Resilience in Healthcare Systems: Cyber security and Digital Transformation

Garcia-Perez, A., Cegarra-Navarro, J. G., Sallos, M., Martínez-Caro, E. & Chinnaswamy, A

DOI 10.1016/j.technovation.2022.102583
ISSN 0166-4972
ESSN 1879-2383

Publisher: Elsevier

Technovation xxx (xxxx) xxx

Contents lists available at ScienceDirect

Technovation

journal homepage: www.elsevier.com/locate/technovation

Resilience in healthcare systems: Cyber security and digital transformation

Alexeis Garcia-Perez [a,*], Juan Gabriel Cegarra-Navarro [b], Mark Paul Sallos [c], Eva Martinez-Caro [b], Anitha Chinnaswamy [d]

[a] Centre for Business in Society, Coventry University, Priory Street, Coventry, CV1 5FB, UK
[b] Faculty of Economic and Business Science, Technical University of Cartagena, Spain
[c] Lecturer in Information Systems. Higher Colleges of Technology, Dubai, Academic City, United Arab Emirates
[d] Aston Business School, Aston University, UK

ARTICLE INFO

Keywords:
Healthcare digital transformation
Healthcare digital resilience
Healthcare cybersecurity
Cybersecurity knowledge
Security in transformation

ABSTRACT

The digital transformation of the healthcare sector is an essential development as societies move into a post-industrial, knowledge-based economy. The adoption of the latest technologies and their applications in the health and care systems must be managed effectively from the perspective of their cyber security and resilience. However, there is still a limited understanding of the key concepts that must define the strategic vision of a resilient and sustainable digital transformation of the healthcare sector. Using data collected at the peak of the COVID-19 pandemic from owners and C-level executives from critical infrastructure sectors in the United Kingdom, this research analysed core constructs that contribute to the required transformative, adaptive and absorptive capacities for health systems digital resilience. The research found that a balanced base of cyber security knowledge development, uncertainty management, and consideration for the sector's high levels of systemic and organisational interdependence are essential for its digital resilience and for the sustainability of its digital transformation efforts. The paper describes the implications of these findings for research and management practice.

1. Introduction

Technology developments have driven the transformation of societies and the business environment from an industrial to a knowledge economy in recent decades. A combination of knowledge-intensive activities, innovative actions and technological advancement has resulted in innovative products and services, supported by digital-centred strategies (Garcia-Perez *et al.*, 2019). The healthcare sector has been no exception. Stakeholders of the global healthcare ecosystem continuously interact to generate new knowledge (Secundo et al., 2019), generating novel and strategic innovation frameworks (Cohen et al., 2017). Paradoxically, institutions from the healthcare sector are often unable to adopt digital-oriented business models. This is due –among other reasons, to the restrictions imposed by the national frameworks within which they have traditionally operated. Since early 2020, however, the coronavirus COVID-19 pandemic has acted as a catalyst for the adoption of technologies by the sector, driving the implementation of national strategies and international collaborations (Ienca and Vayena, 2020). This has raised a number of questions, from the need to develop new digitally focused business models to the adoption of secure digital practices that serve to protect and increase the resilience of the sector. In other words, digitisation –combined with the transition to the knowledge economy, pose new threats and challenges to the healthcare sector and its supply chain, in particular related to their digital transformation, resilience and antifragility (Cobianchi et al., 2020).

In its 2019 Global Risks report, released less than a year before the COVID-19 pandemic (WEF, 2019; Nicola et al., 2020), the World Economic Forum ranked cyberattacks as the fifth global risk based on impact. The same ranking placed the risk of infectious disease as tenth. Beyond a hindsight-based response to the ranking itself, the emergence and evolution of the COVID-19 pandemic highlighted the interdependence and co-evolutionary dynamic of the healthcare risks and cyber security risks. As the World Health Organisation declared COVID-19 a pandemic (WHO, 2020), the global healthcare sector faced the biggest transformational challenges in its history: the sudden change and adaptation to a new environment where the use of digital technologies

* Corresponding author.
E-mail addresses: Alexeis.Garcia-Perez@coventry.ac.uk (A. Garcia-Perez), Juan.Cegarra@upct.es (J.G. Cegarra-Navarro), MSallos@hct.ac.ae (M.P. Sallos), Eva.Martinez@upct.es (E. Martinez-Caro), A.Chinnaswamy@aston.ac.uk (A. Chinnaswamy).

https://doi.org/10.1016/j.technovation.2022.102583
Received 31 August 2021; Received in revised form 19 May 2022; Accepted 6 June 2022

became an imperative (Madhavan et al., 2021). New applications of data-driven health and care solutions –as reported by scholars in the current issue of *Technovation,* have since ranged from benchmarking the costs of various treatment paths for patients (Basile et al., 2022) to facilitating healthcare research (Shaygan and Daim, 2021) to the applications of blockchain technology in areas such as digitalisation of healthcare services (Cerchione et al., 2022; Massaro, 2021) and value creation in healthcare (Spanò et al., 2021). Today, healthcare organisations routinely collect and store sensitive data about individuals, infrastructures and their supply chain, while healthcare workers rely on information systems to use those data resources. Any incident that affects such systems could have a significant impact on the strategy and operation of the healthcare organisation and its stakeholders. Thus, the challenges related to cyber security have been recently considered a threat to global health (Muthuppalaniappan and Stevenson, 2021).

This research has been driven by the need for a better understanding of the digital transformation of the healthcare sector and its potentially disruptive nature for societies. We argue that in the era of knowledge-based health and care services, the digital transformation of the sector is not only essential but also unavoidable. As a process already underway, it must be managed effectively from the perspective of cyber security and resilience to support the sector's antifragility, defined as the ability to return stronger following unexpected events, macro pressures and disruptions (Cobianchi et al., 2020; Aven, 2015; Taleb, 2012). This paper therefore contributes to the special issue on digital transformation in healthcare by studying resilience as a phenomenon that enables the transformation of healthcare systems to meet the changing and increasingly demanding needs of society. Resilience in this research is studied from a security perspective –particularly from a cyber security standpoint, in line with the digital nature of the current transformation efforts in the healthcare sector. The term, as defined, is essential for antifragile transformations as it ensures that breaking-points in the sector's informational infrastructure are not met – an essential precondition to gain from systemic stress and disorder. Our contribution complements the findings by other scholars in the special issue who have argued that the digital transformation of the healthcare sector is still fragmented and in needs of a strategic vision.

In order to achieve its aim, this paper has been structured as follows: the following section provides an overview of the theoretical background of the research. The section first highlights the growing dependence of the healthcare sector on the use of information technologies, and the imperative for its digital transformation. It then focuses on the subject of resilience and the need for security in the digital transformation of the sector, introducing the key concepts driving this research and the hypothesised relationships between these. Section 3 describes the methodology employed to collect and analyse the primary data. The results of the data analysis are presented and discussed in sections 4 and 5 respectively. Finally, the conclusions of the research are presented in sections 6.

2. Theoretical background

2.1. Digital technologies and the healthcare sector

The goals of healthcare systems typically include high quality, efficiency, equity, affordability and accessibility of healthcare. One of the factors influencing the performance of healthcare systems in achieving these goals is technological change, including the ongoing process of digitisation of health services (Ricciardi, 2019).

In recent years –and significantly driven by the coronavirus Covid-19 pandemic, new technologies have had a huge impact not only in the global economy but also in societies. Today, citizens have integrated the use of digital technologies in their daily activity, including work, education, leisure, transportation, communication, etc. In what has been termed a digital transformation of businesses and societies. Vial (2019, p. 118) defines digital transformation as "a process that aims to improve an entity by triggering significant changes to its properties through combinations of information, computing, communication, and connectivity technologies". The global healthcare sector is expected to be part of this revolution (Ruiz Morilla et al., 2017). However, digital transformation is growing at a slow rate in the sector when compared to other industries (Massaro, 2021). Despite the rapid growth in digital technologies, healthcare systems still have a long way to go in order to incorporate this new way of understanding the relationship between the patient, their health and diseases (Birnbaum et al., 2015; Hermes et al., 2020; Kruse et al., 2016). For example, there is a gap in the adoption of digitally enabled tools for diagnosing, providing treatment, and better management of chronic and other conditions; electronic medical records are still not a part of routine care, both from the supply and from the funders side, except for a handful of players (Willie and Nkomo, 2019).

Meanwhile, scholars agree that the success of the healthcare sector in this new context relies on its ability to embrace a process of digitisation effectively, whilst research on digital transformation in healthcare is also considered in its early stages. Ghosh et al. (2022) has argued that recent research efforts tend to focus on the technologies that are being introduced in the healthcare context rather than their analysis from a strategic or structural perspective. Ghosh's views confirm what Kraus et al. (2021) had perceived as the need to build a more holistic perception of digital transformation in healthcare through research on business model transformation.

According to the World Health Organization (2016), digital health is a rapidly expanding medical field with a significant impact on improving the quality and effectiveness of healthcare, lowering the cost of the healthcare system for patients, and on clinical research. Greaves et al. (2018) define digital health as a multidisciplinary domain that aims to enhance the efficiency of monitoring of the patients, diagnosis, management, prevention, rehabilitation, and long-term care delivery. Thus, the applications of digital technologies in the healthcare sector are varied. They may be related to information technologies including e-services targeted mainly to patients, such as making a doctor's appointment; checking waiting lists; accessing appropriate medical care from their homes; sharing information with others with the same health problems; and accessing personalised and qualified health information (Martínez-Caro et al., 2013; Tortorella et al., 2021). In addition, chronic diseases can be better targeted by leveraging prevention strategies through remote monitoring (Liang et al., 2012). But technology applications on healthcare can now go much further as Industry 5.0 emerges as a new phase of technological development. The objective of Industry 5.0 –regarded as the next industrial evolution, is to leverage the creativity of human experts in collaboration with efficient, intelligent and accurate machines in order to obtain resource-efficient and user-preferred manufacturing solutions compared to Industry 4.0 (Martínez-Caro et al., 2020; Maddikunta et al., 2022). In the healthcare sector, these technologies can lead to several innovative applications, overall classified as intelligent healthcare. These include the use of augmented reality as clinical decision support, remote diagnosis, IoT-based health prescription assistant, collaborative robots for complex medical procedures, digital non-invasive medical techniques, or cloud-based real-time prediction of patient status (Aceto et al., 2018; Tortorella et al., 2021).

Numerous scholars have explored the challenges, barriers and opportunities associated to healthcare digitisation. Throughout this process, digital technologies have become an imperative in every attempt to improve healthcare and its management (Martínez-Caro et al., 2018). While the rising cost of medical care has a major impact on the quality of peoples life (even higher in the case of chronic diseases), constant population growth and aging influence healthcare demands and dictate the need for new and more advanced scientific solutions (Chiuchisan et al., 2014). The digital healthcare services are more convenient to the end users because they save their time, require less effort from them, and are more accessible. In short, the use of digital health has been found to lead to cost savings and increased patient satisfaction (Martínez-Caro

et al., 2013). Furthermore, even before the start of the Covid-19 pandemic scholars had concluded that digital health strategies and toolkits provide an opportunity to not only preserve but improve the quality of healthcare. Digitisation was found to make healthcare more cost-effective and even allow healthcare services to be reinvented in order to make them more dynamic and able to adapt to technological changes (Morilla et al., 2017).

However, despite political commitment and significant investment, the adoption rate of digital technologies in healthcare systems in developing countries is lagging (Jung et al., 2020). The introduction of digital technologies implies profound changes in the ways of working and interacting with the environment (Martínez-Caro et al., 2020). To address this challenge, previous research has tried to determine the enablers as well as the barriers to implementing digital technologies in the healthcare sector (Eden et al., 2016; Jung et al., 2021; McGinn et al., 2011; Whittaker et al., 2009; Burton-Jones et al., 2020). These studies have concluded that success of digital health strategies and tools depends on their adoption by end users, that is, physicians and patients, and –indirectly, on the way such strategies are implemented. As Ricciardi (2019) points out, the impacts of digitisation in the healthcare sector can be great, but over-optimism in this regard, for example due to insufficient recognition of the risks (e.g. in terms of security) associated with some types of digitisation, should be avoided.

Despite these challenges, digital health adoption has accelerated since 2020 due to the COVID-19 pandemic. The need to maintain a physical distance significantly facilitated the use of digital technologies by both patients and healthcare professionals, and provided an opportunity to recognise the benefits of digital health (Manteghinejad and Javanmard, 2021). On the other hand, the healthcare sector has become responsible for collecting and storing increasing volumes of highly sensitive and confidential data whilst simultaneously being required to share it amongst medical staff, patients and other organisations (Offner et al., 2020). Thus, the COVID-19 pandemic revealed not only the need for data sharing but also the need for protect it (Fahey and Hino, 2020). Digital health systems were found to be well suited to provide novel solutions to such a public health emergency. For example, robust surveillance systems, wearables for tracking of physiological parameters or interactive chat services for public dissemination of COVID-19 related information were promptly implemented (Kapoor et al., 2020). However, such improvements have only been possible where certain requirements have been met –e.g. reliable data security protocols, in order to ensure the public confidence on digital health technologies (Dubov and Shoptawb, 2020). This has been particularly relevant considering the increased vulnerability of the digital healthcare sector to cyberattacks during and after the COVID-19 pandemic (CISA, 2020).

The boom of digital health has created a lucrative opportunity for fraudsters. Over 1 billion patient health records can be easily accessed on the dark web and millions of additional records are being added daily (Pointer, 2020). According to the Global Digital Health Partnership (GDHP), the cyber security risk is continuously rising for the sector. For example, ransomware attacks on healthcare organisations were predicted to quintuple by 2021 (Morgan, 2020), even before the unprecedented levels of technology use that followed the start of the Covid-19 pandemic. The theft of personal medical data is increasing because these records are worth more than those of any other industry, due to the high value of personal information (Offner et al., 2020). While 91% of hospital administrators considered the security of data as a top focus in 2021, 62% of them felt inadequately trained and/or unprepared to mitigate cyber risks that may impact their hospital. However, only 4–7% of a health systems' budget is invested in their cyber security, compared to about 15% for other sectors such as the financial industry (Morgan, 2020). As a consequence, the healthcare sector is significantly behind other sectors in its ability to secure its critical data (Forcepoint, 2018).

An outage of digital solutions could lead –in the worst case scenario, to a complete quiescence of operations, which would have severe effects on healthcare value (Kaiser et al., 2021). Such instances could also hinder antifragility strategies given that total systemic disruptions/breakdowns exceed the performance thresholds from which systems can safely return with performance gains. Consequently, the impact of a cyberattack may get more severe if service provisioning is highly dependent on digital solutions for healthcare. Cyber security in healthcare is identified as a health security challenge, but there is low awareness in the health sector of the risk (Gordon et al., 2017). Given the importance of the digital health and the potential the digital revolution presents to healthcare globally, there is a need to ensure that cyber security postures are commensurate with the risks that health systems face.

2.2. Digital resilience and healthcare

Healthcare resilience, described by Oyri and Wiig (2019:1373) as "the ability of healthcare systems to succeed under varying conditions", has been a longstanding cause of concern (Carthey et al., 2001; Thomas and Suresh, 2022). Increasingly, the digital transformation of the healthcare sector has raised its susceptibility to cyberattacks, which are recognised as one of the most significant societal and organisational threats, based on likelihood and impact (WEF, 2019). The healthcare sector's adoption of digital technologies has also been further accentuated by dramatic changes in its current landscape (Alao, 2020). Today, healthcare organisations collect and store increasing volumes of sensitive data about individuals, infrastructures, and supply chains. Any incident that affects those systems may have a significant impact on the strategy and operation of the healthcare organisation and its stakeholders (Scantlebury et al., 2021). However, efforts of digitalisation present both a threat and an opportunity for healthcare resilience. Folke et al. (2010) note how lower-level transformational change can develop higher-level resilience. This relationship between resilience and digital transformation is further explored throughout the following from a cyber security lens.

Based on a review of the literature, a series of themes emerge which shape the conceptualisation of digital resilience in healthcare. Firstly, the degree to which healthcare system resilience is addressed as idiosyncratic, i.e. a distinct domain of resilience, varies amongst authors (Offner et al., 2020; Carthey et al., 2001; Blanchet et al., 2017; Jovanovic et al., 2020). In this context, a series of broad characteristics and taxonomies emerge. For instance, across the available literature, distinctions are made between proactive or reactive measures; or, more broadly, anticipatory, and response-oriented dimensions of the concept. Furthermore, the characteristics of resilient systems are described in varying ways, with examples ranging from systemic functions: Absorptive Capacity, Adaptive Capacity and Transformative Capacity (Blanchet et al., 2017), to broader attributes: Preparedness, Robustness, and Recovery/Adaptation (Jovanović et al., 2020). In less abstract terms, output-based descriptions of such systems focus on safety, service continuity and adaptability, community trust, and ownership (Carthey et al., 2001; Blanchet et al., 2017).

Another notable trend relates to the classification of 'resilience' as a boundary term in healthcare, bridging gaps between scientific and public/political discourse (Blanchet et al. 2017). This echoes a broader cross-disciplinary trend, as noted by Manyena (2006). This highlights the importance of conceptual clarity, balancing abstraction and specificity in modelling healthcare resilience. Further drawing parallels to other organisational domains of resilience, the importance of culture and management in supporting healthcare resilience are highlighted in the literature (Carthey et al., 2001; Ree et al., 2021). These findings are reflected in the emerging research design and in the participant selection. Finally, in line with its systemic orientation (Annarelli and Nonino, 2016), digital (i.e. cyber) resilience in healthcare is considered as an expansion of higher-order/institutional resilience. In other words, the exploration of digital resilience should reflect the increasing scope of digitalisation as a primary enabler (and respectively, a vulnerability vector) for healthcare system performance. This positions the scope

digital resilience within the context of the healthcare institution's overall performance, rather than forming a standalone –i.e. meaningfully independent, category of resilience. Furthermore, digital transformation efforts are explored as potentially meaningful in both same-level digital resilience and higher-level institutional resilience.

In light of this, in the current research context, the security layer of the digital transformability of healthcare organisations is modelled as a function of three constructs, adapted from the Blanchet et al. (2017) conceptual framework. The full framework presents four core constructs which yield Transformative, Adaptive and Absorptive Capacity as health systems resilience drivers. These are: *Knowledge* ("the capacity to collect, integrate and analyse […] knowledge and information"); *Uncertainties* ("ability to anticipate and cope with uncertainties and surprises"); *Interdependence* ("engage effectively with and handle multiple […] dynamics and feedbacks"); and *Legitimacy* ("capacity to build or develop legitimate institutions that are socially accepted and contextually adapted") (Blanchet et al., 2017:432). Given the emphasis placed on supporting transformative efforts, respectively resilience in the context of digital transformation from a security perspective, 'Legitimacy' is seen as an inherently higher-order construct. This means that, while the capacity to nurture social and contextual acceptance in building/developing institutions can affect resilience to security incidents, it is seen as an organisational (i.e. holistic) construct without a clear cross-scale, lower-level functional form. As a result, it was omitted from the emerging model. The remaining three constructs were all adapted and explored as resilience drivers primarily from the perspective of security in the context of healthcare digital transformation.

The first construct has been internally coded as 'Knowledge and Resources' (*Knowledge*) and attempts to gauge three core components: the understanding of relevant threats at an executive level; the currency and availability of knowledge covering the integration of cyber security within operations; and, finally, the effectiveness of mechanisms/measures for detecting, mitigating, and responding to cyber incidents. All three elements are aligned with the requirements of security frameworks (i.e., BS 31111:2018, ISO/IEC, 20180:2018, NIST CSF 2018). They also aim to capture a functional perspective of required elements to "collect, integrate and analyse" (Blanchet et al., 2017:432) actionable knowledge in a broader organisational strategic narrative. The dynamic between knowledge and strategy in a cyber security context has also been highlighted by Sallos et al. (2019), as the basis for both proactive and reactive incident response capacity.

The second construct has been internally coded as 'Awareness of Risk' (*Uncertainty*). Subsequently, it aims to gauge the extent to which an organisation understands three indicators of uncertainty: its core digital assets and the uncertainty emerging from their interactions; the organisation's ability to remain operational in the event of (any/undisclosed) critical digital asset loss; and the extent of the organisation's awareness of the COVID-19 effects on their cyber security risk. The first dimension seeks to evaluate the healthcare organisation's ability to cope with one of the core drivers of systemic uncertainty: digital complexity and emerging interactions/interdependencies. The second is adapted to evaluate the organisation's capacity for business continuity in the event of a non-specific (i.e., likelihood agnostic) disruptive digital incident. And, finally, the third dimension seeks to gauge respondent awareness relative to abnormal shifts in risks as a proxy for anticipatory sense-making (Jovanović et al., 2020). Collectively, these dimensions attempt to capture a functional (i.e., adapted to digital/cyber) representation of an organisation's ability to "anticipate and cope with uncertainties and surprise" (Blanchet et al., 2017:432).

The third construct of the model has been internally coded as 'Partnerships & Supply Chain' (*Interdependence*). In order to explore an organisation's ability to respond to and engage in cross-scale dynamics, it attempts to evaluate an organisation's consideration and integration of its broader value chain as a driver of digital resilience. Supply chain attacks have been a consistent and distinct threat for healthcare systems (Hope, 2020; Sheridan, 2018), which highlights the importance of managing interdependence as a dimension of digital resilience within the space. In the context of the model, the construct captures the involvement in cyber security information/intelligence sharing partnerships; the confidence placed in the security measures of vendors, suppliers, and service providers; and the regular auditing of the cyber security of the supply chain. While the first dimension seeks to gauge the extent to which the respondents have access to a cross-scale cyber security sense-making and communication infrastructure, the second and third dimensions seek to capture a subjective qualifier of the level of security of one's supply chain, contrasted/coupled with the existence of a formal basis for such a qualifier.

The final construct of the model has been coded as 'Security in Transformation' and seeks to capture the security layer of the digital transformative capacity of healthcare organisations. It is important to note that it does not seek to represent security systems in their respective transformation; rather, it models key elements of security which could hinder and, respectively, enable resilience throughout healthcare digital transformation efforts. Given the need for reduced abstraction and contextual adaptation, the construct has been simplified around three elements: an anticipatory element (proactive), a response-oriented element (reactive), and a governance oriented navigational/sense-making element. The first element seeks to evaluate planning effectiveness for securing the healthcare organisation's data. Such planning is an essential element of defining and controlling the stability landscape of the institution around its defined thresholds (Folke et al., 2010). The second element seeks to capture the organisation's availability of communication/signalling mechanisms in the event of a cyber incident. Given the sectoral availability of and reliance on support bodies, effective and timely communication with relevant stakeholders can determine the scope of disruption following an incident. From a systemic perspective, this also underpins the ability of cross-hierarchy communication and response, which can alter institutional pressures, directives, resources, and support. Finally, in line with the importance of effective management and governance as both drivers of digital transformation and effective incident response/recovery in the context of healthcare resilience (Ree et al., 2021), the third construct seeks to capture the existence of ongoing cyber security training and simulations for the management board. Given the board's role in directing and supporting transformational change, such exercises can assist executives' situational awareness and sense-making, the development of shared representational models regarding the nature of novel (often changing) threats, and their ability to evaluate the adequacy of existing response strategies in the context of cyber threats (Larcker et al., 2017).

It should also be noted that, while not explicitly within the scope of the model, healthcare antifragility strategies can be mapped to and supported by the emerging model. Cobianchi et al. (2020:298) suggest a range of such strategies, in the context of the COVID-19 pandemic. These include, Knowledge Sharing, Networking and Technological Transfer strategies, which map to the Interdependence construct highlighted above and leverage collaboration, knowledge exchanges, partnerships, and convergent efforts amongst stakeholder networks. They also include Barbell Strategies, which aim to reduce the exposure to negative effects through a "balanced portfolio". These are reflected in the Uncertainty construct, which describes the institution's awareness of unexpected events, such as the loss of key digital assets, as well as its ability to adapt to and cope with such outcomes. Finally, Hormesis Strategies, exemplified through Innovative Training/Gaming strategies, are assessed in the final construct –Security in Transformation– which contains questions about the participation of executives in simulation exercises such as Cyber Wargames. This overlap highlights the synergy between healthcare resilience, as defined and modelled, and the institutional potential for antifragility in the context of digital transformations.

2.3. Hypotheses development

The emerging model of cyber security as a driver of resilience in the

digital transformation of healthcare systems has been used to generate six hypotheses to be empirically tested.

Hypothesis 1. An organisation's understanding of uncertainty in the digital domain is positively correlated with its perception of the interdependence between its digital resilience and that of its value chain. (Uncertainty —> Interdependence).

In order to overcome uncertainty, the first hypothesis explores the relationship between an organisation's Awareness of Risk/Uncertainty and the level of its cross-level Interdependence and Supply Chain integration. Based on the construct definitions, healthcare systems aware of the risks and uncertainty they face from a security perspective are inferred to be more likely to understand, nurture and control said risks across scales, stakeholders, and supply chains. In this context, cross-level has been defined as the interdependency and interaction (e.g. in the form of cyber security knowledge flows) between organisations and organisational units within the health and care system (Song et al., 1997).

Hypothesis 2. An organisation's understanding of uncertainty in the digital domain is positively correlated with its knowledge of the cyber security problem and investments in its solution (Uncertainty —> Knowledge).

Organisations lacking basic detection, mitigation and response mechanisms, an executive-level understanding of threats, or an understanding of how cyber security affects their operations are unlikely to be sufficiently aware of the risks and uncertainty they face. Respectively, organisations which lack an awareness of domain-specific risks and uncertainty, are unlikely to develop the necessary knowledge and capabilities required for effective defence. Further, a number of studies suggest that uncertainty promotes knowledge transfer between organisations within the same sector and those in their supply chain (Tsang, 2008; Yildiz and Fey, 2010). This has the potential to lead to the creation of knowledge structures that relate to the digital domain (Cegarra-Navarro et al., 2016), which supports the hypothesised interrelation between an organisation's Awareness of Risk/Uncertainty and its relevant Knowledge base.

Hypothesis 3. An organisation's understanding of uncertainty in the digital domain is positively correlated with the security of its digital transformative capacity (Uncertainty —> Security in Transformation).

The third hypothesis posits a relationship between an organisation's Awareness of Risk/Uncertainty and its Security in Transformation –which represents the layer of security underpinning the digital transformative capacity and resilience of healthcare systems. The resulting hypothesis gauges one of the two epistemic layers (the other being evaluated in H6) underpinning Security in Transformation performance. This hypothesis gains relevance in a context where the uncertainty generated by the COVID-19 pandemic –which extends to the digital domain, has led many organisations to step into their digital transformation without necessarily investing in the security challenges associated with it (Butt, 2020).

Hypothesis 4. An organisation's perception of the interdependence between its digital resilience and that of its value chain is positively correlated with its knowledge of the cyber security problem and investments in its solution. (Interdependence —> Knowledge).

The fourth hypothesis evaluates the extent to which an organisation's security knowledge and primary sense-making/control mechanisms are driven by its awareness, communication, and control across the supply chain (Melnic & Botez, 2014; Wang & Hu, 2020). This is particularly relevant in instances where the targeted healthcare entity functions in a higher-complexity healthcare system where security input, feedback and directives are driven by another entity. It also covers instances where, because of supply chain audits and incidents across levels of control, further knowledge is acquired, or further essential security mechanisms are developed.

Hypothesis 5. An organisation's perception of the interdependence between its digital resilience and that of its value chain is positively correlated with the security of its digital transformative capacity *(*Interdependence —> Security in Transformation*)*. Corresponding to the Leavitt's model (1965), the fifth hypothesis posits a relationship between an organisation's (or potentially the healthcare system's) ability to respond to cross-scale dynamics, coded as Interdependence, and its Security in Transformation. This is in line with empirical studies which have suggested that knowledge generated by establishing interdependence and value-based convergence between organisations and their supply chain can be an effective tool to tackle cyber security issues (Bahl and Wali, 2014; Neal and Ilsever, 2016).

Hypothesis 6. An organisation's knowledge of the cyber security problem and investments in its solution is positively correlated with the security of its digital transformative capacity. (Knowledge —> Security in Transformation)

Alongside Hypothesis 3, the sixth hypothesis explores the effect of the second epistemic construct, Knowledge, on Security in Transformation. Based on the theoretical background, there is an inferred relationship between the two constructs, as foundational cyber security knowledge is likely to be a precursor to the digital transformative capacity and resilience of healthcare systems. Furthermore, in order to effectively deal with the cyber security challenges related to its digital transformation, an organisation must possess superior knowledge of the digital domain (Bahl and Wali, 2014; Neal and Ilsever, 2016). Such a knowledge takes the form of cyber security competencies at the tactical and operational levels, required to support a cyber security framework and for the deployment of effective cyber security communication and joint strategies (Dahbur et al., 2017).

Based on the above, the path relationships between variables are hypothesised as shown in Fig. 1.

3. Method

3.1. Sample description and data collection

Data were collected at the peak of the COVID-19 pandemic from owners and C-level executives from critical infrastructure sectors in the United Kingdom. The purpose of the study was informing policy making in the domains of digital transformation and digital resilience. Out of the 400 valid responses to the telephone interviews, 99 belonged to executive board members from organisations in the healthcare sector.

From the 99 responses used in this study, 53 confirmed that their organisations have a budget allocated to cyber security, while 33 respondents did not have one. The majority of the organisations that did not have a budget allocated to cyber security have less than 99 employees (50.5%). Table 1 illustrates the demographical data of the respondents.

Potential bias from non-response was addressed by comparing the 99 responses from the health sector and the 301 responses from the other

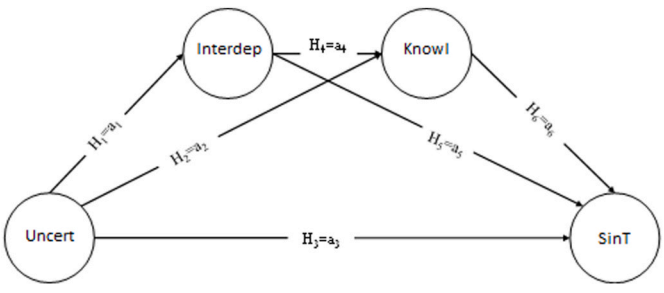

Fig. 1. Conceptual framework.

Table 1
Demographic characteristics of respondents.

Demographics (N = 99)	Frequency	%	
Company size	Company size: <99	50	50,5%
	Company size: 100 - 499	29	29,3%
	Company size: 500+	20	20,2%
A budget allocated to cyber security	Yes	53	53,54
	Not	33	33,33
	Don't know	13	13,13
Job title	Owner /Partner	30	30,30%
	President /Chairman /CEO /General Manager	19	19,19%
	CFO - Chief Financial Officer /Finance Director	1	1,01%
	COO - Chief Operating Officer	3	3,03%
	CIO - Chief Information /Technology Officer	14	14,14%
	CKO - Chief Knowledge Officer	4	4,04%
	Another C-Suite title /Chief Officer	1	1,01%
	Executive /Senior Vice President	2	2,02%
	Managing Director	12	12,12%
	Head of Department	10	10,10%
	Departmental Director	1	1,01%
	Other Director	2	2,02%

sectors in terms of knowledge, uncertainty, interdependence, and security in transformation. The independent sample *t*-test revealed no significant difference between the two groups (p = 0.492, p = 0.271, p = 0.224 and p = 0.789, respectively). Therefore, non-response bias should not be a problem in this study (Armstrong and Overton, 1977). To minimize data bias, we check for common method bias through the Harman's single factor test (Podsakoff et al., 2003; Podsakoff and Organ, 1986). Results of a post-hoc Harman's single-factor test showed that the unrotated factor solution of the one-factor model accounted for less than 50% of the variance (41.21%), indicating no substantial common method bias. This study has also used a confirmatory factor-analytic approach to the Harman one-factor test as a way of testing for the presence of bias (Podsakoff et al., 2003). A worse fit for the one-factor model would suggest that common method variance does not pose a serious threat. The one-factor model yielded a Satorra-Bentler $\chi^2_{(54)} = 144.34$; $\chi^2/d.f = 2.67$ (compared with the measurement model, which yielded a Satorra-Bentler $\chi^2_{(48)} = 70.54$; $\chi^2/d.f = 1.46$). This means that the fit is considerably worse for the one-dimensional model than for the measurement model, suggesting no substantial common method bias (Armstrong and Overton, 1977).

3.2. Measures

All constructs were self-reported and measured using a liker scale of 5-points rating (1 = "completely disagree" to 5 "completely agree" (Please see Appendix A for a summary of the operationalised items).

- Knowledge and Resources: Three items assessed the importance of knowledge of the cyber security problem and investments in its solution. These items measure the understanding of the threats and the effectiveness of measures in place for the detection, mitigation, and response to cyber security incidents. One item also measures the extent to which cyber security is embedded in operations. Sources: Blanchet et al. (2017:432); BS 31111:2018; ISO/IEC, 20180:2018; NIST CSF (2018); Sallos et al. (2019).
- Awareness of Risk: Three items measured the organisation's understanding of uncertainty in the digital domain. These focused on the extent to which organisations were able to protect their digital assets and services, and the interdependencies between these. Sources: Jovanovic et al. (2020); Blanchet et al. (2017:432)
- Partnerships & Supply Chain: The organisation's perception of the interdependence between its digital resilience and that of its value chain was assessed with a 3-item scale. These items focused on the perception of responders regarding the information offered by supply chain members regarding cyber security measures, cyber security compliance and the sharing of cyber security information. Sources: Hope (2020); Sheridan (2018).
- Security in Transformation: The security of an organisation's digital transformative capacity was assessed with a 3-item scale. These items focused on the perception of responders regarding the presence of efficient mechanisms in place for external communication, an effective plan in place to keep data secure and participation in cyber security exercises. Sources: Folke et al. (2010); Ree et al. (2021); Larcker et al. (2017).

3.3. Data analysis

SmartPLS 3.3.3 has been the software package used for data analysis (Ringle et al., 2005). Following Cepeda-Carrion et al. (2019) classification of PLS-SEM and its purposes, the present study is causal, which involves testing hypotheses in a specific model and maximising the explained variance of the dependent, considering the fit indices in the model. Since endogeneity could be a problem, a two-step procedure has been established to evaluate it in our model (Hair et al., 2019): (1) assessment of the measurement model and (2) assessment of the structural model. In order to evaluate the significance of fit indices, path coefficients, weights, and loadings of each composite's indicators we have used the bootstrap procedure (Chin, 1998). Regarding the structural model, considering the confirmatory nature of our PLS-SEM analysis, the fit indices were calculated for the saturated model from our proposed model (Henseler and Schuberth, 2020). The results of the data analysis are presented in the following section.

4. Results

4.1. Measurement model

The measurement model was assessed by following the approach by Hair et al. (2019). Results exhibit that it meets all the commonly designated measures of reliability and validity. First, individual reliability is sufficient because all standardised loadings are larger than 0.7 for all constructs. Second, all measures of composite reliability are larger than 0.8. The values for average variance extracted (AVE) exceed the threshold of 0.5 for convergent validity (Table 2). Finally, a full collinearity test based on variance inflation factors (VIFs) was carried out. According to Kock and Lynn (2012), when a VIF achieves a value greater than 3.3, there would be an indication of collinearity problems. This would warn if a model may be contaminated by common-method variance (CMV). The present model, with a maximum VIF of 2.096 may be considered free of CMV problems.

Table 2
Measurement model.

Construct	Indicator	VIF [a]	Loadings	Composite reliability	AVE [b]
Knowledge and resources	Knowl1	1.421	0.732	0.836	0.631
	Knowl2	1.656	0.869		
	Knowl3	1.306	0.774		
Awareness of risk	Uncert1	1.436	0.822	0.827	0.615
	Uncert2	1.357	0.789		
	Uncert3	1.254	0.739		
Partnerships and supply chain	Interdep1	1.821	0.834	0.857	0.667
	Interdep2	1.297	0.721		
	Interdep3	2.096	0.887		
Security in Transformation	SinT1	1.513	0.821	0.845	0.645
	SinT2	1.428	0.818		
	SinT3	1.367	0.769		

Notes.
[a] VIF: Variance Inflation Factor.
[b] AVE: Average Variance Extracted.

As shown in Table 3, all the constructs show discriminant validity since all HTMT indices are below 0.90 (Henseler et al., 2015). In addition, each construct related more strongly to its own measures than to others (Fornell and Larcker, 1981). Therefore, there is evidence of discriminant validity (Henseler et al., 2015).

4.2. Structural model

As shown Table 4, all fit indices for the saturated model meet the requirements to confirm the proposed measurement model. Based on Benitez et al. (2020), the fit statistics for the model indicate a reasonable data fit. The standardised root mean square residual (SRMR) value of the measurement model was 0.076 and all discrepancies were below the 99%-quantile of the bootstrap discrepancies (Hi99), which suggests very good measurement model fit (Henseler et al., 2016). Therefore, there is a good adjustment between the empirical data matrix and the theoretical model matrix (Henseler, 2018).

Following Hair et al. (2019), we assessed the sign, magnitude, and significance of path coefficients which are the most important result of the structural model. Likewise, the aim of PLS-SEM algorithm maximizes the explained variance of the dependent variables represented by determination coefficient (i.e., R^2). As Hair et al. (2019) argue, the use of bootstrapping (5000 resamples) produces confident intervals to assess the statistical significance of the path coefficients. Thus, the consideration of bootstrap percentile confidence intervals provides greater assurance than merely relying on null hypothesis significance testing. We also report the effect size f^2 which shows the change in R^2 if a specified construct is omitted from the model. A guideline of 0.02, 0.15, and 0.35 represent respectively, small, medium, and large effects (Cohen, 1977). As Table 5 shows, this study not only uses parametric test as t-value but also uses a non-parametric test as percentile confidence interval. If the 95% CI surrounding the standardised direct effect did not include 0, we deemed the direct effect significant. As Table 5 shows, the bootstrap intervals do not contain the zero value. Based on this analysis, the results provided full support for the hypotheses identified in Fig. 1.

5. Discussion

Developments in digital technologies and their applications are changing the dynamics of the environment where health and care systems operate. There is consensus in the literature that success of the healthcare sector in this new context relies on its ability to embrace a process of digitisation. However, digitisation of health and care systems means more than just adoption of the digital technologies for improved operations. Healthcare digitisation implies a transformation of the sector so that it continues to meet the changing and increasingly demanding needs of society. Such digital transformation of the sector therefore becomes a complex process which raises new vulnerabilities in healthcare organisations and their stakeholders –from individuals to organisations to its global supply chain.

As the healthcare sector engages in its digital transformation, its stakeholders face a new type of risk related to digital healthcare assets and services. Risks derived from digital incidents are not only disruptive but difficult to predict or avoid by the healthcare organisation. Such risks could have a direct impact on the physical domain, from the safety of individuals to the operation of the overall system. Thus, the resilience of the healthcare sector today relies on a combination of its transformative capacity and its cyber security.

Our results indicate that the defined drivers of security in healthcare organisations' digital transformation are closely associated with key elements of sectoral cyber resilience. In other words, both the success and sustainability of digital transformation efforts are likely to be affected by the healthcare systems' performance in these elements of resilience. The consistent relationships between the constructs indicate that organisations with low performance in Knowledge, Uncertainty and Interdependence are also likely to perform poorly in Security in Transformation. Furthermore, these results support the theoretical inference that, to achieve the levels of resilience required for sustainable digital transformation, healthcare organisation must develop their transformative, adaptive, and absorptive capacities in the context of cyber security.

As discussed earlier in this paper, the construct Security in Transformation represents key elements of security that could affect resilience throughout the digital transformation efforts of the healthcare sector. Those elements are derived from anticipatory (i.e. proactive), response-oriented (i.e. reactive), and governance-oriented principles of organisational theory. Thus, in terms of hypotheses H3, H5 and H6 our results suggest that the security layer of the digital transformative capacity of healthcare organisations is directly influenced by three key factors, respectively:

1. The extent to which an organisation understands key indicators of uncertainty, including its core digital assets and the uncertainty emerging from their interactions; the organisation's ability to remain operational in the event of critical digital asset loss; and the extent of the organisation's awareness of the COVID-19 effects on their cyber security risk (H3). This is in line with the understanding of Uncertainties by Blanchet et al. (2017:432) when describing the drivers of health systems resilience. Our research expands this theory by exploring the concept in the contextual basis of the digital domain and a crisis such as the COVID-19 pandemic, both of which have directly affected the healthcare sector.
2. The organisation's involvement in cyber security information/intelligence sharing partnerships; its confidence in the security measures of vendors, suppliers, and service providers; and the regular auditing of the cyber security of the supply chain (H5). This adds to the knowledge-based nature of the cyber security problem by Sallos et al. (2019) and their vision of cyber security governance as a multifaceted construct which benefits from a knowledge-centric narrative. Cyber security knowledge may refer, for example, to what cyber security-related information becomes once it has been collected, evaluated, structured and eventually shared across various

Table 3
Discriminant validity (Fornell and Larcker[a]'s and HTMT[b]).

Construct	Uncert	SinT	Knowl	Interdep
1. Uncert	0.784	0.800	0.735	0.553
2. SinT	0.569	0.803	0.819	0.814
3. Knowl	0.504	0.597	0.794	0.646
4. Interdep	0.394	0.596	0.486	0.817

Notes.
Uncert → Uncertainty; Interdep → Interdependence; Knowl → Knowledge; SinT → Security in Transformation.
[a] Diagonal values (square root of AVE are in bold) should be higher than off-diagonal correlations shown below the diagonal line.
[b] Heterotrait-Monotrait Ratio of Correlations (HTMT) thresholds are shown above the diagonal line.

Table 4
Global goodness of fit, confirmatory composite analysis, and bootstrap-based 95% and 99% quantiles.

	Estimated Model	Hi95	Hi99	Saturated Model	Hi95	Hi99
SRMR	0.071	0.075	0.088	0.071	0.074	0.081
d_{ULS}	0.395	0.444	0.606	0.395	0.422	0.508
d_G	0.217	0.260	0.298	0.217	0.263	0.331

Notes.
The figure in bold indicates the level of compliance with the index of adjustment. SRMR: Standardised Root Mean Square Residual, d_{ULS}: Unweighted Least Squares Discrepancy, d_G: Geodesic Discrepancy.

Table 5
Structural model.

Confidence intervals						
Hypotheses	Path coefficient	5% CI_{lo}	95% CI_{hi}	Significance (p-value)	Cohen's f-square	R^2
H_1: Uncert→Interdep	$a_1 = 0.394$	0.139	0.670	0.004	0.193	0.155
H_2: Uncert→Knowl	$a_2 = 0.370$	0.150	0.595	0.001	0.101	0.352
H_3: Uncert→SinT	$a_3 = 0.291$	0.030	0.550	0.030	0.132	0.540
H_4: Interdep → Knowl	$a_4 = 0.341$	0.130	0.552	0.001	0.092	0.352
H_5: Interdep →SinT	$a_5 = 0.343$	0.075	0.668	0.026	0.176	0.540
H_6: Knowl →SinT	$a_6 = 0.284$	0.059	0.494	0.011	0.159	0.540

Notes.
(based on t(4999), two-tailed test). t(0.05, 4999) = 1.960; t(0.01, 4999) = 2.577; t(0.001, 4999) = 3.292.
Uncert → Uncertainty; Interdep → Interdependence; Knowl → Knowledge; SinT → Security in Transformation.

stakeholders in both academic and industry contexts (Barnum, 2012).

3. The organisation's understanding of relevant threats at an executive level; the currency and availability of knowledge covering the integration of cyber security within operations; and the effectiveness of mechanisms/measures for detecting, mitigating, and responding to cyber incidents (H6). This adds an 'actionable' dimension to cyber security knowledge. In doing so, it emphasises the importance of the dynamic between knowledge and strategy in a cyber security context, highlighted by Sallos et al. (2019) as the basis for both proactive and reactive incident response capacity.

In addition to its direct effect on the security layer of the digital transformative capacity of healthcare organisations, the Uncertainty construct was found to have a significant effect on both Interdependence (H1) and Knowledge (H2).

In terms of hypothesis H1, our findings suggest that the extent to which an organisation understands key indicators of uncertainty appears to have a positive impact on its consideration and integration of its broader value chain as a driver of digital resilience. From a governance perspective, it is plausible to assume that a better understanding of the core digital assets and the uncertainty and risks emerging from these –particularly those potentially affecting the operational performance, drives the organisation towards engagement in cyber security intelligence sharing partnerships with vendors, suppliers, and service providers. This leads, in turn, to an increased confidence in the security of its supply chain. Given the healthcare sector's vulnerability to supply chain attacks, such engagement is essential. While the two constructs at the basis of H1 are distinct, their relationship could also be explained in terms of a capability progression. Knowledge, as defined, involves an awareness of irreducible interdependencies. Once organisations develop a sufficient understanding of the threats/risks faced internally, they are likely to expand the scope of their efforts towards the next driver of vulnerability – their extended enterprise.

As for hypothesis H2, our results show that the extent to which an organisation understands key indicators of uncertainty in the cyber security domain has a direct effect on its cyber security knowledge (e.g. knowledge of relevant threats at an executive level, of the integration of cyber security within operations and of mechanisms/measures for detecting, mitigating, and responding to cyber incidents). Similarly, an organisation's consideration and integration of its broader value chain as a driver of digital resilience was found to have a direct effect on the cyber security knowledge base of the organisation, particularly that of its management board. Again, despite the strength of the relationship between Knowledge and Uncertainty, it is unclear at a conceptual level if it follows a sequential logic (where Uncertainty predates Knowledge). The results indicate that the two constructs are highly interdependent, with likely feedback loops driving their interaction across levels. For example, a high degree of Uncertainty awareness driven by an understanding of interdependencies between core digital assets is likely to be required in order to develop effective mechanisms for detection, mitigation, and response to cyber threats –an element of Knowledge. However, the understanding of the integration of cyber security in operations (Knowledge) is likely to be a prerequisite for establishing robustness (i.e. ability to remain operational in the event of access/availability disruptions for key digital assets) – an element of the Uncertainty construct.

In addition to the findings derived from the study of hypotheses H1 to H6, our analysis suggests that the relationship between uncertainty and digital transformation in the healthcare sector is potentially a bidirectional one, particularly when uncertainty is considered in its broader sense. This research has found that digitisation efforts drive uncertainties such as those derived from the spread of cyberattacks or fake news. However, we also argue that the uncertainties caused by crises such as the recent COVID-19 pandemic facilitate the digitisation of healthcare products and services, and the emergence and adoption of technoinnovations such as telemedicine –studied by Drago et al. (2021). Further, in the face of digital resilience, the healthcare sector is expected to facilitate the relationship uncertainty ↔ digitisation in both directions. Understanding the situations of uncertainty caused in both directions and knowing how to deal with them in the best possible way, provide security in the digital transformation. However, this requires the presence in the organisation of not only internal knowledge but also knowledge that comes from collaborations within the healthcare sector and with its global value chain.

6. Conclusion

The digital transformation of the healthcare sector is an essential development as societies move into a post-industrial, knowledge-based economy defined by radical innovations in the information technologies domain. The adoption of the latest technologies and their applications in the health and care ecosystem must be managed effectively from the perspective of cyber security and resilience to support sectoral development and, ultimately, its antifragility. However, there is still a limited understanding of the key concepts that must define the strategic vision of a resilient and sustainable digital transformation of healthcare.

This research has studied three core constructs that contribute to the required transformative, adaptive and absorptive capacities for healthcare systems cyber/digital resilience. These are Knowledge and Resources, Awareness of Risk, and Partnerships & Supply Chain. The analysis of the perspective from C-level executives from the healthcare sector in the United Kingdom indicates that all three defined constructs are meaningful for the required Security in Transformation of the sector. Prescriptively, this means that a balanced base of cyber security knowledge development, uncertainty management, and consideration for the sector's high levels of systemic and organisational interdependence are all essential, as more healthcare systems are undergoing digital transformations. Respectively, the absence of such a base is likely to indicate poor performance across the measures, given the interdependencies found between them. Poorly performing organisations are likely to face a significant degree of vulnerability/risk, while likely

being unaware of it. Such instances present a paradoxical problem as sufficient domain-level knowledge, an understanding of the uncertainty faced, and the risks and opportunities presented throughout the extended enterprise are seemingly co-evolving necessities for an effective self-diagnosis of the digitally transformative capacity of the organisation. In other words, poor performers in these aspects are unlikely to be equipped to effectively gauge the scope of the risk faced through emerging digital transformations –a prerequisite for justifying necessary further investments and development.

6.1. Implications for theory and management practice

Two main practical implications can be drawn from our findings. First, the necessity for oversight bodies to initiate audits of the digital absorptive, adaptive and transformative capacities of healthcare organisations. Such audits can indicate inadequate organisational performance as a way to overcome the aforementioned paradox between knowledge of the digital domain, understanding of the uncertainties that characterise it, and risks and opportunities presented throughout the extended enterprise. As healthcare organisations understand these three concepts as co-evolving necessities for an effective self-diagnosis of their digitally transformative capacity, investments in cyber resilience will increase, paving the way to the sustainable transformation of the sector at systemic level.

Secondly, prudent governance of healthcare systems is of upmost importance as its reliance in digital technologies increase. Through a sustainable integration of cyber security into the management strategy of the healthcare organisation, assumptions of adequate performance must be thoroughly and regularly tested at a board-level. Such regular testing of cyber security performance and the sharing of its results across the sector must lead to actions at systemic levels.

Our findings have two key implications for scholars in different domains related to both healthcare and digital security. The first of this is the need to approach digital resilience as a knowledge problem within and beyond the healthcare sector. As technologies and their applications transform business and societies, there is a growing body of evidence that suggests that the combination of digital technologies and digital competencies is the critical success factors for the sustainable and resilient digital transformation of the healthcare sector. By studying the interdependence between digital transformation and areas such as digital capacity building, digital capabilities and digital capital, scholars from different domains will be contributing to current and future efforts to transition to a knowledge economy.

Additionally, the research emphasises the need to raise awareness across the management board of the cyber/digital resilience problem, the uncertainties associated to it and the importance of managing their interdependence from all other stakeholders in this space.

6.2. Limitations and future research avenues

In addition to the above avenues for future research, this research encourages other scholars to study the subjects of digital resilience and digital transformation from the perspective of other stakeholders within the healthcare sector. Our research has captured the views of C-level executives on these concepts and their relationships. The domain would benefit from the analysis of the problem from the perspective of the individuals and teams responsible for the operational performance of the organisation, the sector and its supply chain. Such a study would complement our findings to bring a more comprehensive perspective of the cyber security challenges currently faced by the healthcare sector, which have the potential to affect its resilience and therefore the sustainability of its digital transformation efforts.

Finally, this study encourages the healthcare and cyber security research and practice communities to further explore the potentially bi-directional nature of the relationship between the concepts of uncertainty and digital transformation, and its implications for theory and practice.

Acknowledgement:

This research has been conducted with funding from the Centre for Business in Society, Coventry University, United Kingdom, for the study of the factors driving digital resilience in critical infrastructure sectors.

The authors also thank the two anonymous reviewers as well as the guest editors of the special issue for their useful comments and suggestions to earlier versions of this article.

Appendix A. Questionnaire Items

Knowledge and Resources (*Knowledge*)
Knowl1. Our management board has a sufficient understanding of the threats digital technologies currently pose to our organisation. [*situationalAwareness*]
Knowl2. Our organisation has effective measures in place for the detection, mitigation, and response to cyber security incidents. [*incidentManagement*]
Knowl3. Our organisation regularly measures the extent to which cyber security is embedded in our operations. [*cyberRiskManagement*]
Sources: Blanchet et al. (2017:432); BS 31111:2018; ISO/IEC, 20180:2018; NIST CSF (2018); Sallos et al. (2019)
Awareness of Risk (Uncertainty)
Uncert1. Our organisation has a sufficient understanding of our key digital assets and services, and the interdependencies between them.
Uncert2. Our organisation has effective measures in place to remain operational even if we lose access to a critical digital asset (e.g., a particular database or application)
Uncert3. The current COVID-19 crisis has increased the cyber security risk for our organisation.
Sources: Jovanovic *et al.* (2020); Blanchet et al. (2017:432)
Partnerships & Supply Chain (Interdependence)
Interdep1. Our organisation is involved in a programme or external partnership for the sharing of cyber security information, expert.
Interdep2. Our organisation has confidence in the cyber security measures our vendors, suppliers and service providers have in place.
Interdep3. Our organisation regularly audits the cyber security compliance of our supply chain.
Sources: Hope (2020); Sheridan (2018)
Security in Transformation
SinT1. In the event of a cyber security incident, our organisation has efficient mechanisms in place for external communication.
SinT2. Our organisation has an effective plan in place to keep our data secure.
SinT3. Our management board regularly participate in cyber security exercises such as table-top and cyber wargames.

Sources: Folke et al. (2010); Ree et al. (2021); Larcker et al. (2017).

References

Aceto, G., Persico, V., Pescapé, A., 2018. The role of Information and Communication Technologies in healthcare: taxonomies, perspectives, and challenges. J. Netw. Comput. Appl. 107, 125–154.

Alao, B., 2020. Managing Digital Transformation Strategies for Business Survival amid Pandemics 2 (8), 626–634. https://doi.org/10.35629/5252-0208626634.

Annarelli, A., Nonino, F., 2016. Strategic and Operational Management of Organizational Resilience: Current State of Research and Future Directions, vol. 62. Elsevier, Omega (United Kingdom), pp. 1–18. https://doi.org/10.1016/j.omega.2015.08.004.

Armstrong, J.S., Overton, T.S., 1977. Estimating nonresponse bias in mail surveys. J. Market. Res. 14 (3), 396. https://doi.org/10.2307/3150783.

Aven, T., 2015. The concept of antifragility and its implications for the practice of risk analysis. Risk Anal. 35 (3), 476–483.

Bahl, S., Wali, O.P., 2014. Perceived significance of information security governance to predict the information security service quality in software service industry: an empirical analysis. Inf. Manag. Comput. Secur. 22 (1), 2–23. https://doi.org/10.1108/IMCS-01-2013-0002.

Barnum, S., 2012. Standardizing cyber threat intelligence information with the structured threat information expression (stix). Mitre Corporation 11, 1–22.

Basile, L.J., Carbonara, N., Pellegrino, R., Panniello, U., 2022. Business intelligence in the healthcare industry: the utilization of a data-driven approach to support clinical decision making. Technovation, 102482. https://doi.org/10.1016/j.technovation.2022.102482.

Benitez, J., Henseler, J., Castillo, A., Schuberth, F., 2020. How to perform and report an impactful analysis using partial least squares: guidelines for confirmatory and explanatory IS research. Inf. Manag. 57 (2), 103168.

Birnbaum, F., Lewis, D.M., Rosen, R., Ranney, M.L., 2015. Patient engagement and the design of digital health. Acad. Emerg. Med.: Official Journal of the Society for Academic Emergency Medicine 22 (6), 754.

Blanchet, K., Nam, S.L., Ramalingam, B., Pozo-Martin, F., 2017. Governance and capacity to manage resilience of health systems: towards a new conceptual framework. Int. J. Health Pol. Manag. 6 (8), 431–435. https://doi.org/10.15171/ijhpm.2017.36.

Burton-Jones, A., Akhlaghpour, S., Ayre, S., Barde, P., Staib, A., Sullivan, C., 2020. Changing the conversation on evaluating digital transformation in healthcare: insights from an institutional analysis. Inf. Organ. 30 (1), 100255 https://doi.org/10.1016/j.infoandorg.2019.100255.

Butt, J., 2020. A conceptual framework to support digital transformation in manufacturing using an integrated business process management approach. Design 4 (3), 1–39. https://doi.org/10.3390/designs4030017.

Carthey, J., De Leval, M.R., Reason, J.T., 2001. Institutional resilience in healthcare systems. Quality in Health Care 10 (1), 29–32. https://doi.org/10.1136/qhc.10.1.29.

Cegarra-Navarro, J.G., Wensley, A., Garcia-Perez, A., Sotos-Villarejo, A., 2016. Linking peripheral vision with relational capital through knowledge structures. J. Intellect. Cap. 17 (4), 714–733. https://doi.org/10.1108/JIC-04-2016-0041.

Cepeda-Carrion, G., Cegarra-Navarro, J.G., Cillo, V., 2019. Tips to use partial least squares structural equation modelling (PLS-SEM) in knowledge management. J. Knowl. Manag. 23 (1), 67–89 https://doi.org/https://doi.org/10.1108/JKM-05-2018-0322.

Cerchione, R., Centobelli, P., Riccio, E., Abbate, S., Oropallo, E., 2022. Blockchain's coming to hospital to digitalize healthcare services: designing a distributed electronic health record ecosystem. Technovation, 102480. https://doi.org/10.1016/j.technovation.2022.102480.

Chin, W., 1998. The partial least squares approach to structural equation modeling. Modern Methods for Business Research 295 (2), 295–336. https://doi.org/10.1016/j.aap.2008.12.010.

Chiuchisan, I., Costin, H., Geman, O., 2014. Adopting the Internet of Things technologies in health care systems. International Conference and Exposition on Electrical and Power Engineering (EPE) 532–535. https://doi.org/10.1109/ICEPE.2014.6969965.

Cisa, 2020. Alert (AA20–099A) - COVID-19 Exploited by Malicious Cyber Actors.

Cobianchi, L., Dal Mas, F., Peloso, A., Pugliese, L., Massaro, M., Bagnoli, C., Angelos, P., 2020. Planning the full recovery phase: an antifragile perspective on surgery after COVID-19. Ann. Surg. 272 (6), e296–e299. https://doi.org/10.1097/SLA.0000000000004489.

Cohen, J., 1977. F tests on means in the analysis of variance and covariance. In: for the Cohen, J.B.T.-S.P.A.B.S. (Ed.), Statistical Power Analysis for the Behavioral Sciences. Academic Press, pp. 273–406. https://doi.org/10.1016/b978-0-12-179060-8.50013-x.

Cohen, B., Amorós, J.E., Lundy, L., 2017. The generative potential of emerging technology to support startups and new ecosystems. Bus. Horiz. 60 (6), 741–745.

Dahbur, K., Bashabsheh, Z., Bashabsheh, D., 2017. Assessment of security awareness: a qualitative and quantitative study. International Management Review 13 (1), 37.

Drago, C., Gatto, A., Ruggeri, M., 2021. Telemedicine as Technoinnovation to Tackle COVID-19: A Bibliometric Analysis. Technovation, 102417. https://doi.org/10.1016/j.technovation.2021.102417.

Dubov, A., Shoptawb, S., 2020. The value and ethics of using technology to contain the COVID-19 epidemic. Am. J. Bioeth. 20 (7), W7–W11.

Eden, K.B., Totten, A.M., Kassakian, S.Z., Gorman, P.N., McDonagh, M.S., Devine, B., Pappas, M., Daeges, M., Woods, S., Hersh, W.R., 2016. Barriers and facilitators to exchanging health information: a systematic review. Int. J. Med. Inf. 88, 44–51.

Fahey, R.A., Hino, A., 2020. COVID-19, digital privacy, and the social limits on data-focused public health responses. Int. J. Inf. Manag. 55, 102181 https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2020.102181.

Folke, C., Carpenter, S.R., Walker, B., Scheffer, M., Chapin, T., Rockström, J., 2010. Resilience thinking: integrating resilience, adaptability and transformability. Ecol. Soc. 15 (4) https://doi.org/10.5751/ES-03610-150420.

Forcepoint, 2018. Life support: eliminating data breaches in the healthcare sector.

Fornell, C., Larcker, D.F., 1981. Evaluating structural equation models with unobservable variables and measurement error. J. Market. Res. 18 (1), 39–50.

Ghosh, K., Dohan, M.S., Veldandi, H., Garfield, M., 2022. Digital transformation in healthcare: insights on value creation. J. Comput. Inf. Syst. 1–11.

Gordon, W.J., Fairhall, A., Landman, A., 2017. Threats to information security — public health implications. N. Engl. J. Med. 377 (8), 707–709. https://doi.org/10.1056/NEJMp1707212.

Greaves, F., Joshi, I., Campbell, M., Roberts, S., Patel, N., Powell, J., 2018. What is an appropriate level of evidence for a digital health intervention? Lancet 392 (10165), 2665–2667.

Hair, J.F., Sarstedt, M., Ringle, C.M., 2019. Rethinking some of the rethinking of partial least squares. Eur. J. Market. 53 (4), 566–584. https://doi.org/10.1108/EJM-10-2018-0665.

Henseler, J., 2018. Partial least squares path modeling: quo vadis? Qual. Quantity 52 (1), 1–8. https://doi.org/10.1007/s11135-018-0689-6.

Henseler, J., Schuberth, F., 2020. Using confirmatory composite analysis to assess emergent variables in business research. J. Bus. Res. 120, 147–156. https://doi.org/10.1016/j.jbusres.2020.07.026.

Henseler, J., Ringle, C.M., Sarstedt, M., 2015. A new criterion for assessing discriminant validity in variance-based structural equation modeling. J. Acad. Market. Sci. 43 (1), 115–135. https://doi.org/10.1007/s11747-014-0403-8.

Henseler, J., Hubona, G., Ray, P.A., 2016. Using PLS path modeling in new technology research: updated guidelines. Ind. Manag. Data Syst. 116 (1), 2–20. https://doi.org/10.1108/IMDS-09-2015-0382.

Hermes, S., Riasanow, T., Clemons, E.K., Böhm, M., Krcmar, H., 2020. The digital transformation of the healthcare industry: exploring the rise of emerging platform ecosystems and their influence on the role of patients. Business Research 13 (3), 1033–1069. https://doi.org/10.1007/s40685-020-00125-x.

Hope, A., 2020. FBI warns of healthcare sector supply chain attacks involving 'kwampirs' malware [online] available from: https://www.cpomagazine.com/cyber-security/fbi-warns-of-healthcare-sector-supply-chain-attacks-involving-kwampirs-malware/. (Accessed 28 August 2021).

Ienca, M., Vayena, E., 2020. On the responsible use of digital data to tackle the COVID-19 pandemic. Nat. Med. 26 (4), 463–464.

Iso/Iec, 2018. Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary. ISO, Geneva. ISO/IEC 27000: 2018.

Jovanović, A., Klimek, P., Renn, O., Schneider, R., Øien, K., Brown, J., DiGennaro, M., Liu, Y., Pfau, V., Jelić, M., Rosen, T., Caillard, B., Chakravarty, S., Chhantyal, P., 2020. Assessing resilience of healthcare infrastructure exposed to COVID-19: emerging risks, resilience indicators, interdependencies and international standards. Environment Systems and Decisions 40, 252–286. https://doi.org/10.1007/s10669-020-09779-8.

Jovanović, A., et al., 2020. Assessing resilience of healthcare infrastructure exposed to COVID-19: emerging risks, resilience indicators, interdependencies and international standards. Environment Systems and Decisions. Springer US. https://doi.org/10.1007/s10669-020-09779-8.

Jung, S.Y., Lee, K., Lee, H.-Y., Hwang, H., 2020. Barriers and facilitators to implementation of nationwide electronic health records in the Russian Far East: a qualitative analysis. Int. J. Med. Inf. 143, 104244 https://doi.org/https://doi.org/10.1016/j.ijmedinf.2020.104244.

Jung, S.Y., Hwang, H., Lee, K., Lee, D., Yoo, S., Lim, K., Lee, H.-Y., Kim, E., 2021. User perspectives on barriers and facilitators to the implementation of electronic health records in behavioral hospitals: qualitative study. JMIR Formative Research 5 (4), e18764.

Kaiser, F.K., Wiens, M., Schultmann, F., 2021. Use of digital healthcare solutions for care delivery during a pandemic-chances and (cyber) risks referring to the example of the COVID-19 pandemic. Health Technol. 1–13.

Kapoor, A., Guha, S., Kanti Das, M., Goswami, K.C., Yadav, R., 2020. Digital healthcare: the only solution for better healthcare during COVID-19 pandemic? Indian Heart J. 72 (2), 61–64. https://doi.org/10.1016/j.ihj.2020.04.001. Elsevier B.V.

Kock, N., Lynn, G.S., 2012. Lateral collinearity and misleading results in variance-based SEM: an illustration and recommendations. J. Assoc. Inf. Syst. Online 13 (7), 546–580. https://doi.org/10.17705/1jais.00302.

Kraus, S., Schiavone, F., Pluzhnikova, A., Invernizzi, A.C., 2021. Digital transformation in healthcare: analyzing the current state-of-research. J. Bus. Res. 123, 557–567.

Kruse, C.S., Kristof, C., Jones, B., Mitchell, E., Martinez, A., 2016. Barriers to electronic health record adoption: a systematic literature review. J. Med. Syst. 40 (12), 1–7.

Larcker, D., Reiss, P., Tayan, B., 2017. Critical update needed: cybersecurity expertise in the boardroom. Rock Center for Corporate Governance at Stanford University Closer Look Series: Topics 17–70.

Liang, X., Barua, M., Chen, L., Lu, R., Shen, X., Li, X., Luo, H.Y., 2012. Enabling pervasive healthcare through continuous remote health monitoring. IEEE Wireless Commun. 19 (6), 10–18.

Maddikunta, P.K.R., Pham, Q.V., Prabadevi, B., Deepa, N., Dev, K., Gadekallu, T.R., Ruby, R., Liyanage, M., 2022. Industry 5.0: a survey on enabling technologies and potential applications. Journal of Industrial Information Integration 26, 100257. https://doi.org/10.1016/j.jii.2021.100257.

Madhavan, N., White, G.R., Jones, P., 2021. Identifying the value of a clinical information system during the COVID-19 pandemic. Technovation, 102446. https://doi.org/10.1016/j.technovation.2021.102446.

Manteghinejad, A., Javanmard, S., 2021. Challenges and opportunities of digital health in a post COVID19 world, 0 J. Res. Med. Sci. 26, 2021–2026. https://doi.org/10.4103/jrms.JRMS_1255_20, 11 (16 February 2021).

Manyena, S.B., 2006. 'The concept of resilience revisited'. Disasters 30 (4), 434–450. https://doi.org/10.1108/S2040-726220140000015002.

Martínez-Caro, E., Cegarra-Navarro, J.G., Solano-Lorente, M., 2013. Understanding patient e-loyalty toward online health care services. Health Care Manag. Rev. 38 (1) https://doi.org/10.1097/HMR.0b013e31824b1c6b.

Martínez-Caro, E., Cegarra-Navarro, J.G., García-Pérez, A., Fait, M., 2018. Healthcare service evolution towards the Internet of Things: an end-user perspective. Technol. Forecast. Soc. Change 136. https://doi.org/10.1016/j.techfore.2018.03.025.

Martínez-Caro, Eva, Cegarra-Navarro, J.G., Alfonso-Ruiz, F.J., 2020. Digital technologies and firm performance: the role of digital organisational culture. Technol. Forecast. Soc. Change 154. https://doi.org/10.1016/j.techfore.2020.119962.

Massaro, M., 2021. Digital transformation in the healthcare sector through blockchain technology. In: Insights from Academic Research and Business Developments. Technovation, 102386. https://doi.org/10.1016/j.technovation.2021.102386.

McGinn, C.A., Grenier, S., Duplantie, J., Shaw, N., Sicotte, C., Mathieu, L., Leduc, Y., Légaré, F., Gagnon, M.-P., 2011. Comparison of user groups' perspectives of barriers and facilitators to implementing electronic health records: a systematic review. BMC Med. 9 (1), 1–10.

Melnic, A.S., Botez, N., 2014. Formal, non-formal and informal interdependence in education. Economy Transdisciplinarity Cognition 17 (1), 113–118.

Morgan, S., 2020. The 2020-2021 Healthcare Cybersecurity Report. https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2020/09/HG-Healthcare-Cybersecurity-Report-2021.pdf.

Morilla, M.D.R., Sans, M., Casasa, A., Giménez, N., 2017. Implementing technology in healthcare: insights from physicians. BMC Med. Inf. Decis. Making 17 (1), 1–9.

Muthuppalaniappan, M., Stevenson, K., 2021. Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. Int. J. Qual. Health Care 33 (1), mzaa117.

National Institute of Standards and Technology, 2018. Framework for Improving Critical Infrastructure Cybersecurity v1.1 [online] available from: https://www.nist.gov/cyberframework/framework. (Accessed 28 August 2021).

National Institute of Standards and Technology, 2018. Framework for Improving Critical Infrastructure Cybersecurity. https://csrc.nist.gov/publications/detail/white-paper/2018/04/16/cybersecurity-framework-v11/final.

Neal, P., Ilsever, J., 2016. Protecting information: active cyber defence for the business entity: a prerequisite corporate policy. Acad. Strat. Manag. J. 15 (2), 15–35.

Nicola, M., et al., 2020. 'The socio-economic implications of the coronavirus pandemic (COVID-19): A review',. International Journal of Surgery 78 (January), 185–193. https://doi.org/10.1016/j.ijsu.2020.04.018.

Offner, K.L., Sitnikova, E., Joiner, K., MacIntyre, C.R., 2020. Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation. Intell. Natl. Secur. 35 (4), 556–585. https://doi.org/10.1080/02684527.2020.1752459.

Podsakoff, P.M., Organ, D.W., 1986. Self-reports in organizational research: problems and prospects. J. Manag. 12 (4), 531–544.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.Y., Podsakoff, N.P., 2003. Common method biases in behavioral research: a critical review of the literature and recommended remedies. J. Appl. Psychol. 88 (5), 879–903.

Pointer, P., 2020. The rise of telemedicine: how to mitigate potential fraud. Comput. Fraud Secur. 2020 (6), 6–8.

Ree, E., Ellis, L.A., Wiig, S., 2021. Managers' role in supporting resilience in healthcare: a proposed model of how managers contribute to a healthcare system's overall resilience. International Journal of Health Governance. https://doi.org/10.1108/IJHG-11-2020-0129.

Ricciardi, W., 2019a. Assessing the impact of digital transformation of health services: opinion by the expert panel on effective ways of investing in health (EXPH). Eur. J. Publ. Health 29 (4). https://doi.org/10.1093/eurpub/ckz185.769.

Ricciardi, W., 2019b. Assessing the impact of digital transformation of health services: opinion by the expert panel on effective ways of investing in health (EXPH). Eur. J. Publ. Health 29 (4). https://doi.org/10.1093/eurpub/ckz185.769.

Ringle, C.M., Wende, S., Will, A., 2005. In: SmartPLS 2.0. University of Hamburg, Hamburg http://www.smartpls.de). https://doi.org/citeulike-article-id:10083551.

Ruiz Morilla, M.D., Sans, M., Casasa, A., Giménez, N., 2017. Implementing technology in healthcare: insights from physicians. BMC Med. Inf. Decis. Making 17 (1), 92. https://doi.org/10.1186/s12911-017-0489-2.

Sallos, M.P., Garcia-Perez, A., Bedford, D., Orlando, B., 2019. Strategy and organisational cybersecurity: a knowledge-problem perspective. J. Intellect. Cap. 20 (4), 581–597. https://doi.org/10.1108/JIC-03-2019-0041.

Scantlebury, A., Sheard, L., Fedell, C., Wright, J., 2021. What are the implications for patient safety and experience of a major healthcare IT breakdown? A qualitative study. Digital Health 7, 1–9. https://doi.org/10.1177/20552076211010033.

Secundo, G., Toma, A., Schiuma, G., Passiante, G., 2019. Knowledge transfer in open innovation: a classification framework for healthcare ecosystems. Bus. Process Manag. J. 25 (1), 144–163.

Shaygan, A., Daim, T., 2021. Technology management maturity assessment model in healthcare research centers. Technovation, 102444. https://doi.org/10.1016/j.technovation.2021.102444.

Sheridan, K., 2018. Supply chain attacks could pose biggest threat to healthcare [online] available from: https://www.darkreading.com/perimeter/supply-chain-attacks-could-pose-biggest-threat-to-healthcare. (Accessed 28 August 2021).

Song, X.M., Montoya-Weiss, M.M., Schmidt, J.B., 1997. Antecedents and consequences of cross-functional cooperation: a comparison of R&D, manufacturing, and marketing perspectives. J. Prod. Innovat. Manag. 14 (1), 35–47. https://doi.org/10.1111/1540-5885.1410035.

Spanò, R., Massaro, M., Iacuzzi, S., 2021. Blockchain for value creation in the healthcare sector. 102440. Technovation. https://doi.org/10.1016/j.technovation.2021.102440.

Taleb, N.N., 2012. Anti Fragile. Penguin, London.

Thomas, A., Suresh, M., 2022. Readiness for sustainable-resilience in healthcare organisations during Covid-19 era. Int. J. Organ. Anal. https://doi.org/10.1108/IJOA-09-2021-2960 (ahead-of-print).

Tortorella, G.L., Saurin, T.A., Fogliatto, F.S., Rosa, V.M., Tonetto, L.M., Magrabi, F., 2021. Impacts of Healthcare 4.0 digital technologies on the resilience of hospitals. Technol. Forecast. Soc. Change 166, 120666 https://doi.org/https://doi.org/10.1016/j.techfore.2021.120666.

Tsang, E.W.K., 2008. Transferring knowledge to acquisition joint ventures: an organizational unlearning perspective. Manag. Learn. 39 (1), 5–20. https://doi.org/10.1177/1350507607085169.

Wang, C., Hu, Q., 2020. Knowledge sharing in supply chain networks: Effects of collaborative innovation activities and capability on innovation performance. Technovation 94 (102010). https://doi.org/10.1016/j.technovation.2017.12.002.

Wef, 2019. The Global Risks Report 2019 [online] available from: https://www.weforum.org/reports/the-global-risks-report-2019. (Accessed 28 August 2021).

Whittaker, A.A., Aufdenkamp, M., Tinley, S., 2009. Barriers and facilitators to electronic documentation in a rural hospital. J. Nurs. Scholarsh. 41 (3), 293–300.

Who, 2020. WHO Director-General's Opening Remarks at the Media Briefing on COVID-19 - 11 March 2020. https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19—11-march-2020.

Willie, M.M., Nkomo, P., 2019. Digital transformation in healthcare–South Africa context. Global Journal of Immunology and Allergic Diseases 7, 1–5.

World Health Organization, 2016. Monitoring and Evaluating Digital Health Interventions: a Practical Guide to Conducting Research and Assessment [online] available from: https://apps.who.int/iris/bitstream/handle/10665/252183/?sequence=1. (Accessed 28 August 2021).

Yildiz, H.E., Fey, C.F., 2010. Compatibility and unlearning in knowledge transfer in mergers and acquisitions. Scand. J. Manag. 26 (4), 448–456. https://doi.org/10.1016/j.scaman.2010.09.010.