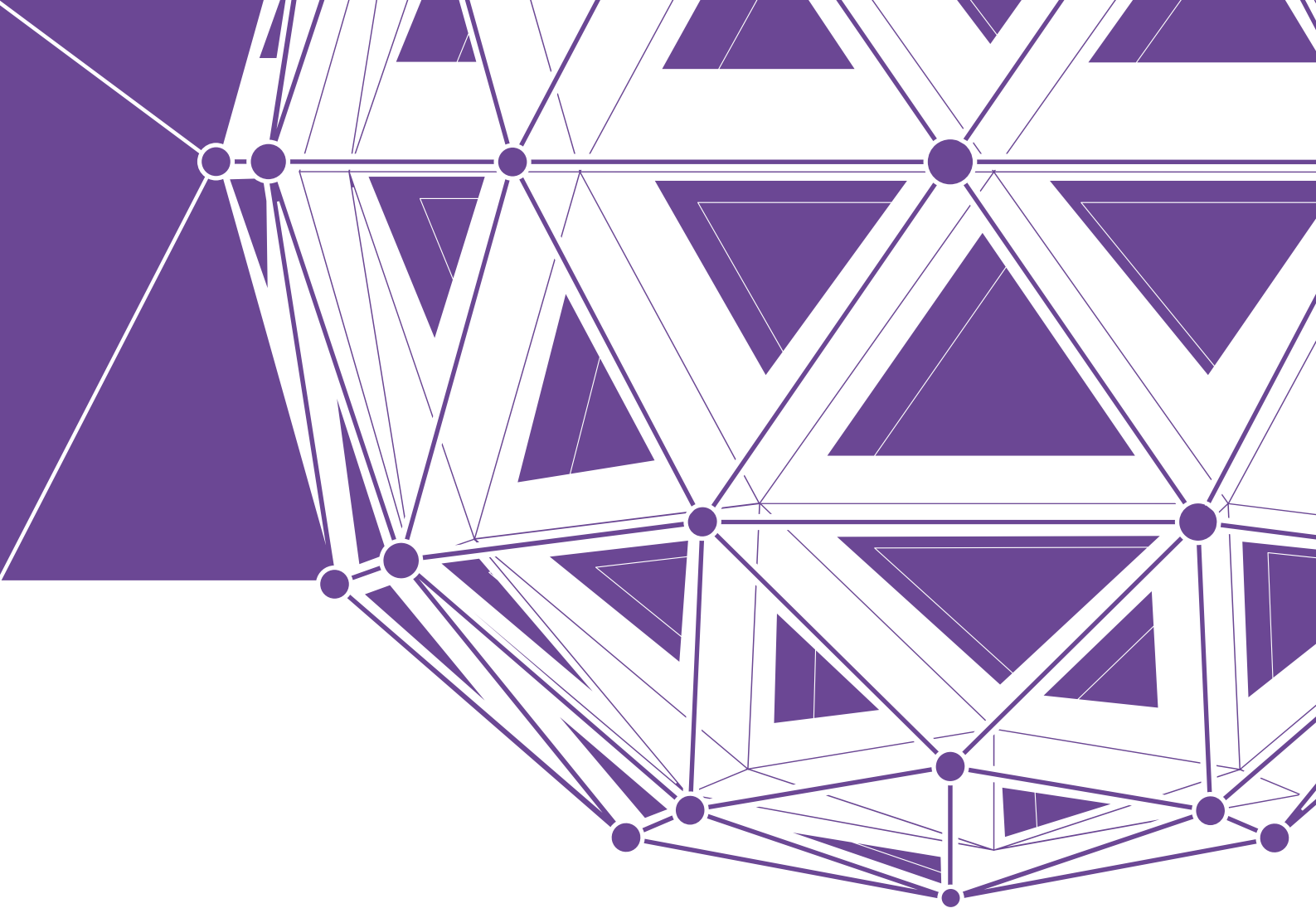


GLOBAL DIGITAL HEALTH
PARTNERSHIP

SECURING DIGITAL HEALTH

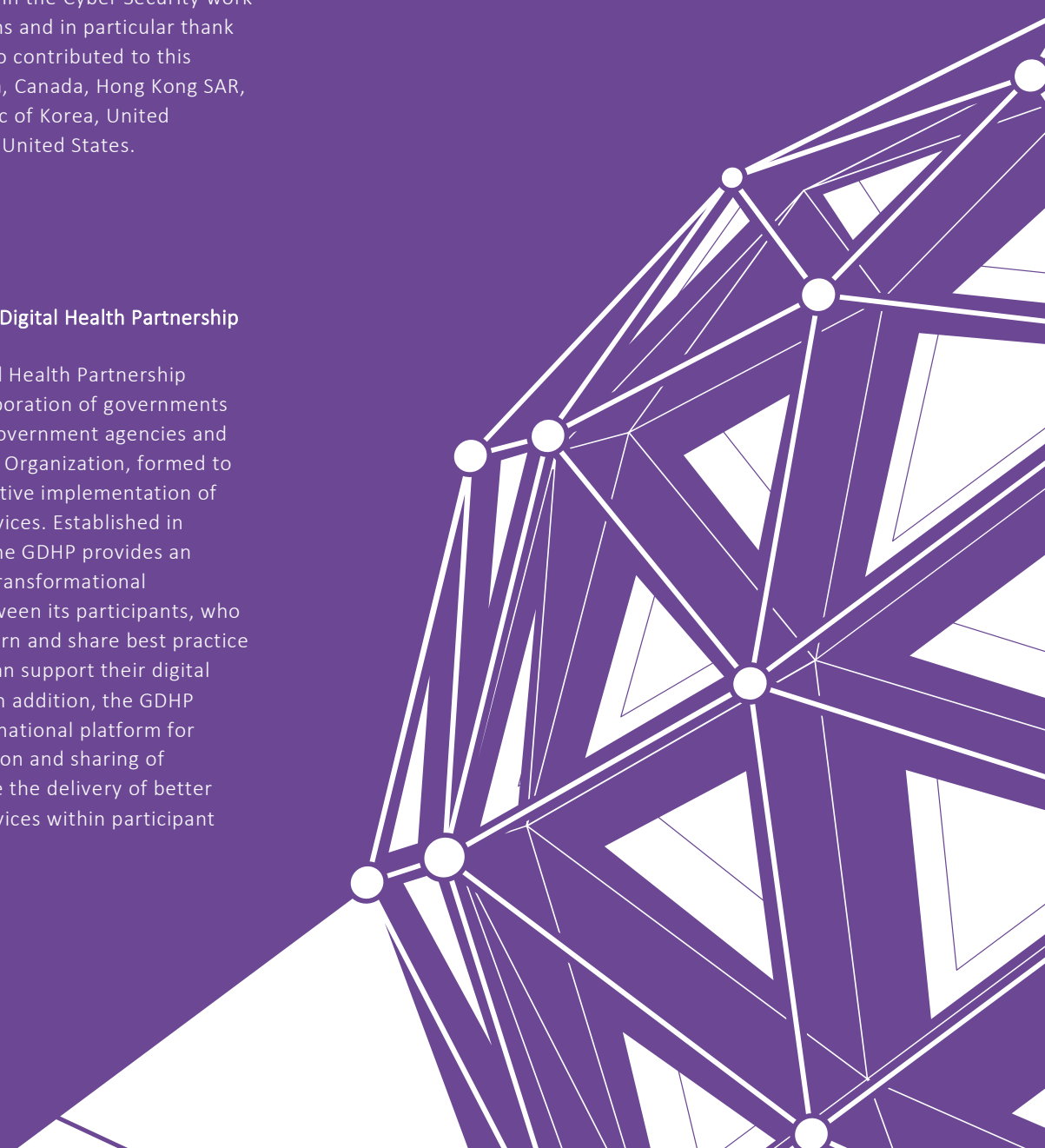
Initial reflections for steering global cyber security efforts in health

Acknowledgements

The GDHP would like to thank the Chair of this work stream, Rob Shaw (Deputy CEO, NHS Digital) and Co-Chair, Ann-Marie Cavanagh (Acting Deputy Director-General Data and Digital, Ministry of Health of New Zealand), for engaging GDHP participants in discussions, meetings and other activities to drive and develop this work. The GDHP would also like to thank member countries who participated in the Cyber Security work stream discussions and in particular thank the countries who contributed to this report – Australia, Canada, Hong Kong SAR, Portugal, Republic of Korea, United Kingdom and the United States.

About the Global Digital Health Partnership

The Global Digital Health Partnership (GDHP) is a collaboration of governments and territories, government agencies and the World Health Organization, formed to support the effective implementation of digital health services. Established in February 2018, the GDHP provides an opportunity for transformational engagement between its participants, who are striving to learn and share best practice and policy that can support their digital health systems. In addition, the GDHP provides an international platform for global collaboration and sharing of evidence to guide the delivery of better digital health services within participant countries.



GLOBAL DIGITAL HEALTH
PARTNERSHIP

SECURING DIGITAL HEALTH

Initial reflections for steering global efforts in cyber security in health

CONTENTS

NOTE FROM THE GDHP CYBER SECURITY WORK STREAM CHAIR 5

1 Executive summary 6
1.1 GDHP Background 6
1.2 Key Findings 6
1.3 Recommended next steps 7

2 Key concepts and definitions 8
2.1 GDHP Cyber security work stream 9
2.2 Cyber security working definition 9
2.3 GDHP cyber security work stream progress 10
2.4 Risk Landscape 11

3 Scope and purpose 14
3.1 Cooperation and partnership 15
3.2 How is global-level partnership and cooperation key and new? 16

4 Cyber security culture 17
4.1 Prevention and awareness 17
4.2 Controlling access 20
4.3 Cyber-attack detection and response 21
4.4 Common framework on severity of incidents 21
4.5 Traffic light protocol 22
4.6 Building cyber resilience in people, processes and technologies 23

5 Existing approaches to cyber security in healthcare organisations: examples from GDHP countries 25
5.1 Australia 25
5.2 Hong Kong 26
5.3 Netherlands 26
5.4 New Zealand 27
5.5 Portugal 27
5.6 Republic of Korea 28
5.7 United Kingdom 28
5.8 United States 29

6 Discussion 31
6.1 Wake-up call: Cyber security impacts on the provision of health care 31
6.2 Together we are safer 31
6.3 Proposed collaborative roadmap (2019–2023) 33
6.4 Real-time threat sharing advantages 35
6.5 International real-time threat sharing implementation options 35
6.6 Global digital health cert 36

7 Conclusions 37

8 References 38

9 Abbreviations 39

NOTE FROM THE GDHP CYBER SECURITY WORK STREAM CHAIR

The digital revolution presents health and care with unparalleled opportunities to increase the accuracy, precision, and efficiency of the delivery of patient and clinical outcomes and advancements. However, these opportunities also introduce hitherto unknown, unintended, and unmanaged vulnerabilities and risks from the cyber domain that can, if left unchecked, erode the potential that the digitisation of health and care brings. With the cyber threat to health and care continuously rising, the Global Digital Health Partnership brought together a number of countries to collectively and collaboratively address this most complex of problem areas.

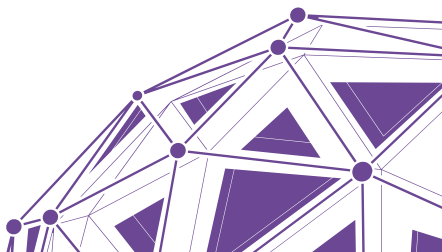
Our objective is to not only promote, but also provide, tools, mechanisms, and best practices to effectively reduce the risk of cyber-attacks and vulnerabilities. At the London summit in September 2018 we collectively agreed, among other things, on a definition of cyber security for the international health and care sector – a key building block for any meaningful collaboration to pivot off – which is as follows:

> *The means by which health care, better services, and enhanced patient outcomes are delivered and ensured through a resilient and secure digital ecosystem that encompasses culture, people, process, and technology.*

This paper applies this definition to the state of cyber security in the health and care sectors of our participating countries. It provides insight into common challenges, risk vectors, and cross-system weaknesses as well as providing a framework for managing and mitigating these concerns in a sustainable and achievable manner with example approaches from a number of participating countries.

Core to this paper is the notion that cyber security is ultimately a team sport with no national borders. Sharing of information to assist in improving the security of the health sector for GDHP participant countries has been, and continues to be, a primary focus of the Cyber Security Work Stream. This report pays significant attention to the rationale and mechanisms by which we can, and will, improve information sharing internationally.

Rob Shaw CBE
Chair
Global Digital Health Partnership Cyber Security Work Stream



1 EXECUTIVE SUMMARY

1.1 GDHP BACKGROUND

The Global Digital Health Partnership (GDHP) is an international collaboration of governments, government agencies and multinational organisations dedicated to improving the health and wellbeing of their citizens through the best use of evidence-based digital technologies. The GDHP is currently developing collaborative work divided into five work streams:

- Cyber Security
- Interoperability
- Evidence and Evaluation
- Policy Environments
- Clinical and Consumer Engagement

This document aims to consolidate cyber security work and has been developed by the Cyber Security Work Stream participants. Content was also contributed by the Lisbon GDHP Cyber workshop, enriching the document. This work stream is focused on strategies that can strengthen the processes and practices designed to protect healthcare-related devices, systems and networks, as well as the data within them, from security risks and security incidents. Effective cyber security reduces the risk of security incidents and protects organisations and individuals from the unauthorised exploitation of systems, networks and technologies, which in turn enables greater adoption of digital health technologies.

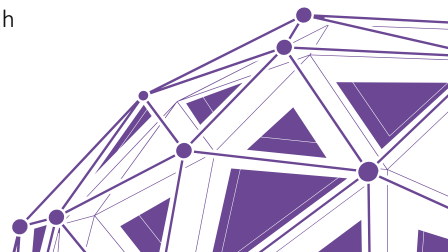
1.2 KEY FINDINGS

The key findings from this paper are:

- Many countries seek to improve the maturity of their cyber security defences in health – especially because of the importance of improving adoption of digital technology as a driver of improved quality, efficiency and disease prevention.
- There is a need to actively share information on cyber threats across international organisations.
- There is support for a coordinated international security incident response team to provide improved incident response.
- A collaborative approach is required to produce material to raise awareness and competence in cyber security.

Researching and developing this paper has highlighted many opportunities to meaningfully increase the maturity in risk-based cyber security management across the international health sector. Effective cyber security encompasses technologies, processes, and people in the broader digital health context.

Recognising information security and cyber security as value-enablers for health entities and for the health sector is key to building a relationship of trust in the health



information systems and technologies ecosystem. There are examples of good practice in the international health sector that can be shared, along with a strong desire to improve maturity.

Cyber security risks contribute to a complex and diverse risk profile that healthcare organisations must manage with appropriate responses based on local constraints and business objectives; the risks cannot be addressed in isolation. A risk-based approach to cyber security is required that encompasses the people, process and technology dimensions of organisations and their specific cyber context.

Information sharing about cyber security threats across international organisations with a similar threat context enables organisations to prepare proactively for new and emerging threats. Currently, there is minimal sharing of information related to cyber threats, and it is based on individual relationships between countries, rather than formal agreements that support fast and effective sharing of key information. The development of formal sharing agreements and protocols will increase the understanding of the cyber threat landscape and deliver the following benefits:

- improve the response to cyber security incidents
- reduce resource impacts for implementing good security processes
- support the development of a unified international view of good cyber security practices for the health sector.

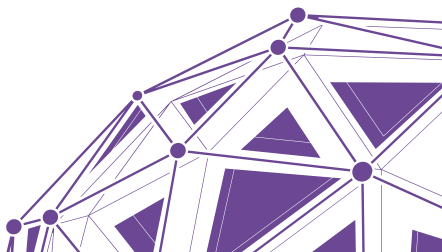
Computer security incident response teams (CSIRTs) are a key component of protecting the digital community from cyber threats. Cooperative CSIRTs can deliver improved incident response, due to a shared understanding of threats and response actions, but there is currently no united approach across the global health sector for incident response. The creation of a global CSIRT for the health sector, as agreed in the Lisbon workshop, would enable the sharing of skills and resources in an industry where there is an internationally recognised skills shortage. This would improve the ability of all GDHP participating countries to improve their cyber abilities, regardless of their current maturity, in the adoption of digital health technologies. Additional cooperation with national and sectoral bodies should also be considered because threats do not have geographical or sectoral boundaries, so neither should knowledge and information sharing.

Improving awareness and competence in cyber security is a key step towards mitigating the threats across the overall health sector. Taking a collaborative approach to developing these materials will provide more consistent messages to healthcare professionals, which in turn strengthens the message and may prove to be a more efficient use of resources for all participating countries.

1.3 RECOMMENDED NEXT STEPS

Clearly there are reasons for joining efforts in this area: heterogeneity is one, as well as opportunities for learning from best practices. The recommended next steps were updated following discussion at the Lisbon workshop. The main recommendations from this work are:

- Develop collaboration protocols for sharing ideas, information (including near-miss security incidents) and best practices on digital health cyber security.



- Collaboratively develop awareness-raising materials targeted to senior officials, ministers, and other high-profile stakeholders in the health sector.
- Promote cyber security workshops with technical experts, IT practitioners and people from the field, a cross countries and across sectors.
- Continue to work collaboratively on concrete activities within the health sector following a five-year vision that addresses a global cyber security strategy based on six dimensions:
    1. Governance and strategy organisation
    2. Prevention, education and awareness
    3. Protection measures and capacity building
    4. Response to threats
    5. Research, development and innovation
    6. Collaboration and collaborative response.
- Establish a Global Digital Health CSIRT (GDH_CSIRT) to provide a reliable, technical, hands-on process for responding to major cyber security incidents in the international healthcare sector.

2 KEY CONCEPTS AND DEFINITIONS

The vision of the Global Digital Health Partnership (GDHP) is to support governments and health system reformers to improve the health and wellbeing of their citizens through the best use of evidence-based digital technologies.

Countries around the world are making significant efforts in programs to modernise health service delivery. They face a common set of policy and delivery opportunities and challenges in realising the full benefits of digital health services and the safe, high-quality information sharing they enable. The increased use of digital health services by the main stakeholders (individuals and health professionals) provides access to information that contributes to the continuous provision of care in time, while increasing the dependence on application platforms and consequently their exposure to risks. Technology components inevitably include vulnerabilities in their design, integration, the code that runs them, or the processes with which they interact with people.

Cyber incidents and attacks are growing significantly, with more than 150 countries and 230,000 systems across sectors being affected. Consequently, this causes a substantial impact on essential services connected to the internet, including hospitals and ambulance services (1). In recent years, there has been a 70 per cent increase in these attacks on health entities. These attacks compromise the normal functioning of institutions. The increased focus of the health sector on this issue is therefore justified considering the criticality of the health sector and the type of user information stored within information systems.

Vulnerabilities of information systems coupled with growing security threats create risks. Organisations are vulnerable to attacks, data breaches, and other cyber incidents, impacting patient security. The potential impact caused by these issues should be

qualified in terms of CIA – Confidentiality, Integrity and Availability – of systems and patient data.

Thus, health organisations must understand these risks through well-defined and well-managed cyber security initiatives. Organisations should deliver a holistic vision involving the organisation, processes, people and technology.

This paper disseminates agreed recommendations and best practices on cyber security for healthcare providers and IT providers and other stakeholders in the healthcare sector, as well as advancing ways by which countries in the GDHP can cooperate in this field. An example is the establishment of the requirements for an early warning and alert system to support international collaboration of governments and government agencies in cyber security.

This paper will enable the GDHP to establish common ground on the concepts and topics of cyber security and trigger interest from high-level authorities for further international collaboration.

2.1 GDHP CYBER SECURITY WORK STREAM

The GDHP Cyber Security Work Stream focuses on strategies that can strengthen the processes and practices designed to protect healthcare-related devices, systems and networks – as well as the data within them and the people who work with them – from security risks and cyber-attacks. Strategies include the people that work and interact with these devices, systems and networks. A positive cyber security culture throughout the workforces of health and care organisations is key to delivering secure patient outcomes.

From the outset, the Cyber Security Work Stream's deliverables have focused on the following aims:

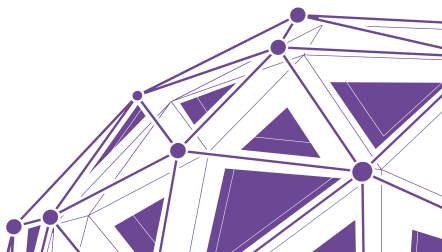
1. Developing **a network of sharing** to support participants' knowledge of cutting-edge developments and solutions, concrete experiences, lessons learned and best practice in cyber security management
2. Creating **a framework and exploring requirements for an early warning and alert system** supporting international collaboration of governments and government agencies in cyber security.

2.2 CYBER SECURITY WORKING DEFINITION

Cyber security has been defined by GDHP participants as:

> *The means by which health care, better services, and enhanced patient outcomes are delivered and ensured through a resilient and secure digital ecosystem that encompasses culture, people, process, and technology.*

Effective cyber security mitigates the risk of cyber-attacks and reduces the scale and severity of the impact caused by security incidents. It protects organisations and individuals from the unauthorised exploitation of systems, networks and technologies. Through the effective implementation of cyber security controls, digital health technologies can be adopted with significantly lower risks to the confidentiality, integrity, and availability of patient information.

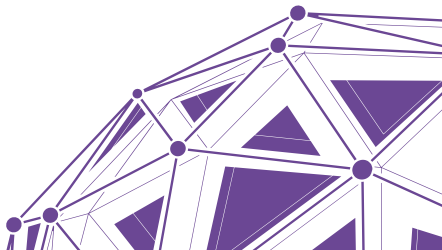


2.3 GDHP CYBER SECURITY WORK STREAM PROGRESS

Since the inaugural summit in Washington in April 2018, the Cyber Security Work Stream has delivered, and is delivering, a number of artefacts and deliverables that have been shared with all member countries. These are summarised in Table 1.

Table 1: GDHP Cyber Security Work Stream Wave One Deliverables

#	Deliverable	Description	Status
1	Cyber Security definition for health and care	The development and agreement of a recognised definition by Member States	✓ Delivered
2	Cyber Response contact details	Each Member State to provide details of relevant contacts	Ongoing
3	Cheat sheets and playbooks for Open Source Threat Intelligence collation	Artefacts to support Open Source Threat Intelligence collation across Member States	Ongoing
4	Threat advisories thresholds	Sharing of Member States definitions of threat hierarchies / ratings	✓ Delivered
5	Lessons learned documentation	Artefacts on incidents, breaches, and near-misses to be used as learning aides	✓ Delivered
6	Incident handling run-books	Documentation on Member States' best practices for incident response	✓ Delivered
7	Training materials	Sharing of best-practice training materials and syllabus	Ongoing
8	IoT Code of Conduct	Development of an agreed Code of Conduct for the use of the "internet of things" (IoT) in health and care	✓ Delivered
9	Public & private cloud guidance	Reference architecture and best-practice guidance for the secure use and deployment of private and public cloud environments	✓ Delivered
10	Secure-by-design and DevSecOps reference architecture	A common reference architectural framework for health and care	Ongoing
11	Establishment of a Cyber Technical Group	A dedicated group of specialists to support the strategic group under the workstream (see Section 6.6 for more details)	✓ Delivered
12	Collaboration space	For the joint working on documentation and artefacts between Member States	Ongoing



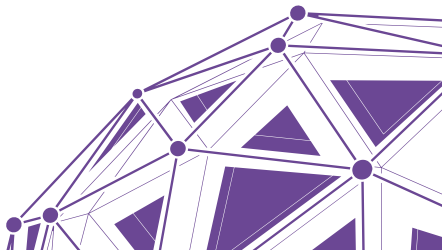
#	Deliverable	Description	Status
13	Health and care cyber alerts platform	For collaborative sharing and information gathering on cyber incidents and threats to health and care (see Section 6.5 for more details)	Ongoing
14	Baseline cyber survey	An anonymised survey to understand common strengths, challenges, and areas for enhanced cooperation	✓ Delivered
15	Cyber security foundational capabilities assessment paper	A framework and best-practices paper on the development of foundational cyber capabilities in health and care	Ongoing

Collectively, these deliverables form Wave One of the Cyber Security Work Stream's deliverables. During the workshop in Lisbon in January 2019, it was agreed that additional structure was required in order to fully realise the benefits of those deliverables that are Ongoing. These are Wave Two deliverables. These include the wrapping up of the deliverables orientated towards Threat Sharing and Collaboration into a single sub-work stream to establish a Global Digital Health Threat Sharing Platform, further details of which can be found in Section 6.5.

2.4 RISK LANDSCAPE

According to the Global Cybersecurity Index (2) in 2016, nearly one per cent of all emails sent were malicious attacks, the highest rate in recent years and expected to increase. In 2017, a significant cyber-attack caused major disruptions to companies and hospitals in over 150 countries, prompting a call for greater international cooperation. Business operation models are changing, becoming increasingly interdependent and based on digital business processes. On one hand, digital solutions allow efficiency, productivity and lower costs, but they increase exposure to risks which can compromise people's data in the healthcare sector. In addition to new challenges posed by digital transformation, health organisations already face a complex set of existing security risks from legacy systems, distributed supply chains and insider threats. Thus, cyber security in organisations must be transversal, continuously assessed and up to date. Legacy security models are no longer adequate and cyber security is now at the heart of any business building trust into the fabric of digital operations (3).

Organisations face an overarching risk if they establish a "stable" static cyber defence. The risk landscape is constantly changing, so it is key to keep continuous improvement and innovative approaches at the core of any strategy.



For context regarding the issues the healthcare industry needs to address, it is interesting to analyse the Protected Health Information Data Breach Report (PHIDBR) (4), based on the analysis of real-world events. It states that:

- Fifty-eight per cent of incidents involved insiders—health care is the only industry in which internal actors are the biggest threat to an organisation.
- Medical device hacking may create media hype but the assets most often affected in breaches are databases and paper documents.
- Ransomware is the top malware variety by a wide margin—70 per cent of incidents involving malicious code were ransomware infections.
- Basic security measures are still not being implemented—lost and stolen laptops with unencrypted protected health information (PHI) continue to be the cause of breach notifications.

2.4.1 IDENTIFIED CYBER SECURITY CHALLENGES

Cyber incidents are an increasingly frequent threat to all countries and organisations. At the Lisbon workshop, participants were asked to identify the biggest challenges they face regarding cyber security; the results of this exercise are included below. This identified a common set of challenges like human resources training and awareness, legacy in ICT and governance. It also highlighted the diverse size and nature of health systems in GDHP countries and the individual local challenges they encounter.

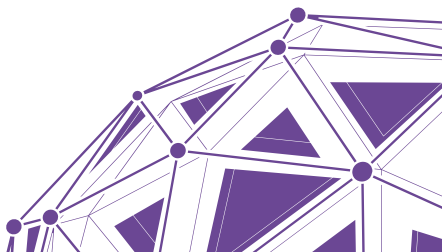
The findings from this workshop have been categorised into four key groups: People, Technology, Process and Technology/Process crossover.

People challenges:

- insufficient cyber skills and resources
- workforce cyber security skill/talent gaps
- human resources (scarcity, budget, recruitment, retaining, etc.)
- cyber features as a board-level priority
- lack of staff awareness and training
- strategic and operational-level awareness
- lack of understanding of what constitutes cyber security and how this differs from legislated privacy requirements
- low level of cyber maturity across the health sector.

Technology challenges:

- lack of encrypted traffic monitoring
- lack of local internet monitoring
- prevalence of advanced persistent threats
- ransomware and zero-day attacks
- mobile application security



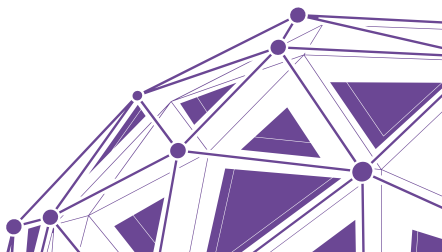
- IoT and cloud security
- emerging technologies
- cyber security engine (i.e. antivirus).

Process challenges:

- incorporating cyber security risks into existing enterprise risk management processes
- complex regulatory environment
- legacy IT, unsupported technologies, and extended IT ecosystems
- governance across a distributed health sector
- cooperation and collaboration (mostly across operational non-ICT functions)
- diverse governance processes and risk outside of jurisdictional responsibilities
- wide diversity of healthcare organisations
- managing trusted insider risk within healthcare organisations.

Technology/Process crossover challenges:

- vulnerable/exposed internet facing systems
- unpatched/legacy systems and assets
- weak/insufficient (privileged and fine grain) access management and controls
- password and credential management
- historic weakness of ICT regime.



3 SCOPE AND PURPOSE

It is important to build a relationship of trust in the extended ecosystem of surrounding health information systems and technologies to nurture cyber security conditions that:

- recognise security as an element that creates value for the health sector
- establish a strategy and model for the topics of information security and cyber security in the health sector, taking into account a holistic vision to ensure stakeholders acknowledge the situation and understand the risks and impacts.

The Cyber Security Work Stream aims to collectively develop an approach to security by learning and understanding each country's particularities and diversities. It aims to identify and develop strategies and best practices in cyber security, as it is a common threat for all participants. To pursue this goal, a framework like that in Figure 1 can serve as a good term of reference, but it should be cautiously applied when considering its adoption for a national strategy as opposed to looking at cooperative efforts between different countries who may be facing different situations.

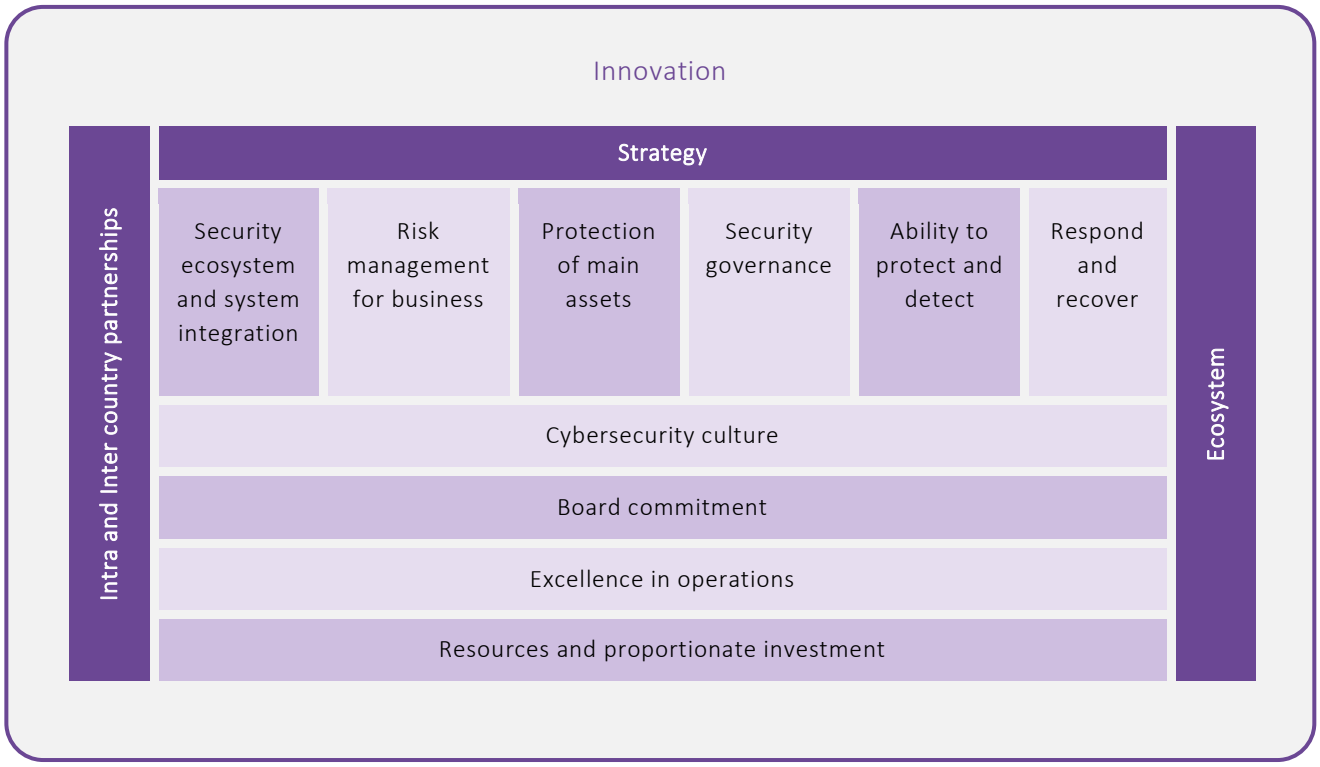


Figure 1: Cyber security framework

To foster cyber security, it is essential for organisations to implement a risk-based approach to cyber security, supported by:

- thorough identification of the organisation's vital assets comprising people, processes, locations, suppliers, systems, and data
- systematic and continuous analysis of the cyber context of the organisation – identifying vulnerabilities, threats and threat actors that pose the most risk to the organisation
- Implementation of adequate measures to protect the vital assets from the identified risks

Without knowing the organisation's context and the main risk scenarios to which it is exposed, it becomes increasingly difficult to design an effective cyber security strategy within resource and investment constraints. As experience shows, diagnosis before prescription is as true for cyber security as it is for a patient.

There are three main dimensions that should be tackled in cyber security. In order, they are people, process and technology. Currently, we often see a discourse regarding the role of managing people and process to ensure security, but in practice there is generally more investment in the area of core, hard technology than the soft skills of people including health professionals, IT professionals and patients. In addition, the silent and discrete “underground” work of defining good processes and refined frameworks for audit and continuous improvement is also rarely prioritised.

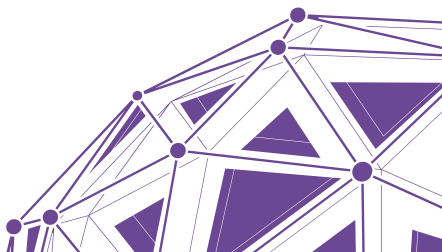
It is recommended that each GDHP participating country use a common three-layered approach to cyber security strategy focused on people, process, and technology. This would enable the mapping of all participating countries to deal with these topics and facilitate the sharing of experience about best practices.

3.1 COOPERATION AND PARTNERSHIP

The fourth dimension that is very important to include for managing security across GDHP participants is cooperation and partnership. Cooperation and partnership enable countries to map their initiatives against the initiatives of other national digital health authorities via the GDHP or other collaboration venues such as the EU eHealth Network, or joint actions such as the eHealth Action. Equally important, and perhaps even more enriching, are the collaborations with non-health agencies or bodies, from which health care can learn a lot.

Cyber security is a matter that is not specific to health. Recognising the value of establishing a spirit of national and international cooperation and synergy with others, it is important to promote and have a presence in several initiatives that allow the sharing of knowledge, trends and capabilities in this area. It is important to acknowledge that the maturity level of countries differs in cyber security matters. However, with joint efforts and common thinking, countries can strengthen their cyber security strategies at the national level and, through cooperation, countries benefit from the sharing of information about threats and about initiatives that have already been implemented.

This is more important as the interconnectedness of digital health across borders is increasing, as is the flow of patients seeking health care. The resilience of the overall system is only as strong as the weakest link in the chain.



> *Alone we can do so little, together we can do so much.*
>
> Helen Keller

Responsibility for security incidents often lies with the user as opposed to the technology. The greater the awareness of system users, the greater the overall security of the system will be (5). Lifelong sensitisation is a key factor in preserving information security and the health-cyberspace, creating a more resilient society, stimulating the development of digital skills and allowing users to understand their responsibilities in using and protecting properly the information and resources entrusted to them. As a result, cyber security can contain complex concepts, with physical and personnel security being two core concepts within the information security highlights. For example, the UK's Centre for the Protection of National Infrastructure (6) has a useful set of advice and definitions:

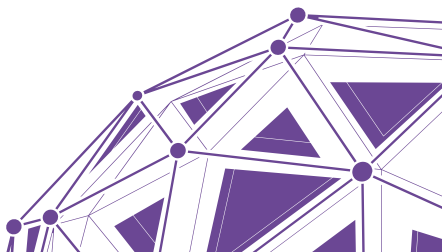
> *Personnel Security is a system of policies and procedures which seek to mitigate the risk of workers (insiders) exploiting their legitimate access to an organisation's assets for unauthorised purposes;*
>
> *People security is about shaping and controlling the environment to promote vigilance and an effective security culture, and to influence and deter those seeking to cause harm.*

3.2 HOW IS GLOBAL-LEVEL PARTNERSHIP AND COOPERATION KEY AND NEW?

In the context of cyberspace, and following the paradigm of interconnection of people, documents and machines that it predisposes, it is important to share a network of contacts in order to solve and deal with incidents of cyber security and vulnerabilities (5).

This paper focuses on the idea of security and global cooperation. It also highlights that implementing and expanding the use of digital health – efforts many countries are engaged in – can be jeopardised by cyber-attacks.

The paper lists key elements of cyber security thinking to create a common understanding between participating countries. This does not aim to be extensive but rather illustrative of the types of topics the industry is facing. It also includes a "wake-up call" on why more focused attention and energy need to be given to this by all in the digital health domain. Finally, it considers what GDHP countries can do together to work towards a solution to these issues and why more focused attention is required by all participants in the digital health domain.



4 CYBER SECURITY CULTURE

There are many aspects to cyber security. Senior responsible staff are not expected to know the technical details of, for example, how to set up an effective firewall system, an awareness campaign, or a process to ensure effective close-down of password use in a hospital organisation. They are, nonetheless, required to know that these things matter and make a big difference to how resilient healthcare organisations are.

Organisations and healthcare institutions must be aware of, and prepare their human resources to understand, the impact of their actions on patient services and their individual security responsibilities in this context. This includes providing training and creating awareness of existing threats. It is crucial to also have a responsible person and an expert team prepared to act in risk situations in addition to general staff awareness.

The objective is not to make everyone who works in the health sector a cyber security expert but to make them all aware of their responsibilities towards patients in delivering a secure service. Therefore, not to know is OK, but not to make yourself available to learn in this area, is not.

4.1 PREVENTION AND AWARENESS

The first objective in developing a prevention strategy for avoiding or mitigating cyber risks is to determine what must be protected and to document that in a recommendation that includes common threats. The recommendation must define the responsibilities of the organisation and employees while also setting responsibilities for implementation, enforcement, audit and review actions. It should also:

- identify the assets that need protection
- understand the risks that pose a threat to these assets
- understand the security obligations of the organisation
- understand the current maturity and capability of the organisation in mitigating these security risks.

Technical and Organisational Measures (TOMs) are crucial to monitoring and ensuring the adoption of recommendations. These TOMs refer to the three pillars of cyber security: **Confidentiality, Integrity and Availability**.

To ensure **Confidentiality**, there needs to be control over the access of information, restrictions on data-storing and data-transferring. Another key point in confidentiality is the elimination and destruction of information after it is no longer required.

Protecting **Integrity** relates to database access controls and making sure that data is consistent. There should be processes in place to ensure uniformity in released application versions and that software gets updated at the right time. Logging and auditing should be a core feature in every application the organisation uses. Antivirus and URL / spam filters should be in place in all the proper nodes.

Availability is about making sure all critical applications are redundant. For example, the proper cooling and humidity controls are in place in the datacentre and there is redundancy in the power supply, while also making sure the datacentre is protected against fire or flooding hazards. It is also about ensuring backup and data recovery mechanisms are in place, and suitably maintained and tested.

It is the responsibility of the organisation to train its workers. Within the organisation, controlled events like sending simulated phishing emails to workers, including senior management staff, is a simple way to spot who is in need of further training.

Auditing and continuous improvement programs go a long way to making sure TOMs are being correctly implemented. Monitoring should be a part of the process, not an afterthought.

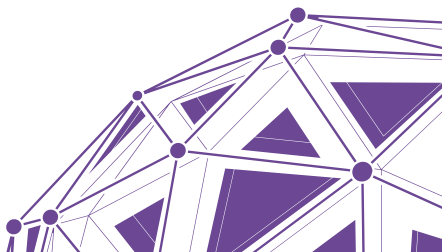
Lastly, it is fundamental to implement a holistic, structured and bespoke security process for one's organisation, with all its assets properly identified.

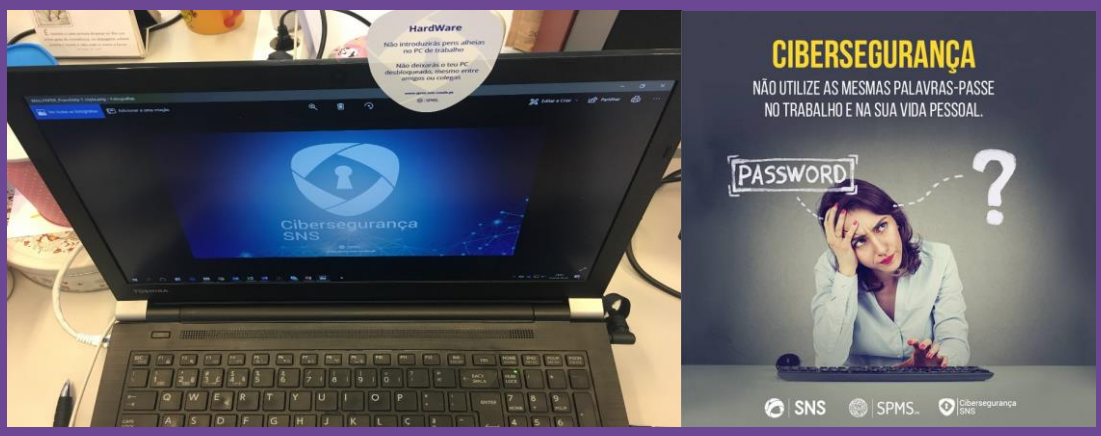
To ensure the security of the organisation, there should be two very distinct, very important kinds of people: the ones who are cyber security pros and the ones who are pro-cyber security.

A cyber security pro is an individual with a highly differentiated set of skills, typically an IT person, who understands the intricacies of the technical details. It is an individual who, in a worst-case scenario such as during a breach of the organisation's perimeter, can take effective action to control the incident. These individual skills must also include the capacity for risk management.

The profile of the pro-cyber security individual is very different. He or she is anybody who, through their day-to-day activities, is completely aware of the processes and behaviours necessary for a secure cyberspace and information system. This is someone who adopts all the necessary security measures stipulated in the organisation's policies and someone who works and contributes to them.

So, to put it in practical terms, a cyber security pro is directly involved in security activities, such as the CISO of an organisation and those working alongside them. A pro-cyber security person, on the other hand, is someone pushing cyber security awareness activities within the organisation and all those who in their daily activities act according to best practices.





Example from Portugal: *Two examples of "fun" cyber awareness. The image on the left shows the 10 commandments of cyber security in stickers which the "cyber security patrol" can use when they find a behaviour that is not correct. To the right is a simple infographic to put on the organisational intranet or, as is the case here, on the SPMS Facebook account.*

Figure 2: Cyber security awareness materials from Portugal

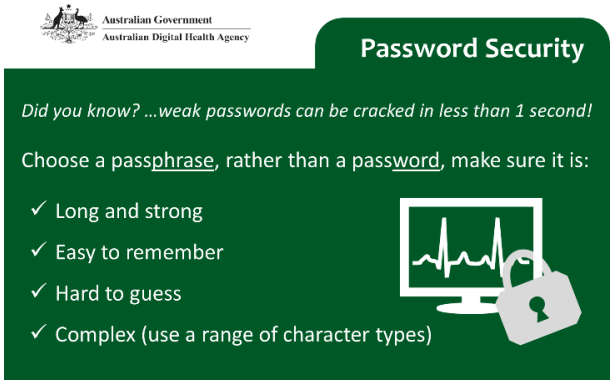


Figure 3: Security awareness materials from Australia

4.2 CONTROLLING ACCESS

In all security initiatives, ensuring who gets access to what in a legal, controllable, proportional and auditable manner is key. Privileged access management (PAM) should be a tool used to control who accesses data and the systems being accessed. PAM solutions can streamline user access (and terminate it) without making security a blocker to business objectives. All security controls should be appropriate and proportionate to the threat. An example is using PAM privileged access management as opposed to adopting disproportionate access controls across all systems. The controls should be relevant to the data and systems being accessed.

One of the underlying principles of information security relates to the concept of security rings and standard ISO 27001 of the International Organization for Standardization (ISO). Here, depending on the value of an asset more/less layers of protection must exist, thus creating the need for multiple lines of defence. The media type must be protected (from internal and external intruders) depending on the type of information it stores.

In order to effectively protect the information stored within an organisation, the information needs to be identified and appropriately classified based on the level of impact the compromise of the information would have to the organisation. Figure 4 illustrates this approach to information classification.

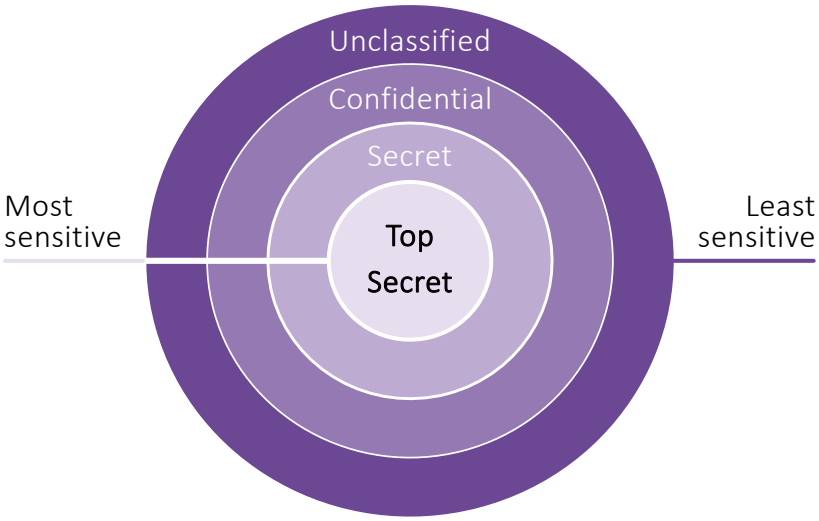


Figure 4: Information classification

Users should not have access to all systems and information. Access should be restricted and granted on a basis of their need-to-know in order to effectively perform their duties. To manage this access it is necessary to establish user accounts by issuing identifiers, authentication methods to verify these identifiers, and authorisation rules that limit access to resources.

Identification – Identification is a unique identifier. It is what a user (person, client, software application, hardware, or network) uses to differentiate itself from other users of the system.

Authentication – Authentication is the process of validating the identity of a user. When a user presents its identifier, before gaining access, the identifier (identification) must be

authenticated. Authentication verifies identities, thereby providing a level of trust. There are three basic factors used to authenticate an identity (Something you know; Something you have; Something you are).

Authorisation – Authorisation is the process of allowing users who have been identified and authenticated to use certain resources. Limiting access to resources by establishing permission rules provides for better control over users' actions. Authorisation should be granted on the principle of least privilege, granting no more privilege than is required to perform a task/job, and the privilege should not extend beyond the minimum time required to complete the task. This restrictive process limits access, creates a separation of duties and increases accountability.

4.3 CYBER-ATTACK DETECTION AND RESPONSE

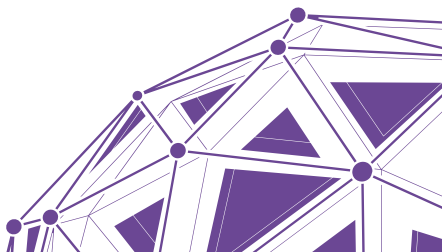
Response to an incident should be well planned, and the response plan should be written and ratified by appropriate levels of management. The most important elements of this strategy are timely detection and notification of the compromise.

A Computer Security Incident Response Team (CSIRT) should be established with specific roles and responsibilities identified.

4.4 COMMON FRAMEWORK ON SEVERITY OF INCIDENTS

The NHS Digital Data Security Centre Threat Triage Matrix provides a clear, concise, and codified framework – Triage Matrix – from which to assess and determine the severity of a given incident, threat, breach, or attack. Not only does it drive consistency in diagnosing the severity of an incident, but it also ensures that the most relevant and proportionate response process is triggered in a timely and effective manner. Perhaps this can be used more extensively among GDHP countries.

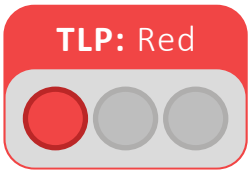
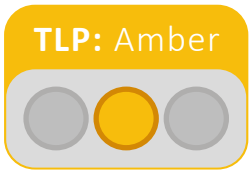
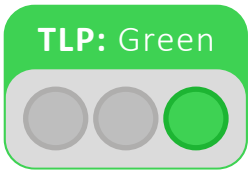
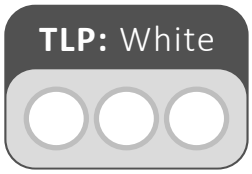
NHS Digital has also provided a "run book" for managing incidents. It includes not only the technical aspects of any incident, but also media handling, regulatory considerations, and senior decision-making aspects. Even though this artefact is currently being updated (as part of its yearly review and the latest version will be shared when ready and as appropriate) it nonetheless provides participating countries with a robust and proven national-level response process.

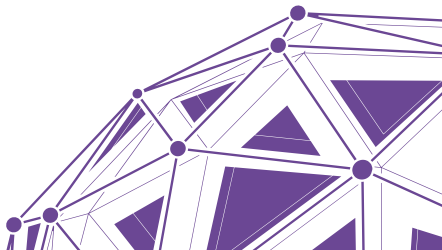


4.5 TRAFFIC LIGHT PROTOCOL

It is also important to establish a common language to facilitate greater sharing of information. Traffic Light Protocol (TLP) is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colours to indicate expected sharing boundaries to be applied by the recipient(s).

Table 2: Traffic Light Protocol (TLP) definitions

			
Not for disclosure, restricted to participants only.	**Limited disclosure, restricted to participants' organisations.**	**Limited disclosure, restricted to the community.**	**Disclosure is not limited.**
When should it be used?			
Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organisations involved.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organisations as well as with peers within the broader community or sector.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.
How may it be shared?			
Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP: RED information is limited to those present. TLP:RED should mostly be exchanged verbally or in person.	Recipients may only share TLP:AMBER information with members of their own organisation, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.	Recipients may share TLP:GREEN information with peers and partner organisations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.



4.6 BUILDING CYBER RESILIENCE IN PEOPLE, PROCESSES AND TECHNOLOGIES

Cyber resilience is about managing security using a multi-layered approach. Changing the culture around digital information, and by nurturing an appreciation for a strategy that encompasses preparation, prevention, detection, response, and recovery, organisations will gain true cyber resilience and the ability to respond and recover quickly from an attack.

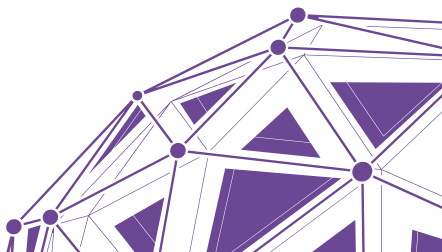
Based on Abraham Maslow's famous hierarchy of needs for self-actualisation, the framework of Forrester – Targeted-Attack Hierarchy of Needs (7) (8) – focuses on the core needs required for defending the IT environment against targeted attacks, laying the foundation for a resilient security strategy. The needs in order of importance are:

- an actual security strategy
- a dedication to recruiting and retaining staff
- a focus on the fundamentals
- an integrated portfolio that enables orchestration
- prevention
- detection and response.

Figure 5: Forrester's Targeted-Attack Hierarchy of Needs

In order to meet these needs, a secure healthcare environment must ensure:

- roles and responsibilities are clear in organisations
- the availability and integrity of services
- Critical National Infrastructure (CNI) is identified and protected
- excellent coordination of resources
- engagement with data security
- systems and situation assessment capability
- greater inter-working between national authorities on cyber incidents and organisations
- creation of a key-contact centre, equipped and staffed
- regular updates on planning
- up-to-date emergency/incident contact lists held centrally
- training and awareness
- Cyber Response Plans including communication plans (how to respond to an incident and maintain business continuity).



5 EXISTING APPROACHES TO CYBER SECURITY IN HEALTHCARE ORGANISATIONS: EXAMPLES FROM GDHP COUNTRIES

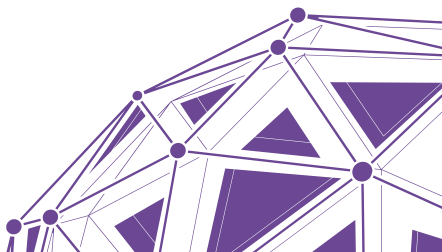
Different approaches and initiatives exist already from which GDHP countries can learn and build common thinking. The existing approaches to cyber security in healthcare organisations were updated after the Lisbon workshop. Some examples are provided here, showing the diversity that exists in the methods, but also showing the significant convergence in the objectives and final goal.

5.1 AUSTRALIA

Digital Health Cyber Security Centre

The Australian Government has created a Digital Health Cyber Security Centre within the Australian Digital Health Agency. The Australian Digital Health Agency's Cyber Security Strategy is focused on four pillars: partner, secure, inform and respond. Partner involves the cooperation with other national and international cyber organisations; secure includes the implementation of appropriate technical and non-technical security controls within the National Digital Health Infrastructure; inform is about providing the healthcare organisations that make up the healthcare sector with the knowledge and information needed to respond appropriately to cyber threats; and respond involves responding directly to cyber incidents that occur within the National Digital Health Infrastructure, and providing coordination and support during incidents throughout the healthcare sector.

The Cyber Security Centre provides operational security support for the My Health Record system, the national centralised health record summary in Australia. In addition, the Cyber Security Centre provides cyber security education and awareness support and resources for health organisations across Australia, including the provision of cyber threat alerts to assist in awareness of new and emerging cyber threats that may impact Australian healthcare organisations. During a national health sector cyber crisis, the Digital Health Cyber Security Centre coordinates the response across the sector, liaising closely with other Australian Government organisations such as the Australian Cyber Security Centre and CERT (Computer Emergency Response Team) Australia.



5.2 HONG KONG

The government of the Hong Kong Special Administrative Region has developed and maintained the information security management framework for its Bureaux and Departments with wide coverage of policies, guidelines and best practices with the aim of promoting a secure environment for conducting digital businesses and operations. The HKCERT, which is operated under the government subvented Productivity Council, coordinates cyber security incident responses, and promotes information security awareness and prevention of cyberattacks. The law enforcement agency, the Hong Kong Police Force, is responsible for all investigation and prosecution of cybercrime-related matters.

The Hospital Authority of Hong Kong

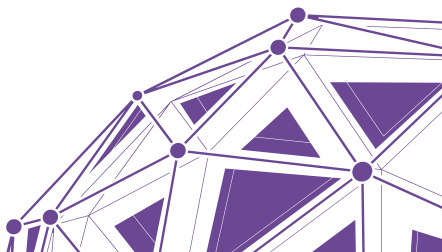
The Hospital Authority of Hong Kong is a statutory body responsible for managing public healthcare services via public hospitals, specialist outpatient clinics and general outpatient clinics. The Hospital Authority established its own information security and cyber security framework based on the aforementioned government framework and international best practices. Its overarching objective is to provide IT systems with high security over patient care services and personal data protection.

The Hospital Authority develops and operates a unified healthcare system that covers whole outpatient and in-patient treatment journeys. The Hospital Authority treats cyber security as a major cornerstone to maintain stability and availability of hospital systems and protection of patient personal data. The Hospital Authority closely collaborates with the HKCERT, Hong Kong Police Force and the corresponding government departments to establish regular forums and reporting channels to enhance cyber security protection and maintaining secure critical infrastructure in Hong Kong.

The Hospital Authority took a step forward during its digital transformation to upgrade from the existing defence-in-depth strategy to integrating cyber security into DEVOPS and the Security Operations Centre. Dedicated roles of Chief Information Security Officer and Chief Privacy Officer were created and corresponding teams were formed and charged with responsibilities to oversee IT security and privacy protection. The IT systems under the Hospital Authority are integrated and centralised to allow execution of a standardised security framework and data protection. These fine-tuned roles, integrated strategy and operation will enable the Hospital Authority to further strengthen the overall cyber security risk assessment, monitoring, detection, and response to cyber security threats and incidents. Dedicated IT security teams are being consolidated to oversee upcoming cyber security challenges and manage the transformation to improve its processes, toolkits and knowhow to build up cybersecurity capacity and uplift its cyber security resilience.

5.3 NETHERLANDS

Zorg-CERT (Z-CERT) provides a CERT service for all healthcare organisations in the Netherlands – all hospitals, specialised hospitals, and mental health institutions. Services include threat advisories, operational alerts, monitoring of specific internet locations and domain names, incident response, and facilitation of communication between the healthcare organisations. The CERT is a not-for-profit organisation that is primarily funded by its member organisations, although it has received government funding for the first two years to provide the capital required to commence operations.



5.4 NEW ZEALAND

The New Zealand Ministry of Health has a cyber security team whose role is to work with the New Zealand health and disability sector to build its cyber security maturity and resilience. The aim of this team is to build better health sector-specific cyber threat awareness, and to provide quality sector-specific guidance and resources.

Each district health board manages its IT systems individually. However, the Ministry of Health works closely with the sector to ensure all relevant information about cyber risk management is shared. If a serious cyber security event were to occur, the Ministry of Health would lead the response in accordance with the sector-wide cyber event response plan.

The Ministry of Health manages the Health Information Security Framework, which gives specific advice on actions to prevent cyber-attacks and steps that can be taken to assist with recovery after any attack.

5.5 PORTUGAL

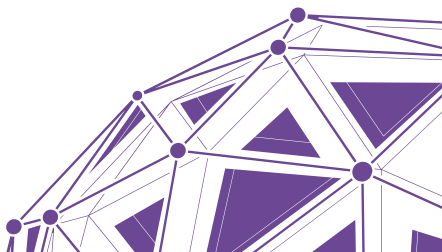
Portugal has a National Strategy for the Health Information Ecosystem focused on people, process, technology and initiatives. The ICT strategy – defined by ecosystem of health information systems (eSIS) – includes improved governance and management, strategic management, architectural management, risk and security management, innovation management, supply chain management, skills and competency management and ICT service management.

Portugal has a National CERT (CERT.PT), which is integrated in the Portuguese National Cybersecurity Cabinet (CNCS), the national body for cyber security, responsible for coordinating responses to incidents involving state entities, essential service operators, operators of national critical infrastructure and digital service providers.

In the healthcare sector, SPMS (the shared service agency of the Ministry of Health) has a strategic partnership with the Cabinet and plays an active role in the definition of the National Strategy for Cybersecurity. Specifically in relation to healthcare institutions, there are two published normative definitions that are relevant to the strategy: one regarding the establishment of a centralised Mandatory Incident Notification Model concerning security incidents; and the second establishing a governance model regarding the implementation of the health cyber security policy.

As such, the Portuguese health ecosystem shares a contact network where SPMS is responsible for receiving and centralising cyber security incidents from all other NHS institutions. This procedure guarantees that SPMS is the single contact point involved in the notification of health cyber security events to the Portuguese National Cybersecurity Cabinet.

Portugal also has a model of governance that promotes the involvement of, and sharing of responsibilities between, all parties, namely government agencies, governing bodies, health professionals, and information technology professionals. This model promotes the adoption of a holistic view of cyber security that considers the dimensions of Organisation, Processes, People and Technologies. It includes incentives to do research on cyber security, establishing partnerships with national and international public education and research institutions.



5.6 REPUBLIC OF KOREA

Health and Welfare CERT & ISAC

Korea's Ministry of Health and Welfare divides cyber security tasks into public and private sectors. In the public sector, the Health and Welfare Cyber Security Center (CERT) was established in December 2008 to establish a cyber security plan in the field of health and welfare in accordance with the National Cyber Security Management Regulations. The CERT provides services such as vulnerability assessment, crisis response simulation training, and security education to healthcare delivery organisations.

The private sector established Korea's Health and Welfare ISAC in 2018 to enhance security for healthcare delivery organisations and conduct cyber security services. Health and Welfare ISAC provides its members with security control, information sharing, infringement response, education and training services. The Health and Welfare ISAC's target is to encourage security control and provide training to improve security awareness at all healthcare delivery organisations operating in Korea. Korea is expected to minimise the damage caused by cyber infringement accidents in healthcare delivery organisations, comply with legal regulations, and reduce the security investment cost of healthcare delivery organisations through the Health and Welfare ISAC. It plans to continuously expand its services by diagnosing weaknesses in healthcare information systems, diagnosing the information security level of healthcare delivery organisations, and developing security technologies specialised in health and welfare fields.

5.7 UNITED KINGDOM

NHS Digital Data Security Centre

The Data Security Centre (DSC) is the technical and delivery authority for cyber security within the NHS. It is a government-funded organisation whose mission is to provide "Security at the Point of Need" across the healthcare sector and enable local and national healthcare organisations to deliver enhanced patient and clinical outcomes through the delivery of secure services and technology.

DSC's Cyber Security Strategy is based on two strategic limbs, namely:

The development of a world-leading Cyber Security Operations Centre (CSOC): which builds upon the original CareCERT structure. The CSOC provides a number of security services and capabilities across health and care including, but not limited to: protective monitoring; threat intelligence; and hunting. Membership is free and, once signed up, the healthcare organisation provides an overview of its network infrastructure. The CERT provides regular free vulnerability scanning; specialist security consultancy and advisory services; advice and guidance artefacts; running of the Public Key Infrastructure for health and care; and incident response services

The augmentation of organisational (e.g. hospitals) security capability and resiliency through targeted local interventions: this limb provides a number of services directly to the healthcare organisations, which assist the CERT to identify threats to the healthcare organisations. They have sensors installed in all member organisation networks, allowing real-time visibility of the cyber threats present in healthcare organisations including, but not limited to: on-site maturity and capability assessments; technical remediation and improvement services; the Data and Security Protection Toolkit to aid self-assessments, reporting, and improvement; technical training; operational readiness services; cultural

transformation; perimeter security services; endpoint protection capabilities; and identity and access management capabilities.

The DSC's mission is supported by a number of public sector organisations including:

- **The Department of Health and Social Care:** which provides the DSC with policy and governance support and guidance as well as supporting funding bids and articulation of benefits realisation and value creation.
- **NHS England:** which provides a Capital Infrastructure fund to support local organisations reduce the number of legacy security systems, reduce the use of unsupported software, and improve critical infrastructure components across the health sector. NHS England also uses the DSC to help address regulatory concerns with respect to data and cyber security across the system (including NHS enforcement notices).
- **The National Cyber Security Centre:** which provides a number of free-to-use services such as Public DNS and external vulnerability scanning services to health and care. It also acts as a trusted advisor to the DSC across a range of cyber security-related matters.
- **The Care and Quality Commission (through NHS Improvement):** which provides a variety of inspections across the sector including cyber security inspections using a defined framework. Severe contravention or failings under these inspections can lead to "special measures" whereby corrective action is enforced and proactively monitored to ensure improvement.

The DSC's initial focus is on secondary care providers and organisations (as well as national applications and networks); work is currently underway to address pharmacies, social care providers, and other primary care organisations. While the Cyber Security Strategy and program is new, significant improvements have already been made, including the raising of the average cyber maturity of secondary care organisations from 57 per cent to 66 per cent in a little under four months.

5.8 UNITED STATES

National Cyber Strategy

On 20 September 2018, the White House released the first comprehensive National Cyber Strategy since 2003. The strategy's stated objective is to "ensure the American people continue to reap the benefits of a secure cyberspace that reflects our principles, protects our security, and promotes our prosperity." The White House cyber strategy contains four pillars:

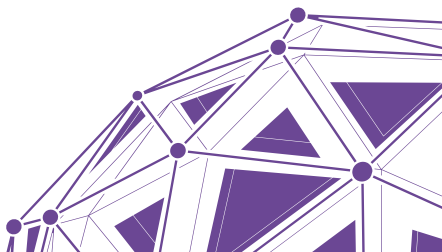
1. **Pillar I:** Protect the American People, the Homeland, and the American Way of Life by securing federal networks and information, securing critical infrastructure, combating cybercrime and improving incident reporting;
2. **Pillar II:** Promote American Prosperity by fostering a vibrant and resilient digital economy, fostering and protecting US ingenuity and developing a superior US workforce;
3. **Pillar III:** Preserve Peace Through Strength by enhancing cyber stability through norms of responsible state behaviour and attributing and deterring unacceptable behaviour in cyberspace; and

4. **Pillar IV:** Advance American Influence by promoting an open, interoperable, reliable and secure internet and building international cyber capability.

The US Department of Health and Human Services' (HHS) Health Sector Cybersecurity Coordination Center (HC3) is an operational cyber security centre designed to support and improve the cyber defence of the US Healthcare and Public Health (HPH) sector. HC3 strengthens coordination and information sharing within the sector and cultivates cyber security resilience by providing timely and actionable cyber security intelligence to healthcare organisations and developing strategic partnerships between these organisations. HC3 is built on the notion of discovery, analysis, and resolution. Its goal is to have the visibility to discover issues affecting the HPH sector and provide the needed expertise to analyse cyber concerns. HC3 goes a step further by synthesising the information so the sector can resolve its cyber issues.

HC3's strategic priorities are to:

- provide the HPH sector with timely, relevant, and actionable intelligence on cyber security threats
- promote organisational cyber security capacity within the sector
- foster a cyber security community through partnerships and collaboration.



6 DISCUSSION

6.1 WAKE-UP CALL: CYBER SECURITY IMPACTS ON THE PROVISION OF HEALTH CARE

Strategies like adding additional information systems to improve cyber security or placing complete faith in information technology to identify and propose technological solutions, is hardly proving effective. Security policy change is required to respond effectively to all the different challenges an organisation must face – like global threats, tracking vulnerabilities, applying security policies across different systems and endpoints, diverse and changing staffing profiles, frequent introduction of new technologies, and many others. The approach to cyber security needs to change from a defensive stance focused on malware to a more realistic and resilient approach, a cyber-resilient approach.

Countries are facing new challenges resulting from the digital society and digitisation across sectors. In health care challenges exist from and in health care, which are transforming the way services are provided, the way information is accessed, how citizens and healthcare providers communicate, and the secondary use of data. This raises complex issues relating to citizen consent, secure access of information and other cyber security challenges.

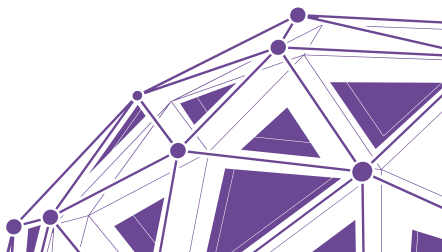
Securing global digital health efforts may mean that we need to devise a common strategy to help protect our digital transformation investments and efforts in health care. This can be done by addressing in a separate document a five-year vision addressing, among other things, the following questions:

- What is a good strategy and what does it look like?
- What is a good “worldwide common” strategy in the context of voluntary cooperation?
- What are the fundamental principles?
- What short-term gains can be achieved from a common effort?
- What are the top threats facing the healthcare sector?

6.2 TOGETHER WE ARE SAFER

International cooperation is needed to deal with the cross-border nature of cyber threats (8). Given the well-recognised global shortage of skilled cyber security professionals (9), working together can reduce the burden on each individual country to achieve a secure digital health service.

The Global Cybersecurity Index (GCI) (2) has the objective of helping countries in the area of cyber security by encouraging a global commitment into this field. To that end, a conceptual framework with five pillars was defined in which capacity building and cooperation and their sub-pillars are key to jointly achieving a safer approach.



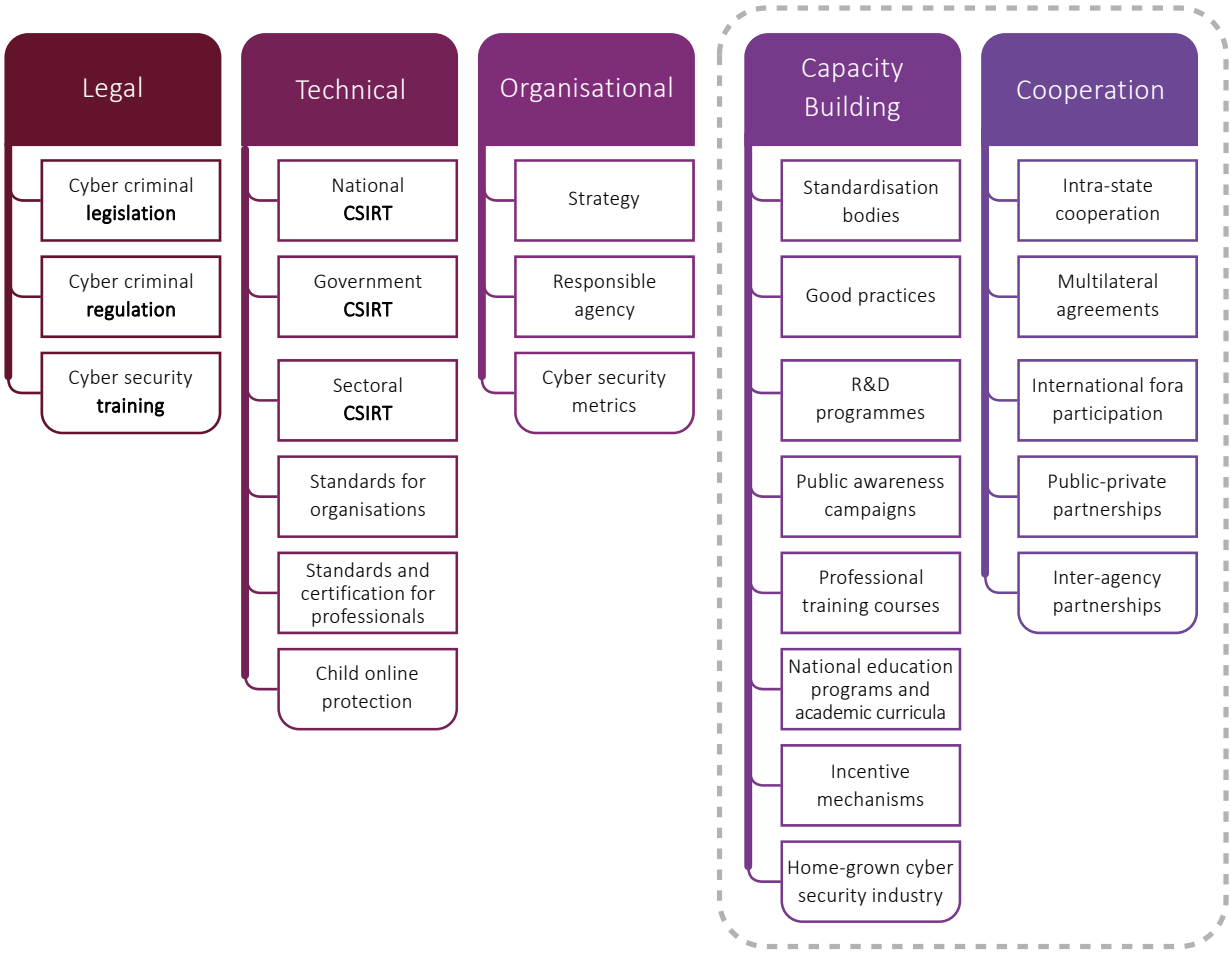


Figure 6: GCI pillars and sub-pillars

There are examples of capacity building and cooperation that would be useful to address the new challenges countries are facing resulting from digitisation and digital transformation. Table 3 has been updated based on examples provided by GDHP participants at the Lisbon Workshop.

Table 3: Capacity Building and Cooperation Examples

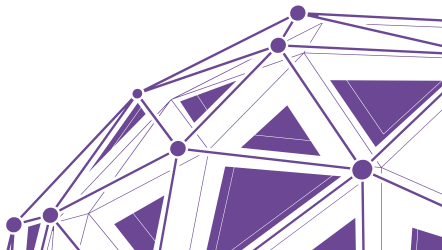
Country/ Organisation	Initiative	Website
USA	Resource Center for State Cybersecurity	https://www.nga.org/bestpractices/divisions/hsps/statecyber
Australia	Oldest CERTs (1993) AusCERT	www.auscert.org.au
	The Council of Registered Ethical Security Testers	https://www.crestaustralia.org
NATO	Cooperative Cyber Defence Centre of Excellence	https://ccdcoe.org
Sweden	Nordic National CERT Technical Cooperation	https://www.msb.se/en/tools/news/nordic-cyber-security-exercise-was-conducted-in-linkoping
UK	National Cyber Security Centre	https://www.ncsc.gov.uk

6.3 PROPOSED COLLABORATIVE ROADMAP (2019–2023)

Taking the example of the cooperation for digital health under the EU eHealth Network, and in accordance with the World Health Organization (WHO), we know that cooperation between countries is beneficial. This allows the sharing of knowledge and best practices, making it possible to solve problems jointly (10). At the European level, the Multiannual Work Programme 2018–2021 (11), under the motto eHealth in support of better health, shows the importance of empowering people. Demonstrating the value of the innovative use of health data, exchanging continuity of care and the significance of interoperability, data protection and data security.

A collaborative roadmap can be devised for the Cyber Security Work Stream of the GDHP. This should be the focus of coming efforts, as a five-year vision is key to achieving cooperation at an international scale. This vision can include, but is not limited to, the following efforts to jointly make our digital health ecosystem safer:

- common policy documents
- awareness-raising documents
- co-created educational material
- common CERTs
- information sharing processes.



The GDHP Cyber Security Work Stream decided at the Lisbon workshop that the list of activities/deliverables could be aligned with the six dimensions indicated below, creating activity bundles. The suggested method is a common approach that will benefit from looking at this roadmap in progressive steps:

1. **Governance and strategy organisation**

   The existing challenges in cyber security imposed by digital transformation require transversal and cross-sectoral governance with a coherent coordination and response capacity from the responsible bodies. As a result, it is important to build robust security information systems and to build capacity response by communities and teams.

2. **Prevention, education and awareness**

   Awareness raising is crucial for information sharing and threat identification is crucial. It is important that not only public entities but also companies, civil society and final users are informed to adopt prevention measures to risk exposure. Schools and universities should play an active role in teaching cyber security concepts to students and future professionals, and, together with governments, should be responsible for encouraging digital literacy. Joint efforts could mean sharing of information and awareness materials, strategies and successful experiences between member states.

3. **Protection measures and capacity building**

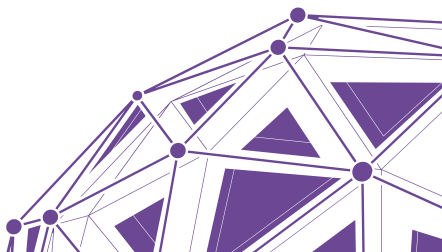
   Cyber security is a cross-sectoral concept that doesn't only relate to information technology, as it directly impacts national economies and the daily lives of citizens. Mapping the infrastructure of information systems and changes in national and international laws related to cyber security are important to build these secure environments and to prepare national entities to respond to threats and recover from disasters in adverse scenarios. Cooperation should also be built with private companies.

4. **Response to threats**

   A first step in any cyber security approach is to map the threats to the systems and services. A systematic and methodical process can be used to map the common threats and weaknesses between GDHP participant countries. This would ensure we target our interventions to the most common challenges, while also identifying those that are less common, but still relevant. Less common challenges may only pose threats in the present to some countries but can be future potential threats for other countries. Sharing of best practices in threat identification and national responses can further develop collective capacity.

5. **Research, development and innovation**

   Although cyber security is a current challenge, the new technological and systems challenges require sustainable development and future thinking. National and international partnerships on research, development and innovation and emerging technologies for cyber security must be incentivised, not only in academia but also in industry. The adoption of secure-by-design and secure-by-default must be a focus and, again, the identification of best practices and the cross-fertilisation of academic efforts between participating countries could be a way forward.



6. Collaboration and collaborative response

The complexity and number of cyber-attacks is on the rise, and the ability to effectively respond and recover from an attack is key to the success of any digital service. As the health sector's reliance on digital technology increases, so does its attractiveness to cyber criminals and threat actors who want to gain access to sensitive information. The health sector has a relatively low maturity in relation to cyber security, requiring significant support from cyber security experts to support the development of effective defence and response activities to protect sensitive health data.

There are several government and privately funded organisations world-wide that provide cyber security support to the healthcare sector. Some of these organisations provide services under the banner of a Computer Emergency Response Team (CERT). Others provide these services through broader health service organisations, such as national health departments.

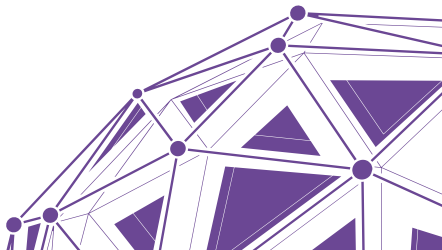
The GDHP has implemented a discussion forum to allow for the sharing of threat information in near real time via a Slack-based platform. This platform allows for the sharing of TLP:white and TLP:green information (see Table 2) on threats and Indicators of Compromise (IOCs). The GDHP is developing a pilot of an alert system that will provide immediate real-time information regarding major cyber activity that impacts the global health sector, such as the WannaCry incident.

6.4 REAL-TIME THREAT SHARING ADVANTAGES

As successful cyber security attacks have become both more complex and more frequent, the need has never been greater to work collaboratively to stop malicious attackers before they are able to do harm to digital healthcare systems. One of the most effective ways to establish this collaboration is through the creation and sharing of IOCs. These are the specific artefacts and information that allow for the detection of intrusions or other activities conducted by attackers. IOCs include artefacts such as hashes of known malicious files, IP addresses or Domain Name System (DNS) names of command and control (C&C) servers, registry keys and the contents of malicious files. The sharing of IOCs between organisations within the digital healthcare ecosystem can help to raise the overall security posture of the sector. The sharing of information about emerging threats is central to the fight against cyber threats, and given the global nature of cyber security, ideally this information needs to be shared across national borders.

6.5 INTERNATIONAL REAL-TIME THREAT SHARING IMPLEMENTATION OPTIONS

The development of an online threat sharing portal, allowing two-way sharing of information within the digital healthcare sector will support the increase of cyber maturity across the international healthcare sector. This portal would allow direct reporting of threats, IOCs and other suspicious behaviours by members of the international healthcare community, allowing GDHP organisations to provide threat analysis to the community in a secure manner. The portal would additionally provide an environment for security professionals within the sector to discuss any problems or issues they are having through an online forum.



Currently, this information is shared manually via the existing Slack platform. Looking to the future, it would be beneficial to transition to an automated sharing mechanism as we mature our threat intelligence capabilities. The development of capabilities to automate the ingestion of an intelligence feed into the existing cyber security tools would enable dynamic use of this information to protect international digital health information, systems and services.

A potential option for threat sharing is using Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) feeds to share information in a format that can be automatically consumed by security appliances. STIX and TAXII are community-driven technical specifications designed to enable automated information sharing for cyber security situational awareness, real-time network defence and sophisticated threat analysis.

6.6 GLOBAL DIGITAL HEALTH CERT

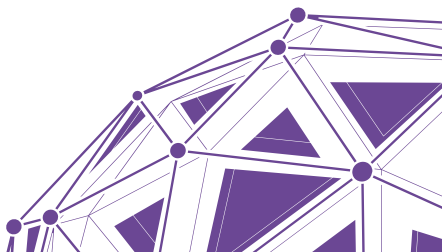
GDHP cyber work stream participants have proposed to establish a CSIRT/CERT that operates globally involving all participating countries. This is proposed to be fully functional by 11 May 2019, and it is a gradual process.

To support this proposal, and aligned with the deliverables defined for the cyber security work stream, collaborative platforms are under creation, such as the Slack, portal website and app version.

It is important to clarify the operation concepts, the triggers for national and internal action and “significant incident” taxonomy, and the incident virtual response room, that are critical for the operations of systems and countries. Incident response should include incident diagnosis and risk diagnosis, which would be protected by cyber security protocols.

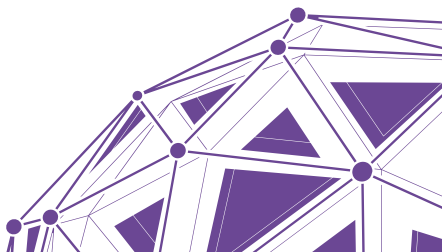
The GDHP participants of the workshop held in Lisbon also highlighted the importance of identifying the roles and responsibilities in a formal crisis and response plan.

For this purpose, a memorandum was created to identify the first wave of countries that are willing to join, and we foresee the formalisation process to be confirmed with the multilateral signature of an international collaboration protocol.



7 CONCLUSIONS

- Cyber risk can threaten not just data and everyday operations in health care, but by creating a sense of fear and threat, it can also threaten the momentum for digital health transformation.
- Different countries are at different levels of maturity in their national cyber security efforts, and likewise their digital health domain may be at different levels of maturity and therefore more or less protected.
- Most challenges are the same. Costs are high and solutions need creativity. Sharing local and national best practices is therefore both possible and desirable.
- There is currently a wide range of approaches used to support cyber security incident response in the health sector internationally. The most common approach, based on the information available, is a central coordination point for cyber response. Some countries provide operational support on a day-to-day basis but this approach is in the minority.
- There is a risk of loss of patient confidence globally if many countries experience serious cyber-attacks.
- This is obviously a journey and an iterative process and we should therefore measure success in terms of how we share information and learn lessons from previous incidents.
- It may be possible and desirable to create a common international approach to provide real-time visibility and incident response support.
- The cyber security strategies that can strengthen the processes and practices designed to protect healthcare-related devices, systems and networks, as well as the data within them, from security risks and cyber-attack should be based on six dimensions:
    1. Governance and strategy organisation
    2. Prevention, education and awareness
    3. Protection measures and capacity building
    4. Response to threats
    5. Research, development and innovation
    6. Collaboration and collaborative response.



8 REFERENCES

1. European Commission. State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks. European Commission: Press Release Database. [Online] September 19, 2017. http://europa.eu/rapid/press-release_IP-17-3193_en.htm.

2. Global Cybersecurity Index (GCI) ITU. [Online] 2017. https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci.01-2017-pdf-e.pdf.

3. PWC. Cybersecurity Confidence in your digital future. [Online] 2014. https://www.pwc.com/sg/en/risk-assurance/assets/gc-cyber-security.pdf.

4. Verizon. Protected Health Information Data Breach Report. 2018.

5. Bradshaw, Samantha. Combating Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity. [Online] 2015. [Cited: 12 11, 2018.] https://cigionline.org/publications/combatting-cyber-threats-csirts-and-fostering-international-cooperation-cybersecurity.

6. CPNI - Centre for the Protection of National Infrastructure. Personnel and People Security. [Online] https://www.cpni.gov.uk/personnel-and-people-security.

7. Forrester. Introducing Forresters Targeted Attack Hierarchy of Needs. Forrester. [Online] May 20, 2014. http://blogs.forrester.com/rick_holland/ 14-05-20-introducing_forresters_targeted_attack_hierarchy_of_needs.

8. Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime. Heinl, C H. 1, 2014, Asia Policy, Vol. 18, pp. 131-159.

9. Fourie, Leon, et al. The global cyber security workforce - an ongoing human capital crisis. [Online] 2014. [Cited: 12 11, 2018.] http://unitec.researchbank.ac.nz/handle/10652/2457.

10. World Health Organization. WHO's work with countries. World Health Organization. [Online] 2018. https://www.who.int/country-cooperation/what-who-does/inter-country/en/.

11. eHealth Network MWP sub-group. Multiannual work programme 2018-2021. October 31, 2017.

9 ABBREVIATIONS

C&C	Command and control
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
DNS	Domain Name System
eHN	eHealth Network
EIF	European Interoperability Framework
EU	European Union
GCI	Global Cybersecurity Index
GDHP	Global Digital Health Partnership
H2020	Horizon 2020
ICT	Information and communications technology
IOC	Indicator of Compromise
IoT	Internet of Things
ISO	International Organization for Standardization
mHealth	Mobile Health
NATO	North Atlantic Treaty Organization
PHI	Protected Health Information
PHIDBR	Protected Health Information Data Breach Report
STIX	Structured Threat Information eXpression
TAXII	Trusted Automated eXchange of Indicator Information
TLP	Traffic light protocol
ToM	Technical and Organisational Measure
WHO	World Health Organization