hits-nhs-systems-across-uk-12666611.

White, Gareth R. T., Robert A. Allen, Anthony Samuel, Ahmed Abdullah, and Robert J. Thomas. 'Antecedents of Cybersecurity Implementation: A Study of the Cyber-Preparedness of U.K. Social Enterprises'. *IEEE Transactions on Engineering Management* 69, no. 6 (December 2022): 3826–37. https://doi.org/10.1109/TEM.2020.2994981.

This publication is available at **www.gov.scot**

Any enquiries regarding this publication should be sent to us at

The Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

ISBN: 978-1-83521-396-4 (web only)

Published by The Scottish Government, September 2023

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS1349922 (09/23)

w w w . g o v . s c o t