NOVEMBER 2020

Qatar Foundation
World Innovation Summit for Health

SAFEGUARDING OUR HEALTHCARE SYSTEMS

A GLOBAL FRAMEWORK FOR CYBERSECURITY

Niki O'Brien
Guy Martin
Emilia Grass
Mike Durkin
Saira Ghafur

ONE WORLD
OUR HEALTH

Suggested reference for this report: O'Brien N, Martin G, Grass E, Durkin M, Ghafur S. Safeguarding our healthcare systems: A global framework for cybersecurity. Doha, Qatar, World Innovation Summit for Health, 2020.

ISBN: 978-1-913991-03-6

SAFEGUARDING OUR HEALTHCARE SYSTEMS
A GLOBAL FRAMEWORK FOR CYBERSECURITY

Report of the Leading Health Systems Network 2020

CONTENTS

FOREWORD

The past decade has seen a surge in the use of new digital technologies across all healthcare settings, which has led to significant improvements in access and care delivery. We have also amassed a wealth of information through these technologies that will help to shape the future of care and dramatically improve health outcomes globally.

A key challenge is how to keep this data safe and secure, and to ensure that patients and the public can trust healthcare organizations with highly confidential information about themselves and their families. There is no quicker way of undermining the public's trust than by allowing essential systems to be compromised or personal data to be lost.

The number of cyberattacks on healthcare organizations has significantly increased in the past five years. In healthcare, these attacks pose more than just a threat to information security: they can jeopardize patient safety. It is therefore critical that we prepare ourselves as much as possible for future incidents.

During the COVID-19 outbreak, cybercriminals exploited the widespread fear and confusion caused by the pandemic. We have seen a new wave of cyberattacks against healthcare organizations, including the World Health Organization (WHO) and the US Centers for Disease Control and Prevention (CDC). Other major attacks, such as the WannaCry ransomware attack on the National Health Service (NHS) in the UK in 2017, have exposed the stark vulnerabilities within health systems and the potential impact on the safe delivery of care.

This report identifies key insights in the international healthcare cybersecurity landscape and proposes a global cybersecurity readiness framework for healthcare organizations.

While there is still much to do in this area, I hope that this publication will serve as a starting point for health systems to assess and ultimately improve cybersecurity. Improved awareness, governance and accountability in this area is essential to protect healthcare organizations from future attacks and ensure that we provide safe care for all patients.

Professor the Lord Darzi of Denham, OM, KBE, PC, FRS
Executive Chair, WISH, Qatar Foundation
Co-Director, Institute of Global Health Innovation, Imperial College London

EXECUTIVE SUMMARY

Digital technology has transformed health systems, helping to reduce costs and improve the management of patient care. But the rapid global adoption of emerging technologies in healthcare has led to increased vulnerability to cyber threats that can erode patient trust and compromise the safety and confidentiality of patient data. The number of cyberattacks is rising, and healthcare systems and organizations around the world are lagging behind other sectors in developing cyber readiness – the ability to act against cyberattacks. The challenges in cybersecurity planning across high-, middle- and low-income health systems are varied. There has been a lack of investment and support to raise awareness of its global importance. Urgent work is needed to help healthcare organizations develop a common language and scale-up cybersecurity planning.

While there has been cybersecurity investment in high-income countries, success can be hindered by the challenge of working with outdated Health Management Information Systems (HMIS). However, in low– and middle-income countries there is a chance to design a system with cybersecurity at its foundation.

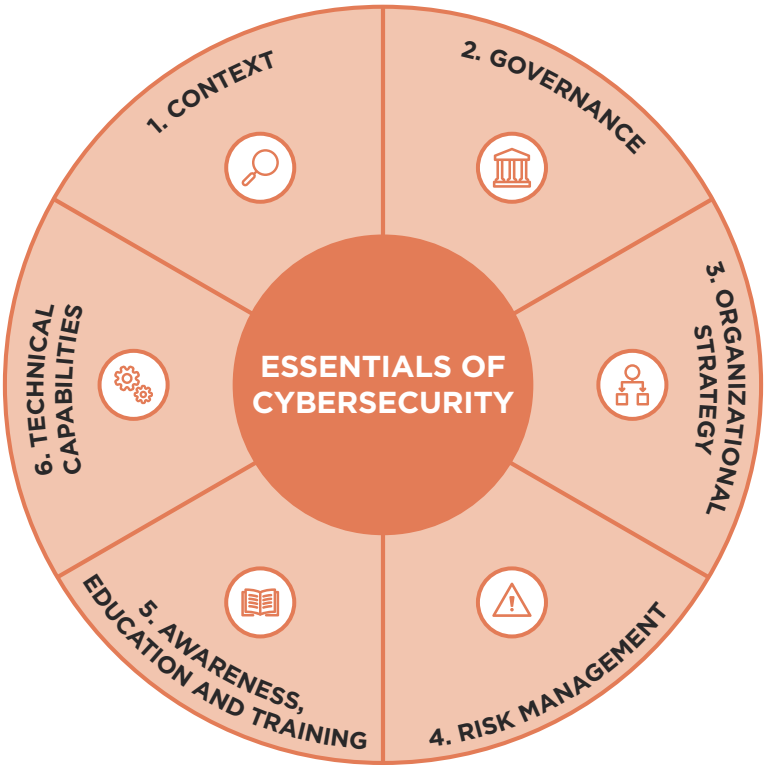
In this report we look at existing cybersecurity frameworks worldwide. And we examine why, despite being one of the sectors most targeted by cyberattackers, the healthcare sector remains one of the worst adopters of cybersecurity frameworks.

In response to this urgent sector need, we asked members of the Leading Health Systems Network (LHSN) – an international group of health systems and providers hosted at Institute of Global Health Innovation (IGHI), and key experts in the areas of IT, cybersecurity, health policy and health systems – about their experiences and organizational efforts related to cybersecurity. An initial survey of LHSN member institutions explored the current global cybersecurity landscape. We then convened a group of experts from a range of health systems to provide input on the most relevant elements of a global framework for cyber readiness in healthcare. The resulting Essentials of Cybersecurity in Healthcare Organizations (ECHO) framework was developed by the IGHI, Imperial College London, with input from the LHSN.

The ECHO framework includes the most important elements of a global cybersecurity framework for healthcare (see Figure 1). It outlines the six primary dimensions to consider when scaling up cybersecurity in a healthcare organization. The ECHO framework may act as a 'minimum standard' or an aspirational checklist, depending on an organization's

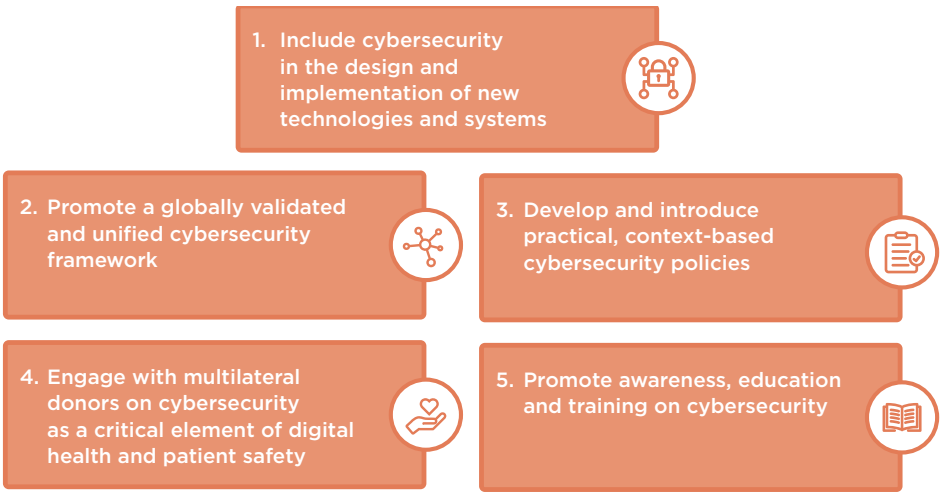
resources and its cyber maturity – that is, the level it has achieved in its ability to protect its information assets against cyber threats. Section 5 of the report examines each of these dimensions in more detail.

Figure 1. The ECHO framework



Developing effective, global guidance on cybersecurity is challenging. While the ECHO framework is a starting point, a number of additional steps are needed to cement cybersecurity readiness for the future. These further building blocks are shown in Figure 2.

Figure 2. Building blocks to cement cybersecurity readiness



The building blocks to improve security in the use of health data and systems for patient safety are outlined as a series of policy recommendations:

1. **Include cybersecurity in the design and implementation of new technologies and systems**

   As countries seek to strengthen health systems through digitization, cybersecurity should be included in the design and implementation of technologies and systems. At national level, appropriate governance and regulation specifically related to cybersecurity in healthcare (such as medical device standards) can help to ensure that best practice is followed at local level. At organizational level, responsibility for overseeing cybersecurity should be designated to individuals with a minimum level of literacy about cyber threats and solutions.

2. **Promote a globally validated and unified cybersecurity framework**

   The readiness framework presented in this report has been designed to be used across all settings – high-, low– and middle-income countries – and introduces a common language as a first step. At the national level, a global cybersecurity framework should be incorporated in high-level policy guidance. At institutional level, a framework should guide the development and sustainability of cybersecurity planning. The next step is to validate the framework globally, which will require strong partnerships to conduct research across institutions and their different contexts to help refine the recommendations.

3. **Develop and introduce practical, context-based cybersecurity policies**

   Any cybersecurity actions or policies need to be risk-based and practical, to appropriately mitigate risks while balancing resource requirements. Top-down priority setting by governments should be accompanied by the building of cyber awareness from the bottom up, with basic technical interventions and systems that do not require vast resources. Different organizations can then assess whether cybersecurity interventions are cost-effective, based on local context and resources.

4. **Engage with multilateral donors on cybersecurity as a critical element of digital health and patient safety**

   It is essential that financial and human resources are readily available to scale up efforts globally. This is especially important in LMICs, which may require support in establishing sustainable cybersecurity practices and technical expertise. At national level, Ministries of Health

and Finance should discuss priority setting for the development of technical capacity within their governance structure and the introduction of appropriate health technology in healthcare organizations. They should also encourage donors to include aspects of security, resilience and technical capacity building. At organizational level, the importance of cybersecurity should be prioritized as part of a wider IT strategy, acting as a catalyst to ground-level advocacy for cybersecurity within global health investment.

5. **Promote awareness, education and training on cybersecurity**

Awareness of the importance of cybersecurity is important at all levels of healthcare – from patient engagement with the topic, to front-line workers understanding how cyber hygiene can be incorporated within their job function, to health and policy planners recognizing the importance of cybersecurity to their organization and the wider health system. At national level, expertise should be sought to develop a national curriculum of cybersecurity in healthcare. At organizational level, resources on cybersecurity should be available to all staff and a culture of awareness should be championed.

SECTION 1. INCREASING AWARENESS OF CYBERSECURITY IN HEALTHCARE

The use of digital technology in healthcare has transformed health systems globally. The benefits of such transformation are vast and varied, including: increased data sharing and analysis; novel management of patient care; increasing patient access; and often reduced costs.[1]

Health systems are becoming increasingly reliant on digital technologies. WHO's *Global Strategy on Digital Health 2020–2024* outlines plans to accelerate the "development and adoption of appropriate digital health solutions to rapidly explore how to make use of digital health technologies to combat pandemic outbreaks, developing infrastructure and applications that allows us to use health data to manage outbreaks". The policy document outlines a plan to ensure that the scale-up of digital health is ethical, safe, secure, reliable, equitable and sustainable, and developed with the security principles of interoperability, privacy and confidentiality.[2] For the strategy to be successful, health systems and their data must be secure, implemented with appropriate security, monitoring systems and staff education. Rigorously enforced technology standards must also be mandated to ensure that data is interoperable and accessible.[3]

While we have begun to see greater investment for healthcare cybersecurity provision in high-income countries (HICs), the security of (often outdated) Health Management Information Systems (HMIS) is usually only substantially updated following a cyberattack or other security breach.[4] As a result, the implementation of security planning to ensure the protection of data and patients is often a significant challenge. In many low- and middle-income countries (LMICs) there is an opportunity to 'leapfrog'* the challenges in HICs and ensure that systems are secure by design. In such settings, the health systems, use of digital technology in health, and HMIS are at an earlier stage of development for the most part.

* The term 'leapfrog' is defined by the World Economic Forum as a means "to accelerate development and achieve results equal to or better than those of mature economies, in less time".[5]

In LMICs, digital technology and electronic health (eHealth) solutions such as electronic health records (EHR) were historically used to inform international bodies or donors on health outcomes (eg HIV, tuberculosis, malaria burden, disease incidence, and so on). In Sub-Saharan Africa, EHRs have a legacy of personal data breaches, particularly for HIV data, with severe or grave ramifications for some individuals. As a result, there is public skepticism about whether health data and the use of digital technology in healthcare is safe.[6] However, there are more recent examples of digital technology, including HMIS, being used successfully at the national and local level. For example, the Rwandan Ministry of Health has co-developed an electronic medical records (EMR) system that holds patient records for 33 health centers across three districts, including a catchment area of about 800,000 people.[7]

Similarly, mobile telecommunication technology (mHealth) is increasingly being used in healthcare systems, particularly in LMICs.[8] Mobile devices are the primary means of internet access in LMICs, which has driven the rise of mHealth in this setting.[9] Globally, health systems are transitioning from paper-based methods to more real-time reporting of routine health data by health workers. This involves the use of mobile devices such as smartphones or personal digital assistants (PDAs) to collect, transmit and aggregate data across multiple sites and levels. Literature shows that breaches can occur while information is stored on a mobile device with weak security safeguards, and when data is sent to centralized servers through unsecure networks. Loss and theft of phones is also a major security concern.[10] However, it should be noted that eHealth and mHealth innovations require different cybersecurity planning considerations: eHealth describes healthcare supported by electronic processes more generally; whereas mHealth exclusively describes healthcare solutions requiring the use of a personal mobile device.[11]

SECTION 2. WHY WE NEED A CYBERSECURITY READINESS FRAMEWORK FOR HEALTHCARE INSTITUTIONS

Defining cybersecurity and associated key terms

Cybersecurity has been defined as "how individuals and organizations reduce the risk of cyber-attack".[12] While this definition is relatively comprehensive and provides a broad explanation of the concept, there is no globally agreed definition of key terms. For example, cybersecurity strategy documents in most countries define 'cybersecurity' as protection against all threats within cyberspace. However, Finland and Austria limit cybersecurity to the protection of critical infrastructure or digital information.[13]

Because cyberattacks have become more sophisticated, and there is a greater chance of large-scale cross-border cyber incidents, national governments are increasingly considering the importance of reinforcing international co-operation and regional agreements.[14,15] Clear, comprehensive, and internationally accepted definitions of cybersecurity and associated key terms are an important step in achieving this goal.

Vulnerabilities in the healthcare sector

Cybercrime in healthcare can have significant implications for patient safety, yet the preparedness for cybercrime events has been reported as relatively poor. Healthcare is more vulnerable compared to other critical sectors, as financing for cybersecurity is not assured, particularly in public sector health systems. In the UK, many National Health Service (NHS) Trusts reportedly spend as little as 1 to 2 percent of their annual budget on IT infrastructure, compared to 4 to 10 percent in other sectors (such as finance and telecommunication).[16] (See WISH 2018 Report on Data Science and AI for further information.)

See WISH 2018 Data Science and AI Report, page 22

In LMICs, financing for cybersecurity in healthcare is an even greater challenge. As governments invest less of their gross domestic product (GDP) in the health sector, there are fewer resources to be directed to data security and building cyber-resilient health systems. Also, in many

LMICs, donor spending represents more than a fifth of health sector financing, with budgets increasingly set aside for specific disease areas or initiatives rather than for strengthening health system management and infrastructure.[17]

Cyberattacks in healthcare

In the last decade, the number and severity of cyberattacks in healthcare settings around the world has significantly increased.[18] A range of attacks have caused major disruption to organizations, resulting in financial loss, and compromising patient safety (see Table 1 for a list of recent cyberattacks).

Table 1. Recent high-level cyberattacks around the world

Organization name	Date of attack	Target	How it impacted on patients
 **NHS (UK)**	May 2017	UK's NHS was a target of the WannaCry attack alongside multiple organizations outside the health sector	Access to systems was blocked, preventing staff from accessing patient data and critical services. Thousands of appointments and surgeries were cancelled.[19]
 **SingHealth (Singapore)**	June 2018	SingHealth, the largest group of healthcare institutions in Singapore	The personal details of 1.5 million patients were stolen, including the outpatient prescriptions of Prime Minister Lee Hsien Loong.[20]
 **Victorian hospital network (Australia)**	September 2019	Hospitals, part of the Gippsland Health Alliance, and the South West Alliance of Rural Health	Surgeries and outpatient care were delayed or cancelled as the incident blocked access to several systems, including the financial management system.[21]
 **Druid City Hospital (DCH) Health System (USA)**	October 2019	DCH Health System Regional Medical Centers	Care for non-critical patients was disrupted for 10 days. An undisclosed amount was paid to the attackers to unlock the seized files and allow services to resume.[22]
 **Life Healthcare (South Africa)**	June 2020	Life Healthcare's Southern African operation	The attack affected admissions and business processing systems as well as email servers, resulting in administrative delays to patient services.[23]

Box 1. Cybersecurity challenges in the COVID-era

Organizations across health, social care and local government have experienced increased cyber threats related to COVID-19, with a significant increase in the number of attacks during this period.[24] The scope of the cyberattacks has varied, and attackers have targeted individuals and organizations globally.

The main threats to cybersecurity during the COVID-19 period have been the result of:

- A significant movement of staff as they are redeployed within existing organizations or externally to help respond to the pandemic. This movement leads to the increased risk in maintaining adequate access controls to IT systems, and also in accidental errors due to working with unfamiliar systems.
- Health systems being stretched, with new IT systems deployed to meet the challenge of delivering remote patient care. This results in the likelihood of the day-to-day management of cyber risks not being prioritized.
- The rapid introduction of new digital solutions while ensuring that patients still have access to healthcare. New technologies have inherent risks of compromising systems, such as design flaws that jeopardize the security of the data they hold.
- Lack of stringent oversight of content input on mobile app platforms, resulting in increasing dissemination of false or misleading information being presented as informal clinical guidance.

The COVID-19 pandemic has shown that cybersecurity needs to be a fundamental and consistent consideration, and that protective mitigation strategies need to be in place. Health systems with good cybersecurity resilience have the tools and expertise to respond to the additional challenges to security during periods of crisis.

Cyber threats challenge patient safety

Cybersecurity is a major patient safety concern. A disruption, corruption or leak of data may significantly disrupt patient care and erode trust. The risks associated with the growing use of digital technology in healthcare – particularly the safety and security of health data – must be considered and

See WISH 2020 Mental Health and Digital Technologies Report, page 28.

managed systematically across institutions with an adaptable approach that responds to emerging threats and lessons learned. (See WISH 2020 Report on Mental Health and Digital Technologies and 2018 Report on Precision Medicine for further information.)

See WISH 2018 Report on Precision Medicine, page 18.

Yet many system leaders and workers within the healthcare sector do not yet recognize the connection between patient safety and cybersecurity, which is often considered a separate technical concern. As a result, relatively little is known about the impact of poor cybersecurity on the delivery of safe patient care.[25] However, a recent analysis of the WannaCry cyberattack on the UK NHS found that hospitals directly infected with the ransomware recorded: significantly fewer emergency and elective admissions, including a 6 percent decrease in total admissions per affected hospital per day; 4 percent fewer emergency admissions; and 9 percent fewer elective admissions.[26] This indicates that the cyberattack could have a significant impact on access to and timeliness of care.

In September 2020 the first reported patient death directly attributable to a cyber-attack was reported; a woman in a life-threatening condition was sent to a hospital approximately 20 miles away following cyber-attack on a hospital in Dusseldorf, Germany, and died subsequently from treatment delays.[27] Given the clear impact on patients – including risks associated with delayed admissions, closures of emergency departments or the inability to view EHRs and vital test results – the ongoing safety of patients should be a clear objective for those responsible for delivering healthcare cybersecurity. Likewise, cybersecurity should be a clear objective in patient safety planning and subsequent strategies.

It is critical to understand and manage the underlying patient safety risk factors related to cybersecurity. This includes addressing poor governance, vulnerable security architectures, financing, and cultures or behaviors that lead to increased risk.[28] It is also essential to work with leadership and frontline staff to take a preventative approach to protecting systems against cyberattacks and to ensure patient safety.[29] (See WISH 2018 Report on Data Science and AI and 2015 Report on Patient Safety for further information.)

See WISH 2018 Data Science and AI Report, page 22.

See WISH 2015 Patient Safety Report, page 21.

SECTION 3. HOW WE CAN SCALE-UP CYBERSECURITY

Existing cybersecurity frameworks

Cybersecurity frameworks are tools commonly adopted by organizations to promote cyber resilience and outline steps to help protect themselves.[30] Good cybersecurity practices can never be one hundred percent effective. However, better prepared organizations are less likely to suffer from breaches, and are more likely to recover from attacks quickly and with less impact.

It is important to understand which data and systems need to be protected and what their key assets are, as well as the potential impact of a successful breach. Furthermore, organizations must identify potential sources of breaches or attacks, their most likely targets or intentions, and their capability to disrupt essential systems.

In the global cybersecurity sector, the USA has long been considered the leader in cybersecurity provision through the NIST Cybersecurity Framework, a voluntary policy framework created in a collaboration between industry and government.[31] The NIST Cybersecurity Framework has been translated into multiple languages and is used in countries around the world. Cybersecurity provision is also a focus of many national governments across HICs, as well as regional bodies such as the European Union.[32,33]

In the UK, several cybersecurity frameworks have been developed to help organizations improve their cybersecurity. Cyber Essentials, a government-backed, industry-supported certification scheme is one example. The assessment comprises a vulnerability scan, which helps identify unpatched (vulnerable code) or unsupported software, open ports, incorrect firewall configuration, and so on.[34] The certification offers learning on different elements of cybersecurity, though does not directly apply these principles to the health sector.

The Data Security and Protection Toolkit is an online self-assessment tool for UK healthcare organizations to measure their performance against identified security standards.[35] Every organization with access to NHS patient data and systems must comply with government regulations by completing the self-assessment.[36]

Box 2. Types of cybersecurity frameworks

Three common types of generic cybersecurity frameworks are used across sectors, depending on the organization's capacity and security needs:[37]

Control frameworks (eg National Institute of Standards and Technology (NIST) SP 800–53 and Center for Internet Security (CIS) Controls) are typically used by organizations with relatively immature IT infrastructure and security provisions. They support organizations to identify a baseline set of controls, access the capabilities of their technology, prioritize the implementation of controls, and develop an initial roadmap for the security team.[38]

Program frameworks (eg International Organization for Standardization (ISO) 27001 and NIST Cybersecurity Framework) are sometimes used in conjunction with control frameworks to: support organizations to develop more comprehensive security based on an assessment of their existing program; compare the maturity of the system to others in the industry; and simplify communication with business leaders.[39]

Risk frameworks (eg NIST 800–39, 800–37, 800–30; ISO 27005; and Factor Analysis of Information Risk (FAIR)) allow cybersecurity personnel to determine how to prioritize cybersecurity efforts and manage the program while considering stakeholders throughout the organization. Cybersecurity professionals use risk frameworks to: define key processes for assessing and managing risk; structure the risk management program; and prioritize security activities.[40]

LMICs also provide excellent examples of national leadership in advancing cybersecurity.[41,42,43] Kenya has adopted a multistakeholder approach to cyber resilience, with collaboration between, but not limited to, the government, telecommunications and financial organizations, academia, public utility services and critical infrastructure providers.[44] Rwanda has established the National Cybersecurity Agency to oversee the protection of critical information infrastructure, the Rwanda Information Security Agency to oversee the management of government infrastructure, and the Rwanda Utilities Regulatory Authority to monitor private operators and service providers.[45,46]

Cybersecurity frameworks in healthcare

The healthcare sector is broadly considered to be one of the worst adopters of cybersecurity frameworks, despite being one of the most targeted critical sectors. Existing cybersecurity frameworks used in healthcare globally may act as a guide in how healthcare organizations develop, select and implement frameworks into their governance structures. For example, the Royal Australian College of General Practitioners has published a set of standards for organizations and businesses within the healthcare sector, with guidance on recovery planning, access management and risk assessment.[47]

However, international healthcare-specific standards are presently missing. In the HIC context, challenges to the implementation of consistent cybersecurity standards across organizations include:

- fragmented governance.
- the need for users to have access to patient records at any time.
- the lack of pressure from leadership to improve security standards and interconnectivity.
- limited resources to expend on cybersecurity solutions, including professional expertise.[48]

Among the Gulf States, only the United Arab Emirates and Saudi Arabia have separate cybersecurity regulations for healthcare. The lack of regulation makes it challenging to develop the governance structure required to improve resilience to cybersecurity challenges.[49] In LMICs, many of the same challenges exist. However, there are additional barriers to consider, including a lack of broad awareness of cybersecurity threats, a common language and IT infrastructure, and financial resources to fund cybersecurity resilience in the health sector.[50,51,52]

It remains a challenge to translate national-level work on cybersecurity into meaningful guidance and action within the healthcare sector. Yet it is imperative to explore the state of cybersecurity across international healthcare settings to produce a global readiness framework for cybersecurity planning across health systems and individual institutions.

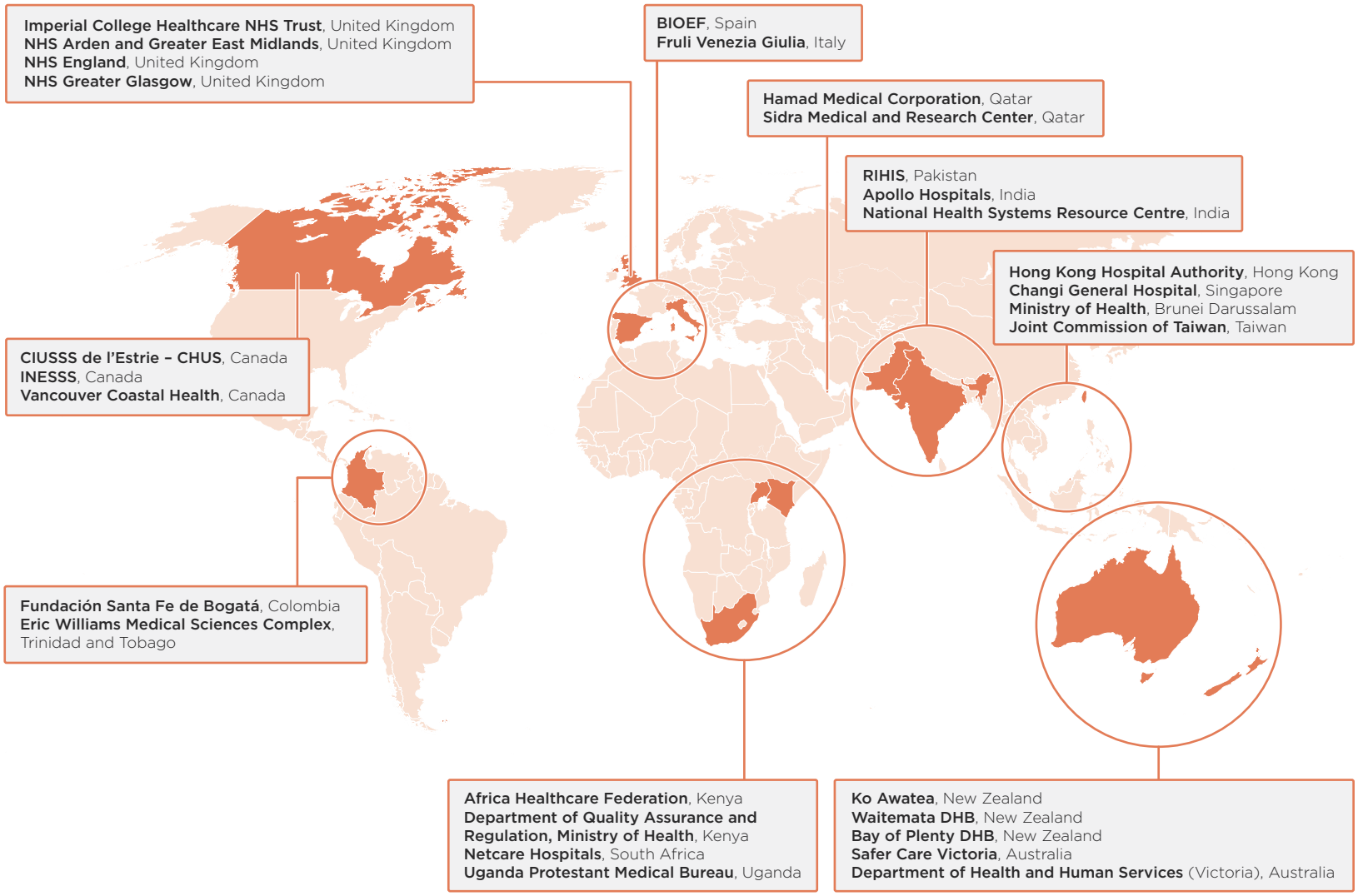
SECTION 4. HOW LHSN MEMBERS HAVE EXPERIENCED CYBERATTACKS AND DEVELOPED CYBERSECURITY

This section provides an overview of LHSN member institutions' experiences and organizational efforts related to cybersecurity.

LHSN overview

Hosted at the Institute of Global Health Innovation at Imperial College London, the LHSN is a collaborative network of healthcare leaders and organizations dedicated to improving healthcare delivery. The network connects healthcare leaders and organizations that value the international sharing of evidence and best practice. LHSN supports data collection, collaboration and knowledge exchange among health institutions in ways that bring added value to healthcare systems at international, national and local levels.

Figure 3. Map of LHSN members and participant organizations



Source: www.leadinghealthsystemsnetwork.org/members

The cybersecurity project approach

The LHSN cybersecurity project was conducted in two parts:

Part 1 (Survey): The first part aimed to explore the current global cybersecurity landscape by surveying the experiences of LHSN member institutions around the world. LHSN member institutions incorporate a range of global health-focused institutions, offering a broad view on the state of cybersecurity in the health sector.

The survey contained two main sections:

- **Organizational cybersecurity landscape:** questions designed to assess each organization's experience with cyberattacks and their cybersecurity planning.

- **Cybersecurity maturity:** This section was developed based on the Global Cyber Security Capacity Centre's Cybersecurity Capacity Maturity Model for Nations (CMM)[53] and asked questions about the organizations' level of planning across six domains of cybersecurity to determine the maturity level of their response. After collating and analyzing response data, the research team used the results to supplement Part 2 of the project.

Part 2 (Delphi consensus development exercise*): The second part of the project brought together a range of experts in the areas of cybersecurity, IT and health informatics from different health systems, to identify the most relevant elements of a global cybersecurity framework for healthcare.

A Delphi consensus development exercise was conducted electronically with a group of 34 experts from 16 countries. The Delphi technique uses structured communication and systematic research, relying on the panel of experts to reach consensus on given topics. The experts answer questionnaires in successive rounds, with a facilitator providing an anonymized summary of the experts' judgment after each round. The participants are encouraged to revise their earlier answers in light of the information they gain before the beginning of each round. Finally, the process is stopped after a predefined condition is met (for example, by a predetermined number of rounds, or a consensus).[54]

* A full description of this exercise and the results have been published in *BMJ Innovations* http://dx.doi.org/10.1136/bmjinnov-2020-000572.

During Part 2 of the project, the experts answered questionnaires in three rounds. Consensus was defined as agreement on the most important topics or components relevant for a global healthcare cybersecurity readiness framework. This was achieved after the third round.

Results of the LHSN cybersecurity project

Part 1 (Survey) results

A total of 17 institutions took part in the survey, across six geographic regions (see Figure 4). Of the hospitals/medical centres, 17.6 percent were public, 5.8 percent were faith-based, and 17.6 percent were private; 17.6 percent of the institutions were regional Ministries of Health; 17.6 percent were non-governmental organizations (NGOs); 5.8 percent were research institutions; and 17.6 percent were classified as 'other' (see Figure 5).

All of the institutions directly providing healthcare services noted that they used EHRs in some capacity, although there was a varied level of digital maturity across the different organizations.

Figure 4. Participation by region as defined by the World Health Organization (WHO) (N=17)

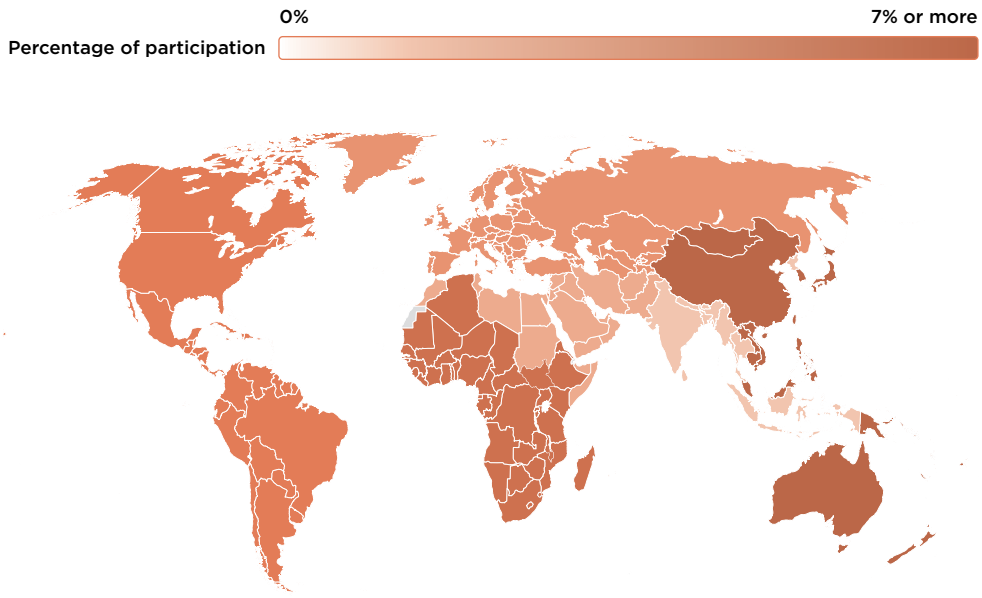
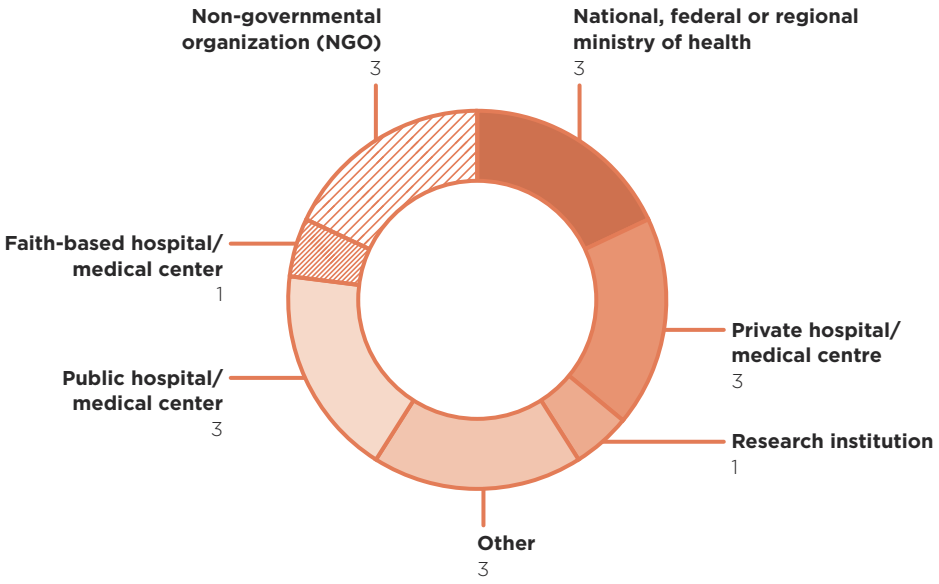


Figure 5. Participation by sector (N=17)



1. Attitude to cybersecurity

Survey respondents were asked what they considered to be the greatest threat to cybersecurity within their organization.

- The most common perceived threat to cybersecurity related to data. Participants noted the potential loss or manipulation of health records as a key concern, noting that the data could be used for blackmail or to defraud an individual or organization. This could result in a loss of trust in healthcare organizations and reputational damage.

- Several respondents also noted the risk of service disruption as a major threat to cybersecurity and resilience. Others outlined their concerns for the consequences of such service disruptions, particularly patient harm or death, or the financial implications for patients and the organization itself.

- Threats related to organization management were a concern for many. Insider or internal threats such as intentional or unintentional data leaks and cyberattacks impacting on operations (specifically the ability to deliver patient care) were the major consequences outlined as a result of poor management.

- The final threat area noted by respondents was related to technology. The major concerns in this area were systems vulnerabilities and ransomware. However, unique to the health sector, respondents noted concerns around the threat of automation of medical

and related services, exposure to potentially fatal service disruptions, and the obsolescence and diversity of information systems and biomedical equipment.

2. Cyberattack experiences

- Within the sample, there was an increasing frequency of cyberattacks across all institutions over the past two years. 56 percent of organizations had experienced a cyberattack in the previous 12 months (see Figure 6). However, some respondents may not have been aware of the cyberattacks that have taken place.

- Survey respondents reported a range of impacts of cyberattacks, including work system outage, data loss, patient appointments cancelled, projects delayed, and the opportunity cost of these consequences. However, it should be noted that the full extent of the attacks may not have been known by the organizations.

- Respondents were positive overall about their effectiveness in dealing with the cyberattacks that had occurred in the previous 12 months. The average self-reported cybersecurity effectiveness score was 7 out of 10. However, 37 percent of respondents gave their institution a score of 6 or below.

Figure 6. Experiences of cyberattacks in the past 12 months (N=16)

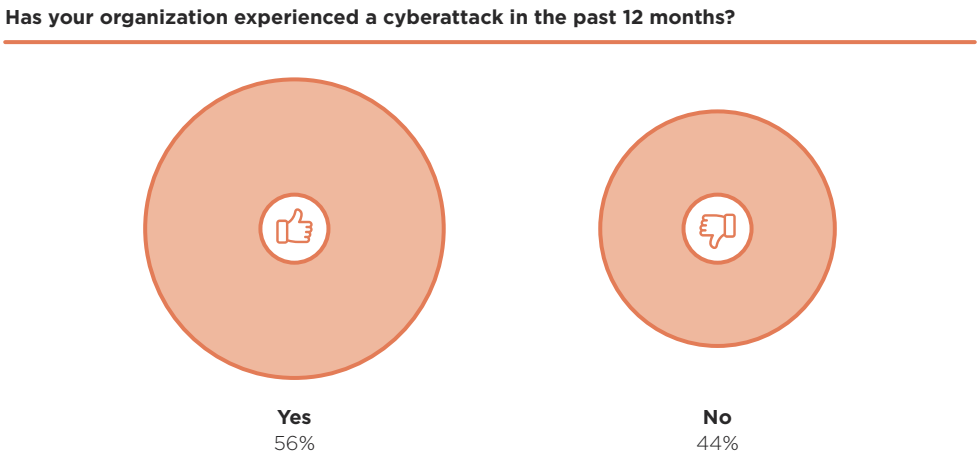
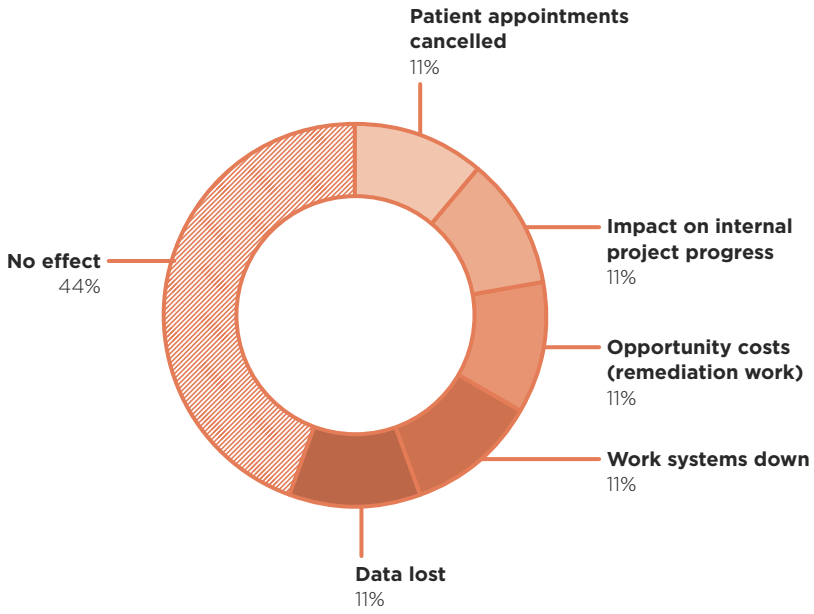


Figure 7. Reported impact of the most serious cyberattack reported (N=9)



3. Cybersecurity governance

- The majority of respondents were required to report cyber incidents as part of local or national regulatory or legal requirements (69 percent) (see Figure 8).

- Of those who were required to do this reporting, 73 percent reported internally to senior leadership/board (including the Chief Information Security Officer or the Chief Information Officer), 55 percent reported to a national data protection agency, and 36 percent reported to the Ministry of Health.

- The majority of those who said they were not required to report cyber incidents as part of national regulatory or legal requirements were working within LMIC health settings. Half were classified as not-for-profit/non-governmental healthcare organizations.

Figure 8. Cybersecurity regulatory requirements (N=16)

Is your organization required to report cyber incidents as part of any local or national regulatory/legal requirements?

Yes
69%

No
25%

Don't know
6%

- Within the sample, the majority (94 percent) reported that cybersecurity was part of the organization's leadership or board agenda (see Figure 9).
- Only 62 percent reported that training was available for the organization's leadership (see Figure 10).
- 60 percent reported that a member of the board had been appointed a cybersecurity lead/responsible for cybersecurity (see Figure 11).
- The majority of organizations (75 percent) had not performed a simulation of a major cyberattack (see Figure 12).

Figure 9. Cybersecurity and organizational leadership agenda (N=16)

Is cybersecurity part of your organization's leadership/board agenda?

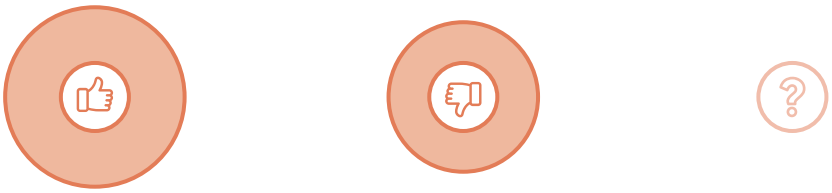
Yes
94%

No
0%

Don't know
6%

Figure 10. Cybersecurity training for organization leaders (N=13)

Is cybersecurity training available for your organization's leadership?



Yes
62%

No
38%

Don't know
0%

Figure 11. Cybersecurity and organizational leadership responsibility (N=15)

Has a member(s) of the board been appointed cybersecurity lead/responsible for cybersecurity?

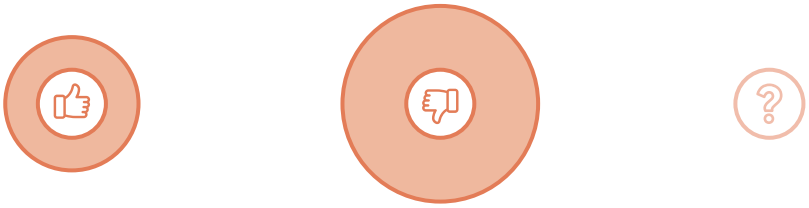
Yes
60%

No
33%

Don't know
7%

Figure 12. Organizational cyberattack simulation (N=12)

Has your organization performed a simulation of a major cyberattack incident?



Yes
25%

No
75%

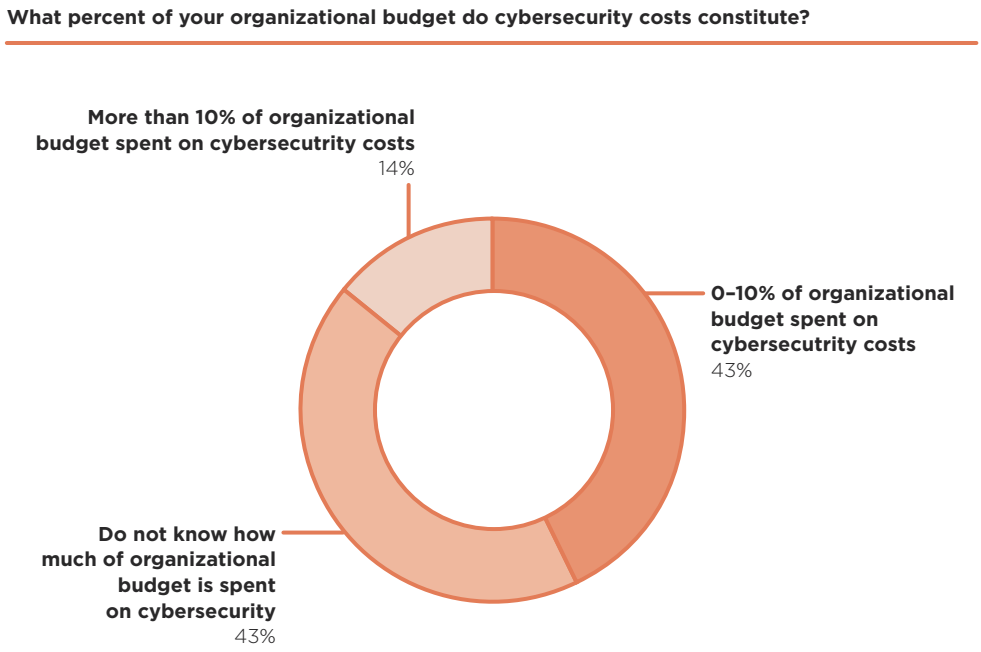
Don't know
0%

4. Financial governance

Survey respondents were asked specifically about financial governance in their organization.

- 88 percent of respondents noted that the organization had a dedicated budget for cybersecurity.
- The percentage of organizational budget that constitutes cybersecurity costs varied from 0 to 10 percent (43 percent of respondents) to 61 to 70 percent (7 percent of respondents) (see Figure 13).
- The range of percentages reported may be due to the different types of healthcare organizations that took part in the survey, or different interpretations of 'organizational budget'.
- A total of 43 percent of respondents did not know the percentage of organizational budget for cybersecurity. However, 71 percent of respondents noted that the budget for cybersecurity had increased in the past 12 months.

Figure 13. Percentage of organizational budget for cybersecurity costs (N=14)



5. Measuring cyber maturity

Questions were developed based on the dimensions and maturity levels outlined in the Global Cyber Security Capacity Centre's CMM to assess the cyber maturity of the organizations.[55]

The CMM outlines five dimensions that that cover the scope of cybersecurity by defining areas that should be considered when seeking to develop capacity.[56] The maturity levels describe how a country has progressed in relation to specific aspects of cybersecurity across the dimensions. There are five stages of maturity: start-up, formative, established, strategic, and dynamic. The dimensions and maturity levels outlined in the CMM were chosen as a starting point for the survey development as they have already been validated globally, though not specifically in healthcare.

As part of the survey design process, the research team developed the aspects of cybersecurity across six dimensions, rather than five, to better reflect and measure maturity in healthcare specifically, and at organizational rather than national level.[57] Respondents were asked questions across six domains: governance (planning for cyberattacks and to improve cybersecurity); awareness (organizational knowledge of cyber threats, incidents and appropriate response); education (training of stakeholders within the organization on cybersecurity); regulation (the national legislative requirements on cybersecurity); technology (the security of technology and IT infrastructure within the organization); and resilience (the organization's ability to respond to cyber threats and attacks).

Each response was scored on a scale of maturity: 1 (start-up), 2 (formative), 3 (established), 4 (strategic), 5 (dynamic).[58] The average score for each dimension and region is shown in Figure 14.

Figure 14. Cyber maturity score by dimension/region (N=13)

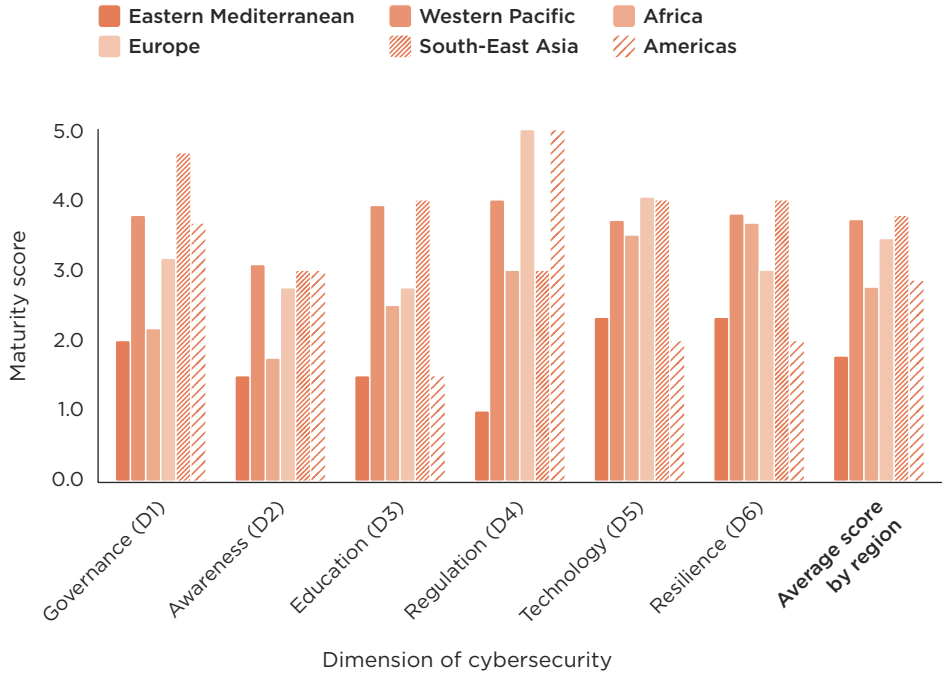


Table 2. Cyber maturity categorization by region (N=13)

Region	Maturity score	Categorization
Africa	2.7	Established
Eastern Mediterranean	1.7	Formative
Europe	3.4	Established
The Americas	2.8	Established
South-East Asia	3.7	Strategic
Western Pacific	3.7	Strategic

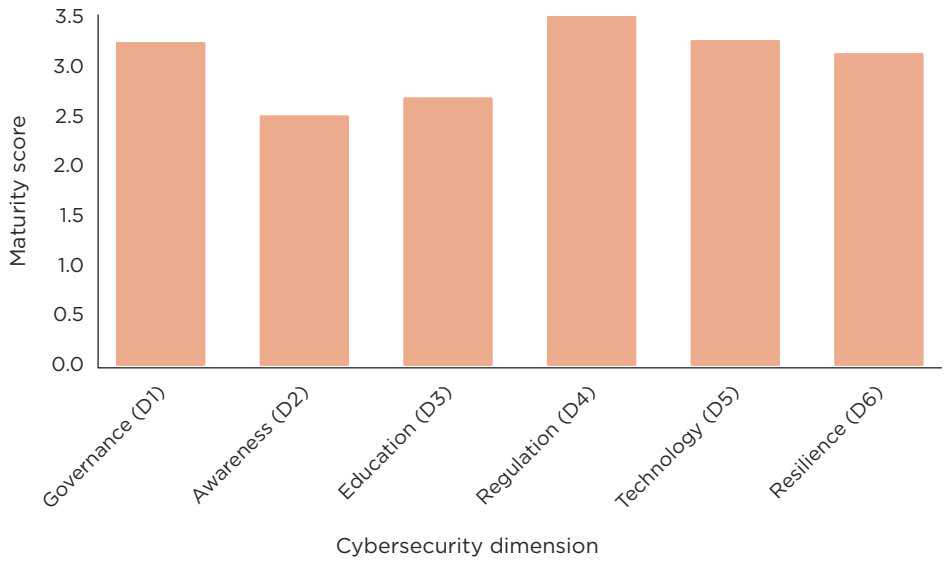
The regional scores outlined particular areas where respondent organizations had particular maturities and areas for improvement. The score for Europe and the Americas was particularly high in regulation, whereas the score for the Eastern Mediterranean and South-East Asia region relatively poor. The South-East Asia region's score was particularly high in the domain of governance, as was the score for the Western Pacific Region. The Africa region scored highest in technology and resilience, while scoring lowest in education and awareness. The region of the Americas scored the lowest in education.

Calculating the scores across domains, the South-East Asia region had the highest maturity score (3.7), categorized as 'strategic' in its maturity level (Table 2). The Western Pacific region was also categorized as

'strategic' in its maturity level (3.7). Notably the organizations in these regions were overrepresented in reporting the number of cyberattacks their organization had experienced in the preceding 12 months. Overall, they reported the fewest attacks as compared to reported attacks in other regions (N=8). Three regions were categorized as 'established' based on their maturity scores: European region (3.4), the Americas (2.8), and African region (2.7). The Eastern Mediterranean region was categorized as 'formative' based on its maturity level score (1.7).

The dimension (D) with the highest maturity score was D4 regulation (3.5) (see Figure 15). Other dimensions scoring above 3 ('established') were D1 governance (3.2), D5 technology (3.2): and D6 resilience (3.1). However, D2 awareness (2.5) and D3 education (2.6) scored less than 3, suggesting that these areas are less developed among respondent organizations.

Figure 15. Cyber maturity score by dimension (N=13)



Summary of survey results

This survey showed that cyber threats are a critical concern for healthcare organizations globally. The most common perceived risk to cybersecurity related to data, as participants noted their reliance on EHR and their concern for the potential loss or manipulation of health records. Reports of existing attacks highlighted the far-reaching impact of cyberattacks on patients and the organization, including delays to healthcare delivery.

Results showed that some level of governance and awareness training for executives on cybersecurity is a consideration at the global level. However,

the maturity analysis showed that, in several regions, more work must be done to develop guidelines to scale-up these areas. Taken together, the maturity scores of individual organizations offer optimism that cybersecurity is a tangible consideration in healthcare globally. However, more must be done to develop the holistic cybersecurity response to be dynamic in responding to the increasingly complex nature of cyberattacks.

Research limitations

Limitations of the research should be considered when interpreting the survey results. The primary limitation is the small sample size. While the results showcase results from all six regions, the sample size of 17 institutions is small, and some regions had greater representation than others in completed surveys. Therefore, it is possible that the same survey with a larger number of participants could produce different results. The survey was completed by a variety of types of organization, and it is possible that the results do not accurately reflect the cybersecurity landscape in any one particular health setting. Also, the survey was self-reported and there was no opportunity for the research team to independently verify the accuracy of responses.

Part 2 (Delphi consensus development exercise) results*

A consensus development exercise was conducted electronically with a group of experts from 16 countries. The experts answered questionnaires in three rounds (including an initial scoping round), with a facilitator providing an anonymized summary of responses after each successive round, as well as the reasons provided for the judgments. A total of 42 participants were recruited to take part in a scoping round where they identified 65 components that they felt were essential in a cybersecurity framework. Of the 42 recruited participants, 34 ultimately completed the scoping questionnaire. They had a range of expertise, working across sectors including healthcare (N=7), government (N=7), corporate (N=6), academia (N=5), independent consultant (N=5), and development/NGO (N=4). These 65 components were grouped into six categories by the research team (N=4).

In Round 1 of the survey, participants were asked how important each of the 65 identified components were to a global cybersecurity framework on a scale of 1 to 9, with the aim of building consensus on the priority components. A total of 59 components received consensus as important elements of a global cybersecurity framework based on the responses from 33 participants.

* A full description of this exercise and the results have been published in *BMJ Innovations* http://dx.doi.org/10.1136/bmjinnov-2020-000572.

A draft cybersecurity framework was developed after a review of the 59 components that had received consensus in Round 1, alongside comments provided by the participants, and a discussion between the research team.

In Round 2, 30 participants appraised the draft cybersecurity framework. Consensus on the cybersecurity framework presented was reached following the completion of this round.

Research limitations

There are some limitations to the expert consultation, including the geographical spread of the experts. While every effort was made to include a diverse range of country experts in the research, the majority came from HICs, with 23.5 percent from middle-income countries. No input was received from low-income countries, although some of the participants had previously worked in these settings and had expert insights based on this experience. This limitation highlights the challenge of developing a global framework for cybersecurity, where there may be limited expertise in the subject area in LMICs. Further research in this area will seek to include greater participation from LMICs, where possible.

Using the research to develop a framework

Following the analysis of the state of cybersecurity globally and consensus among the experts who took part in the Delphi exercise, we developed a more comprehensive version of a global framework for cybersecurity in healthcare – the Essentials of Cybersecurity in Healthcare Organizations (ECHO) framework. The ECHO framework is outlined in detail in Section 5.

SECTION 5. DEVELOPING A GLOBAL FRAMEWORK FOR CYBERSECURITY IN HEALTHCARE

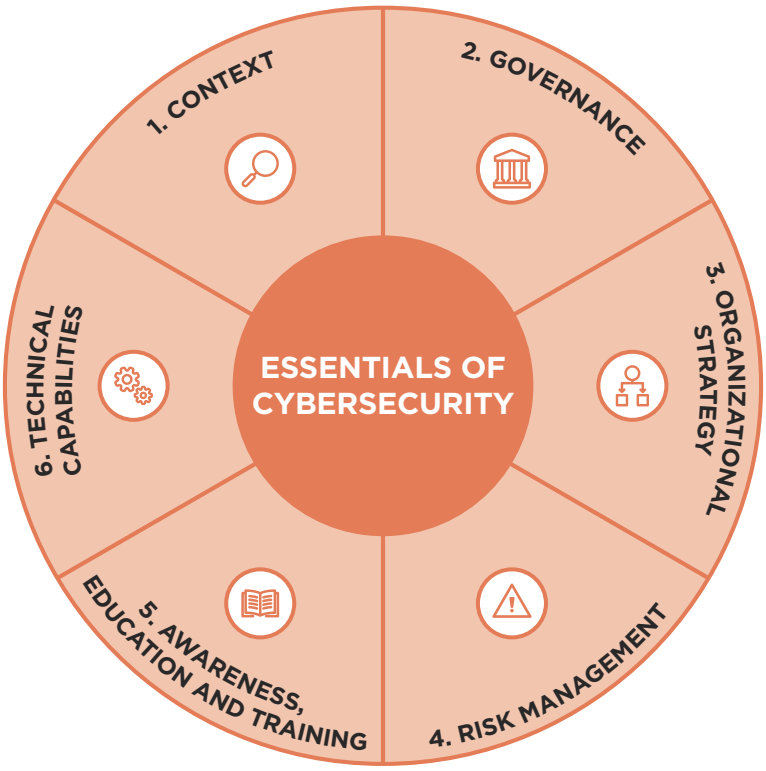
Cybersecurity frameworks

Cybersecurity frameworks are tools that are commonly adopted by organizations to promote cyber resilience and outline steps to protect themselves against cyberattacks.[59] In healthcare there are particular considerations related to patient and health data, as well as specific healthcare technologies. To better plan for cyberattacks and improve resilience, it is important to understand which data and systems need to be protected within a healthcare organization.

The ECHO framework

As outlined in Section 4, the ECHO framework in Figure 16 was developed through the expert consultation with cybersecurity, IT and health informatics professionals, alongside the research team at Imperial College London and the LHSN.

Figure 16. The ECHO framework



The ECHO framework is based on components identified by a panel of global experts as the most important elements of a global cybersecurity framework for healthcare. It outlines the six primary dimensions to consider when scaling up cybersecurity in a healthcare organization. The framework offers a common language for the essential issues that need to be addressed. It may be viewed as a 'minimum guide' or an aspirational checklist, depending on an organization's cyber maturity and resources.

Here we examine each of the ECHO framework's six dimensions in more detail.

Dimension 1. Context
Context describes the wider conditions in which the institution and its IT systems and cybersecurity operate. Context takes into account the social and cultural aspects in determining the best way to introduce cybersecurity measures, as well as considerations related to available financial resources and the maturity of the IT and cybersecurity landscape.
Staff members' willingness to adopt cybersecurity elements
IT systems' maturity level
Cultural factors and norms that undermine or promote security
Implementation costs (eg financial, human resources)

Context is the first dimension of the ECHO framework. Cybersecurity planning must be developed in such a way that it is feasible and sustainable. Considering the components listed for 'Context' will help to develop planning that can be financially achieved and sustained, that is responsive to the organization's maturity level, and acceptable and implementable to stakeholders across the organization, including frontline staff.

Dimension 2. Governance
Governance describes policies and protocols to reduce the threat of cyberattacks on IT systems by implementing cybersecurity. Often governance exists at multiple levels – regional, national and local – and requires engagement from multiple participants, internal and external to the organization.
Incident communication plan
Health/clinical information standards
Communication of threats to stakeholders
Clinical safety assessment process
National and local legislative requirements (eg ISO 27001, CREST, NIST, General Data Protection Regulation)
Appropriate 'work from home' policy, as well as 'bring your own device' (BYOD) policy
Best practice guides

Technical governance
Medical device standards
System and organization controls (SOC)-2/Pen test criteria
Firewall protocols

Dimension 2 highlights the importance of the governance landscape that each healthcare organization operates in. There are national and local legislative requirements that must be considered in the scale-up of cybersecurity, alongside technical governance that is unique to the health sector (such as medical device standards). Organizations should also seek to develop their own governance to ensure that threats and incidents are communicated effectively at board level.

Dimension 3. Organizational strategy
Organizational strategy describes policies, planning and the allocation of responsibility for IT and cybersecurity at organization level. Organizational strategy must take into account contextual considerations and relevant governance requirements.
Business continuity plan (eg clinical incident response plan, automatic backup of data)
Organizational cybersecurity strategy (eg responsibility and ownership assignment, balancing power, risk management framework)
Appropriate budgets for cybersecurity improvement
Communications strategy related to cybersecurity
Cybersecurity as a regular item discussed at board level
Multidisciplinary Security Steering Group within the organization
Procurement strategy (for systems and technology) to support cybersecurity

The third dimension of the framework outlines key areas of organizational strategy that should be developed to guide cybersecurity planning and sustainability. It is essential to have buy-in at the strategic level within healthcare organizations. Therefore, it is highly recommended that cybersecurity be addressed at board or senior management level, with a business continuity plan. Ensuring proper oversight for cybersecurity within the organization is essential for sustaining its effectiveness and success.

Dimension 4. Risk management
Risk management describes the process of identifying, assessing and mitigating threats to the organization's IT systems and cybersecurity. The section below relates to identification, assessment and mitigation of risk where possible, though many of the components extend across these areas.
Identifying risk
Monitor evolving risk landscape (threat detection)
Phishing detection and prevention
Asset identification and management (an asset is any data, device or other component that supports information transfer)
Data and network mapping
Identification of dependencies on entire supply chain and other partners
Assessing risk
Risk assessment/vulnerability identification (including on third-party suppliers, Internet of Things (IoT) and identifying outdated/unpatched devices)
Lessons learned/root cause analysis appraisals of cyber incidents
System audits (either automated or by auditors)
Mitigating risk
Systems network monitoring, logging and alerting (eg updating a comprehensive list of vulnerabilities)
Development of emergency processes (acknowledging what may not be financially possible and how to mitigate such a risk)
Internal risk management (including interoperability)
External risk management (including interoperability)
Scenario planning/simulation (simulation exercise to practice a significant cyber event/attack)
Third-party audit of controls (external assessment of cybersecurity processes)

Risk management is the broadest dimension of the framework, as it covers identifying, assessing,and mitigating risk in the context of cyber-security. Work is needed across each of these areas to monitor the risk landscape, detect possible threats, assess the importance of each risk and identify any lessons learned from previous incidents. Organizations must also ensure that systems and processes are developed and maintained to minimize risk. Risk management in the context of cybersecurity in health-care is ever evolving, as constant innovation in healthcare solutions and technologies bring about new risk profiles.

Dimension 5. Awareness, education and training
Education/training and awareness describes the actions that should take place to ensure that all stakeholders within the organization (including staff and patients) have at least a basic knowledge of the role of IT and cybersecurity in patient safety, and how to raise any concerns. Those with cybersecurity responsibilities should be adequately trained.
Employee engagement and cyber awareness raising
Measures to ensure that only appropriately trained and qualified individuals are given cyber responsibilities
Technical staff training, with minimum cyber literacy requirements for staff
Provision of material/resources outlining regulations, best practices and reporting systems in place

Education, training and awareness is another crucial element of scaling up cybersecurity, as an organization's cybersecurity is only as strong as its employees' skills and motivation. Dimension 5 outlines the key areas of education, training and awareness that should be considered to prepare staff adequately to manage cybersecurity threats relevant to their role. Such education, training and awareness may be implemented in a variety of ways, but should include clear, easily accessed information for all staff. Cybersecurity should not only be a consideration for IT departments, but should involve all staff across the organization.

Dimension 6. Technical capabilities
Technical capabilities describes the range of technical requirements needed to safeguard cybersecurity. Technology in this context should be designed to support, not hinder, the delivery of care. Depending on the contextual considerations (eg organizational needs, available budget, and so on), the following technical requirements may act as a guideline of minimum core requirements or may be an aspirational list to work toward.
Access control (based on principles to minimize the risk of unauthorized access)
Passwords/authentication – Domain-based Message Authentication, Reporting and Conformance (DMARC)/identity management/multi-factor authentication
Secure mobile devices and medical devices (including diagnostic modalities)
Technologies for threat detection and processes that send alerts
Regular patching and software updates
Data encryption
Network segmentation (improves security and performance by dividing a computer network into smaller parts to better control how traffic flows across the network)
Appropriate anti-malware/anti-virus and firewalls
Data anonymization (eg for data extracts for research)

Checklist with minimum hardware and software requirements for technology to manage patient information
Gateway security (a type of security solution that prevents unsecured traffic, including viruses/malware, from entering an organization's internal network)
Cloud capability (and standards) to ensure better security

The sixth dimension of the ECHO framework relates to organizations' technical capabilities and their relationship to cybersecurity. These capabilities will vary widely across healthcare institutions. It is therefore important that components within this dimension are not considered in isolation but used alongside one another to build a robust cybersecurity culture in the organization. The components of dimension 6 highlight the key areas to consider in scaling up cybersecurity through appropriate technical capabilities.

Using the ECHO framework

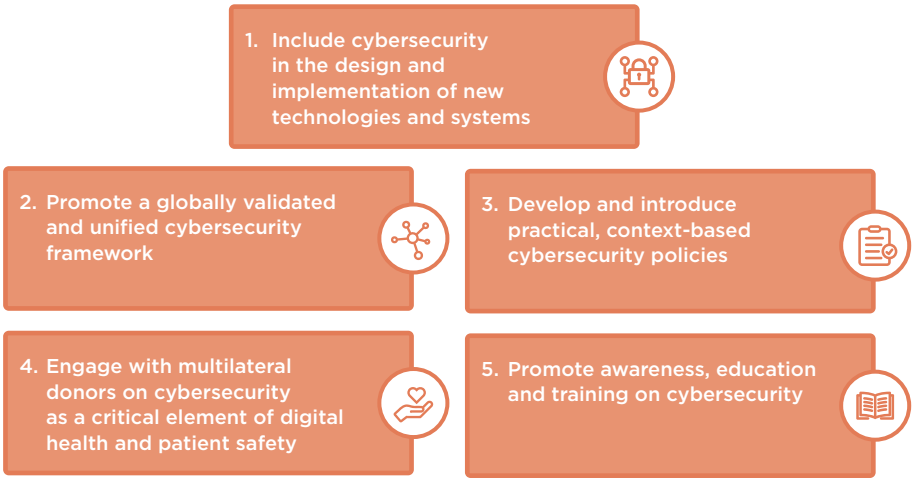
Some technical components are intentionally omitted – for example, artificial intelligence. As already noted, the framework is not intended to be a mandated checklist for institutions, but rather a guide that is applicable for healthcare organizations globally. Organizations with advanced technical capabilities should use the principles of governance and risk management to guide the full list of technical capabilities that they must consider as part of their cybersecurity. The ECHO framework may act as a 'minimum guideline' in this context. Organizations with less advanced technical capacity should also consider the framework as a minimum guideline, but one to aspire to, depending on the context and needs of the organization.

SECTION 6. POLICY RECOMMENDATIONS

This report offers insight into the current state of cybersecurity across a diverse range of healthcare settings worldwide. It highlights the current challenges and opportunities that healthcare systems face in realizing effective cybersecurity as a core element of patient safety.

While the ECHO framework offers a starting point for global healthcare providers to consider and promote cyber resilience across all settings, further steps are needed to cement cybersecurity readiness for the future. These are shown in Figure 17, and outlined below as our proposed recommendations to safely improve the use of health data and systems for patient safety.

Figure 17. Building blocks to cement cybersecurity readiness



1. **Include cybersecurity in the design and implementation of new technologies and systems**

As countries seek to strengthen health systems through digitization, cybersecurity should be included in the design and implementation of technologies and systems. At national level, appropriate governance and regulation specifically related to cybersecurity in healthcare (such as medical device standards) can help to ensure that best practice is followed at local level. At organizational level, responsibility for overseeing cybersecurity should be designated to individuals with a minimum level of literacy about cyber threats and solutions.

2. **Promote a globally validated and unified cybersecurity framework**

The readiness framework presented in this report has been designed to be used across all settings – high-, low– and middle-income countries – and introduces a common language as a first step. At the national level, a global cybersecurity framework should be incorporated in high-level policy guidance. At institutional level, a framework should guide the development and sustainability of cybersecurity planning. The next step is to validate the framework globally, which will require strong partnerships to conduct research across institutions and their different contexts to help refine the recommendations.

3. **Develop and introduce practical, context-based cybersecurity policies**

Any cybersecurity actions or policies need to be risk-based and practical, to appropriately mitigate risks while balancing resource requirements. Top-down priority setting by governments should be accompanied by the building of cyber awareness from the bottom up, with basic technical interventions and systems that do not require vast resources. Different organizations can then assess whether cybersecurity interventions are cost-effective, based on local context and resources.

4. **Engage with multilateral donors on cybersecurity as a critical element of digital health and patient safety**

It is essential that financial and human resources are readily available to scale up efforts globally. This is especially important in LMICs, which may require support in establishing sustainable cybersecurity practices and technical expertise. At national level, Ministries of Health and Finance should discuss priority setting for the development of technical capacity within their governance structure and the introduction of appropriate health technology in healthcare organizations. They should also encourage donors to include aspects of security, resilience and technical capacity building. At organizational level, the importance of cybersecurity should be prioritized as part of a wider IT strategy, acting as a catalyst to ground-level advocacy for cybersecurity within global health investment.

5. **Promote awareness, education and training on cybersecurity**

Awareness of the importance of cybersecurity is important at all levels of healthcare – from patient engagement with the topic, to front-line workers understanding how cyber hygiene can be incorporated within their job function, to health and policy planners recognizing

the importance of cybersecurity to their organization and the wider health system. At national level, expertise should be sought to develop a national curriculum of cybersecurity in healthcare. At organizational level, resources on cybersecurity should be available to all staff and a culture of awareness should be championed.

Digital solutions have the potential to revolutionize healthcare and improve the health of people around the globe, but it is essential that we mitigate the accompanying risk of cyber threats. We hope that the ECHO framework and these recommendations help to guide policymakers and healthcare organizations in strengthening their cybersecurity infrastructure and, ultimately, protecting their patient populations.

GLOSSARY

Cyber
Related to computers, information technology, and virtual reality.

Cyberattack
Malicious attempts to damage, disrupt or gain unauthorized access to computer systems, networks or devices, via cyber means.

Cyber incident
A breach of a system's security policy in order to affect its integrity or availability, or to attempt to gain unauthorized access to a system.

Cyber maturity
The level an organization has achieved in its ability to protect its information assets against cyber threats.

Cyber readiness
A state of preparedness or ability to act against cyberattacks.

Cyber threat
An act or possible act that intends to steal data (personal or otherwise), harm data, or cause some sort of digital harm.

Cybersecurity
The practice of protecting data, systems, networks and programs from cyberattacks.

Data
Individual units of information collected together for reference or analysis.

Data breach
The intentional or unintentional release of secure or private/confidential information to an untrusted environment.

eHealth
Healthcare supported by electronic processes in general.

Exploit
May refer to software or data that takes advantage of a vulnerability in a system to cause unintended consequences.

Hacking

Gaining unauthorized access to data in a system or computer.

(Organizational) leadership

May include a board of directors, steering committee or other group of leaders within the institution.

Malware

Can be used to steal data, monitor machine usage or control devices, but almost always requires that an authorized user, mistakenly or otherwise, installs the program onto their machine.

mHealth

Healthcare solutions that use mobile telecommunication technology and personal mobile devices (eg smartphones and tablets).

Phishing

A particular type of email scam, whereby victims are targeted from seemingly genuine persons or services, with the aim of tricking the recipient into either providing personal details or clicking on something that will allow the attacker to do something the user may not be aware of, such as stealing credentials or installing malware.

Ransomware

Malicious software that makes data or systems unusable until the victim makes a payment.

Reporting mechanisms

Systems that enable the reporting of suspected or actual incidents of concern.

Security by design

IT and software that has security built at the foundation.

Sensitive information

Information or data that must be guarded from unauthorized access and unwarranted disclosure to maintain the information security of an individual or organization.

ACKNOWLEDGMENTS

This report was led by Dr Saira Ghafur (Lead for Digital Health) and written by Niki O'Brien (Policy Fellow in Global Health), Dr Emilia Grass (Cyber Security Fellow) and Mr Guy Martin (NIHR Clinical Lecturer), all from the Institute of Global Health Innovation, Imperial College London. We would like to thank Dr Mike Durkin, Institute of Global Health Innovation, Imperial College London for his leadership on the LHSN and his contributions to the report.

We would further like to thank the following individuals and institutions for their contributions to the research (alphabetically):

Individuals

- Saif Abed
- Ali Alidina
- Denise Anderson
- Hutan Ashrafian
- Mikel Bermudez
- Anselmo Bonservizzi
- Adalberto Campos Fernandes
- Deeph Chana
- Stefano Dalmiani
- Rachel Dunscombe
- Anura Fernando
- Clarissa Gardner
- Donika Gjigolli
- Nicolas Gonzalez
- Chris Hankin
- Richard Harrison
- William Humphreys
- Samuel Kibet Keter
- Anthony Kitzelmann
- Ramin Kouzehkanani
- Sabrina Ching Yuen Luk
- Cal Marcoux
- Andrei Migatchev
- Onesmus Mugendi Mwaniki
- Ana Luísa Neves

- Liang-Chi Nien
- Yen-Chien Pan
- Koldo Piñera Elorriaga
- Richard Preece
- Vartan Sarkissian
- Arvind Sivaramakrishnan
- Alin Ungureanu
- Sam Wambugu
- John Williams
- Beau Woods

Organizations

- African Healthcare Federation
- Apollo Hospitals
- Basque Foundation for Health Innovation and Research (BIOEF)
- Changi General Hospital
- Foreign & Commonwealth Office, UK
- Hamad Medical Corporation
- Hong Kong Hospital Authority
- Imperial College Healthcare NHS Trust
- Institut national d'excellence en santé et en services sociaux (INESSS), Quebec
- Institute of Global Health Innovation, Imperial College London
- Joint Commission of Taiwan
- Ministère de la Santé et des Services sociaux (MSSS), Quebec
- Riphah Institute of Healthcare Improvement & Safety (RIHIS)
- Uganda Protestant Medical Bureau
- Waitematā District Health Board
- World Bank

Any errors or omissions remain the responsibility of the authors.

We would like to thank the WISH team for their support and guidance in preparing this report: Nicolette Davies and Gianluca Fontana, Institute of Global Health Innovation, Imperial College London.

REFERENCES

1. World Health Organization. *Draft Global Strategy on Digital Health 2020–2024*. Geneva: WHO; 2020. www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf?sfvrsn=f112ede5_42 [accessed 13 August 2020].

2. World Health Organization. *Draft Global Strategy on Digital Health 2020–2024*. Geneva: WHO; 2020. www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf?sfvrsn=f112ede5_42 [accessed 13 August 2020].

3. National Health Service. *The NHS Long Term Plan*. London: National Health Service; 2019. www.longtermplan.nhs.uk/wp-content/uploads/2019/08/nhs-long-term-plan-version-1.2.pdf [accessed 13 August 2020].

4. Ghafur S, et al. *Improving Cyber Security in the NHS*. London: Institute of Global Health Innovation, Imperial College London; 2019. www.imperial.ac.uk/media/imperial-college/institute-of-global-health-innovation/Cyber-report-2020.pdf [accessed 13 August 2020].

5. World Economic Forum. *Health Systems Leapfrogging in Emerging Economies: From concept to scale-up and system transformation*. Geneva: World Economic Forum; 2015. http://image-src.bcg.com/Images/Health_Systems_Leapfrogging_Emerging_Economies_2015_tcm38-79789.pdf [accessed 13 August 2020].

6. Makulilo AB. Privacy and data protection in Africa: A state of the art. *International Data Privacy Law*. 2012: 2(3), P163–78.

7. Mutale W, et al. Improving health information systems for decision making across five sub-Saharan African countries: Implementation strategies from the African Health Initiative. *BMC Health Services Research.* 2013; 13 (Suppl 2), S9.

8. Wambugu S, Villella C. *mHealth for Health Information Systems in Low- and Middle-Income Countries: Challenges and opportunities in data quality, privacy, and security*. Chapel Hill, USA: MEASURE Evaluation; 2014. www.measureevaluation.org/resources/publications/tr-16-140 [accessed 13 August 2020].

9. Bahia K, Suardi S. *Connected Society: The state of mobile internet connectivity 2019*. London: GSMA; 2019. www.gsma.com/mobilefordevelopment/resources/the-state-of-mobile-internet-connectivity-report-2019/ [accessed 13 August 2020].

10. Wambugu S, Villella C. *mHealth for Health Information Systems in Low- and Middle-Income Countries: Challenges and opportunities in data quality, privacy, and security*. Chapel Hill, USA: MEASURE Evaluation; 2014. www.measureevaluation.org/resources/publications/tr-16-140 [accessed 13 August 2020].

11. Talking Medicines. *What do all these 'health'-terms actually mean?* 6 March 2017. https://talkingmedicines.com/2017/03/digital-health-terms-ehealth-mhealth-telehealth-telemedicine/ [accessed 13 August 2020].

12. National Cyber Security Centre. *What is cyber security?* www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security [accessed 13 August 2020].

13. Organisation for Economic Co-operation and Development. *Cybersecurity Policy Making at a Turning Point: Analysing a new generation of national cybersecurity strategies for the internet economy*. Paris: OECD; 2012. www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf [accessed 13 August 2020].

14. Organisation for Economic Co-operation and Development. *Cybersecurity Policy Making at a Turning Point: Analysing a new generation of national cybersecurity strategies for the internet economy*. Paris: OECD; 2012. www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf [accessed 13 August 2020].

15. Hakmeh J, Shires J. *Is the GCC Cyber Resilient?* London: Chatham House; 2020. www.chathamhouse.org/publication/gcc-cyber-resilient [accessed 13 August 2020].

16. Ghafur S, et al. *Improving Cyber Security in the NHS*. London: Institute of Global Health Innovation, Imperial College London; 2019. www.imperial.ac.uk/media/imperial-college/institute-of-global-health-innovation/Cyber-report-2020.pdf [accessed 13 August 2020].

17. Świątkowska J. *Tackling Cybercrime to Unleash Developing Countries' Digital Potential*. Pathways for Prosperity Commission Background Paper Series; no. 33. Oxford: Pathways for Prosperity Commission; 2020. https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2020-01/tackling_cybercrime_to_unleash_developing_countries_digital_potential.pdf [accessed 13 August 2020].

18. Ghafur S, et al. *Improving Cyber Security in the NHS*. London: Institute of Global Health Innovation, Imperial College London; 2019. www.imperial.ac.uk/media/imperial-college/institute-of-global-health-innovation/Cyber-report-2020.pdf [accessed 13 August 2020].

19. Ghafur S, et al. *Improving Cyber Security in the NHS*. London: Institute of Global Health Innovation, Imperial College London; 2019. www.imperial.ac.uk/media/imperial-college/institute-of-global-health-innovation/Cyber-report-2020.pdf [accessed 13 August 2020].

20. Tham I, et al. *SingHealth cyber attack: How it unfolded*. The Straits Times, 20 July 2018. https://graphics.straitstimes.com/STI/STIMEDIA/Interactives/2018/07/sg-cyber-breach/index.html [accessed 13 August 2020].

21. Cunningham M, Towell N. *Surgeries delayed and patient security fears after cyber attack on Victorian hospitals*. The Age, 1 October 2019. www.theage.com.au/national/victoria/surgeries-delayed-and-patient-security-fears-after-cyber-attack-on-victorian-hospitals-20191001-p52wp1.html [accessed 13 August 2020].

22. Eddy N. *Alabama hospital system DCH pays to restore systems after ransomware attack*. Healthcare IT News; 7 October 2019. www.healthcareitnews.com/news/alabama-hospital-system-dch-pays-restore-systems-after-ransomware-attack [accessed 13 August 2020].

23. Miles R. *Life Healthcare announces cyberattack*. Intelligent CISO, 11 June 2020. www.intelligentciso.com/2020/06/11/life-healthcare-announces-cyberattack/ [accessed 13 August 2020].

24. World Health Organization. WHO reports fivefold increase in cyber-attacks, urges vigilance (press release), 23 April 2020. Geneva: World Health Organization; 2020. www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance [accessed 13 August 2020].

25. 2019 Public-Private Analytic Exchange Program. *A Lifeline: Patient Safety & Cybersecurity: Vulnerabilities of health information technology systems*. Washington DC: Department of Homeland Security, Office of Intelligence & Analysis, and the Office of the Director of National Intelligence. 2019. www.dhs.gov/sites/default/files/publications/ia/ia_vulnerabilities-healthcare-it-systems.pdf [accessed 13 August 2020].

26. Ghafur S, et al. A retrospective impact analysis of the WannaCry cyberattack on the NHS. *npj Digital Medicine*. 2019: 2(98).

27. Eddy M, Perlroth N. *Cyber attack suspected in German woman's death*. The New York Times, 18 September 2020. www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html [accessed 13 August 2020].

28. World Health Organization. *Global Spending on Health: A world in transition*. Geneva: WHO; 2019. www.who.int/health_financing/documents/health-expenditure-report-2019.pdf?ua=1 [accessed 13 August 2020].

29. Ghafur S, et al. *Improving Cyber Security in the NHS*. London: Institute of Global Health Innovation, Imperial College London; 2019. www.imperial.ac.uk/media/imperial-college/institute-of-global-health-innovation/Cyber-report-2020.pdf [accessed 13 August 2020].

30. Martin G, et al. Cybersecurity and healthcare: How safe are we? *BMJ*. 2017: 358, j3179.

31. National Institute of Standards and Technology (NIST). NIST Releases Version 1.1 of its Popular Cybersecurity Framework. NIST; 16 April 2018 (updated 16 January 2020). www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework [accessed 13 August 2020].

32. International Telecommunication Union (ITU). *Global Cybersecurity Index (GCI) 2018.* Geneva: ITU; 2018. www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf [accessed 13 August 2020].

33. Alshammari TS, Singh HP. Preparedness of Saudi Arabia to defend against cyber crimes: An assessment with reference to anti-cyber crime law and GCI index. *Archives of Business Research*, 2018: 6(12), P131–146.

34. Cyber Essentials. *About cyber essentials*. www.cyberessentialsonline.co.uk/about-cyber-essentials/ [accessed 13 August 2020].

35. NHS Digital. *Data Security and Protection Toolkit*. www.dsptoolkit.nhs.uk/ [accessed 13 August 2020].

36. IT Governance. *The DSP (Data Security and Protection) Toolkit*. www.itgovernance.co.uk/healthcare/dsp-toolkit [accessed 13 August 2020].

37. DeNisco Rayome A. *Does your organization need NIST, CSC, ISO, or FAIR frameworks? Here's how to start making sense of security frameworks*. TechRepublic. 7 March 2019. www.techrepublic.com/article/how-to-choose-the-right-cybersecurity-framework/ [accessed 13 August 2020].

38. DeNisco Rayome A. *Does your organization need NIST, CSC, ISO, or FAIR frameworks? Here's how to start making sense of security frameworks*. TechRepublic. 7 March 2019. www.techrepublic.com/article/how-to-choose-the-right-cybersecurity-framework/ [accessed 13 August 2020].

39. DeNisco Rayome A. Does your organization need NIST, CSC, ISO, or FAIR frameworks? Here's how to start making sense of security frameworks. *TechRepublic*. 7 March 2019. www.techrepublic.com/article/how-to-choose-the-right-cybersecurity-framework/ [accessed 13 August 2020].

40. DeNisco Rayome A. *Does your organization need NIST, CSC, ISO, or FAIR frameworks? Here's how to start making sense of security frameworks*. TechRepublic. 7 March 2019. www.techrepublic.com/article/how-to-choose-the-right-cybersecurity-framework/ [accessed 13 August 2020].

41. 2019 Public-Private Analytic Exchange Program. *A Lifeline: Patient Safety & Cybersecurity: Vulnerabilities of health information technology systems*. Washington DC: Department of Homeland Security, Office of Intelligence & Analysis, and the Office of the Director of National Intelligence. 2019. www.dhs.gov/sites/default/files/publications/ia/ia_vulnerabilities-healthcare-it-systems.pdf [accessed 13 August 2020].

42. Peter AS. Cyber resilience preparedness of Africa's top-12 emerging economies, *International Journal of Critical Infrastructure Protection*, 2017: 17, P49–59.

43. Global Partners Digital. *Multistakeholder Approaches to National Cybersecurity Strategy Development*. London: Global Partners Digital; 2018. www.gp-digital.org/wp-content/uploads/2018/06/Multistakeholder-Approaches-to-National-Cybersecurity-Strategy-Development.pdf [accessed 13 August 2020].

44. Global Partners Digital. *Multistakeholder Approaches to National Cybersecurity Strategy Development*. London: Global Partners Digital; 2018. www.gp-digital.org/wp-content/uploads/2018/06/Multistakeholder-Approaches-to-National-Cybersecurity-Strategy-Development.pdf [accessed 13 August 2020].

45. International Telecommunication Union (ITU). *Global Cybersecurity Index (GCI) 2018.* Geneva: ITU; 2018. www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf [accessed 13 August 2020].

46. Rwanda Ministry of Health. National Cyber Security Policy. March 2015. www.minict.gov.rw/fileadmin/Documents/National_Cyber_Security_Policy/Rwanda_Cyber_Security_Policy_01.pdf [accessed 13 August 2020].

47. Royal Australian College of General Practitioners (RACGP). *Computer and Information Security Standards: For general practices and other office-based practices* (Second Edition). East Melbourne: RACGP; 2013. www.racgp.org.au/FSDEDEV/media/documents/Running%20a%20practice/Practice%20standards/Computer-and-information-security.pdf [accessed 13 August 2020].

48. Martin G, et al. Cybersecurity and healthcare: How safe are we? *BMJ*. 2017; 358, j3179.

49. Hakmeh J, Shires J. *Is the GCC Cyber Resilient?* London: Chatham House; 2020. www.chathamhouse.org/publication/gcc-cyber-resilient [accessed 13 August 2020].

50. Catota FE, et al. Cybersecurity education in a developing nation: The Ecuadorian environment. *Journal of Cybersecurity*. 2019: 5(1), P2057–2085.

51. Gercke M. *Understanding Cybercrime: A guide for developing countries*. Geneva: International Telecommunication Union; 2011. www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU_Guide_A5_12072011.pdf [accessed 13 August 2020].

52. Salamzada K, Shukur Z, Bakar MA. A framework for cybersecurity strategy for developing countries: Case study of Afghanistan. *Asia-Pacific Journal of Information Technology and Multimedia*, 2015: 4(1), P1–10.

53. Global Cyber Security Capacity Centre. *Cybersecurity Capacity Maturity Model for Nations (CMM)* Revised Edition. Oxford: Oxford Martin School, University of Oxford; 2016. https://cybilportal.org/wp-content/uploads/2020/05/CMM-revised-edition_09022017_1.pdf [accessed 13 August 2020].

54. eDelphi.org. *eDelphi 2020*. www.edelphi.org/ [accessed 13 August 2020].

55. Global Cyber Security Capacity Centre. *Cybersecurity Capacity Maturity Model for Nations (CMM)* Revised Edition. Oxford: Oxford Martin School, University of Oxford; 2016. https://cybilportal.org/wp-content/uploads/2020/05/CMM-revised-edition_09022017_1.pdf [accessed 13 August 2020].

56. Global Cyber Security Capacity Centre. *Cybersecurity Capacity Maturity Model for Nations (CMM)* Revised Edition. Oxford: Oxford Martin School, University of Oxford; 2016. https://cybilportal.org/wp-content/uploads/2020/05/CMM-revised-edition_09022017_1.pdf [accessed 13 August 2020].

57. Ghafur S, et al. *Improving Cyber Security in the NHS*. London: Institute of Global Health Innovation, Imperial College London; 2019. www.imperial.ac.uk/media/imperial-college/institute-of-global-health-innovation/Cyber-report-2020.pdf [accessed 13 August 2020].

58. Global Cyber Security Capacity Centre. *Cybersecurity Capacity Maturity Model for Nations (CMM)* Revised Edition. Oxford: Oxford Martin School, University of Oxford; 2016. https://cybilportal.org/wp-content/uploads/2020/05/CMM-revised-edition_09022017_1.pdf [accessed 13 August 2020].

59. Martin G, et al. Cybersecurity and healthcare: How safe are we? *BMJ*. 2017; 358: j3179.

WISH RESEARCH PARTNERS

WISH gratefully acknowledges the support of the Ministry of Public Health

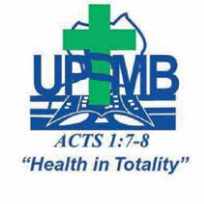

مؤسسة قطر
Qatar Foundation
WISE


مجلس قطر
للمباني الخضراء
QATAR GREEN
BUILDING COUNCIL
عضو في مؤسسة قطر
Member of Qatar Foundation


RIPHAH
INSTITUTE OF HEALTHCARE
IMPROVEMENT & SAFETY


سدرة للطب
Sidra Medicine


thebmj


UPMB
ACTS 1:7-8
"Health in Totality"


UCL


W CHanGE
Center for Health and the Global Environment
UNIVERSITY of WASHINGTON | SCHOOL OF PUBLIC HEALTH


Waitemata
District Health Board
Best Care for Everyone

ISBN 978-1-9139910-3-6

www.wish.org.qa