CYBER SECURITY: FOUNDATIONAL CAPABILITIES

GDHP White Paper on Cyber Security

GLOBAL DIGITAL HEALTH
PARTNERSHIP

Acknowledgements

The GDHP would like to thank the Chair of this work stream, Rob Shaw CBE (Deputy Chief Executive, NHS Digital) and Co-Chair, Fuller Yu (Chief Information Security Officer, Hospital Authority Hong Kong) for engaging GDHP participants in discussions, meetings and other activities to drive and develop this work. The GDHP would also like to sincerely thank the lead author Dan Jeffery (Head of Innovation, Delivery, & Business Operations Data Security Centre, NHS Digital) for driving the development of this white paper and for his close collaboration with country participants and the Secretariat.

The GDHP would also like to thank countries and territories who participated in the Cyber Security work stream discussions and, in particular, thank the countries and territories who contributed their profiles to this report – Argentina, Australia, Canada, Estonia, Hong Kong SAR, Italy, New Zealand, Portugal, the Kingdom of Saudi Arabia, Republic of Korea, the United Kingdom and the United States. Rodney Ecclestone and Clara Lubbers, provided guidance and editorial support to the work stream Chair and Co-Chair, and worked with participant countries to ensure the development of this report.

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.

Published: 20 July 2020

GLOBAL DIGITAL HEALTH
PARTNERSHIP

Suggested Reference

Jeffery D, Shaw R. Cyber Security: *Foundational Capabilities*. Prepared for the Global Digital Health Partnership; July 2020. Sydney, Australia.

CYBER SECURITY: FOUNDATIONAL CAPABILITIES

GDHP White paper on Cyber Security

CONTENTS

1 NOTE FROM THE GDHP WORK STREAM CHAIR

Since the publication of our inaugural white paper, *Securing Digital Health: initial reflections for steering global cyber security efforts in health*, at the New Delhi Summit in February 2019, the Cyber Security work stream has been working tirelessly and collaboratively to develop a Foundational Capabilities Framework (FCF) which builds on the Strategic Framework previously delivered. This white paper not only outlines the FCF, but the work stream has also worked with a number of participant countries to establish what our current collective maturity is with regards to addressing this most pressing of topics, namely: cyber security in an era of digital health care. I truly hope that the findings of our research are used as a catalyst for – and basis from which – collective action and collaboration can take place to address common challenges, and for further work with those countries that have made great strides in complex problem spaces for the benefit of all.

I mentioned in my foreword to the previous white paper that "cyber security is ultimately a team sport with no national borders." The research, findings, and insights afforded by this publication pay tribute to this notion. I am proud and humbled by the honesty, transparency, and integrity that each participating country has demonstrated in helping us understand the current challenges that we need to address so that we can realise the promise of the digital revolution in health care for the benefit of all in the very near future.

There is a nervousness in some countries to highlight their lack of maturity, which is understandable given the sensitivity of this subject. However, whichever end of the spectrum a country is at, whether increasing from 0 to 1, or from 3 to 4, is a big step forward. Lessons can be learned across all aspects of the capabilities and, as I leave GDHP, I hope the foundations are there to assist existing and future participants to raise their maturity using the tools we have provided.

Rob Shaw CBE
Chair
Global Digital Health Partnership Cyber Security work stream

2 EXECUTIVE SUMMARY

After the success of the Summit in New Delhi in February 2019, the GDHP Cyber Security work stream decided to build on its inaugural Cyber Security white paper, *Securing Digital Health: initial reflections for steering global cyber security efforts in health*, by commissioning a second paper that developed a common framework from which to assess foundational cyber capabilities. This commission saw the development of a Foundational Capabilities Framework (FCF) which has been applied to around a half of the GDHP participant countries. The FCF builds on, and represents the next level of detail of, the Strategic Framework which was articulated in the previous white paper.

We followed a simple yet effective methodology (see Figure 1 below) to explore specific areas of cyber security. This paper outlines and articulates the key findings and results. It also provides some initial recommendations and next steps which were discussed by participants at the Hong Kong round in October 2019. These will be taken forward as part of the Cyber Security work stream's deliverable schedule.

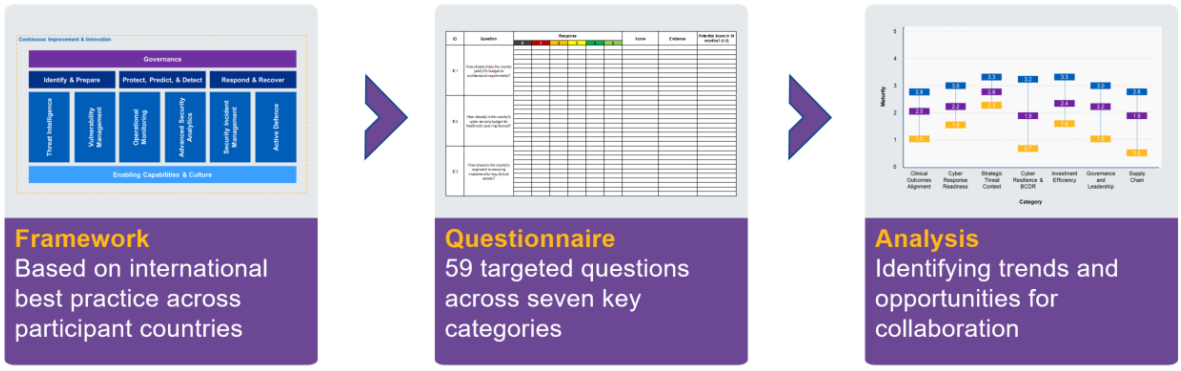

Figure 1: High-level research approach

It was found that GDHP participant countries have an average current maturity score of 2.2 out of 5 (as against the COBIT 5 regime), with an ambition to reach 3.2 out of 5 maturity over the next 18 months. While this is an ambitious target, it is wholly achievable and it is hoped that the GDHP will be able to provide the means through which this increase in maturity can be expedited through the development and sharing of best practice and common templates, artefacts, and accelerators.

The results of this research have also highlighted a number of core areas of opportunity where GDHP participant countries can work together to tackle common problems and/or impart knowledge and experience to assist those participants who are facing challenges in certain areas. This approach of collective collaboration will enable the expediting of maturity across the membership base to the benefit of the delivery of digital health and enhanced patient outcomes. This is imperative as the risks arising from the cyber space are extremely important and universal in nature.

3 INTRODUCTION

3.1. BACKGROUND

In February 2019, the GDHP Cyber Security work stream launched the white paper *Securing digital health: initial reflections for steering global cyber security efforts in health* at the New Delhi Summit. This white paper provided a Strategic Cyber Security Framework from which coordinated, business-aligned, and operationally coherent programs and capabilities could be deployed, delivered, and operated to secure and enable the digital transformation of health care and realise the potential of the digital revolution. Since the launch of this paper, the GDHP Cyber Security work stream participants have worked together to develop a Foundational Capabilities Framework (FCF) which builds on the Strategic Cyber Security Framework and represents the next level of detail and thinking from the Cyber Security work stream. The FCF is designed to be used by all participant countries regardless of where they are in their respective digital transformation journeys. The FCF aligns the business objectives and clinical outcomes with cyber security needs so that cyber security ultimately enables the delivery of patient outcomes in a digital world.

3.2. PROBLEM STATEMENT

This white paper aims to address the following problem:

> *As the digital revolution in health care continues at pace, there is a need to ensure that the benefits and potential of this transformation are recognised through the delivery of robust cyber security regimes across participant countries. Given that participants are at differing stages and maturity in their journey, coupled with the drive towards, and focus on, interoperability, there is an opportunity and need for the establishment of a unified cyber capabilities framework for health care. This not only needs to cover the traditional elements of cyber security, but also needs to pay specific attention to the risks posed by networked legacy medical devices and the emergence of the medical IoT (Internet of Things) landscape.*

3.3. AIM OF THE RESEARCH

The primary aim of this research is to identify and understand common areas of opportunity and challenge within cyber security across the participant countries, as well as providing an overview of general cyber maturity for each participating country. Additionally, this research will enable the work stream to refine, advance, and develop its current work schedule in a manner that drives greater improvement and maturity in this rapidly evolving problem space so that we can ensure continuous relevance, benefit, and value for each participating country.

This research also provides participating countries the capability framework itself. As mentioned above, this framework builds on the previous Strategic Framework and, as such, it provides participating countries with an additional tool that they can use to help structure, shape, and measure their own respective cyber security programs, capabilities, and structures in a consistent and predictable manner.

3.4. SIGNIFICANCE FOR POLICY MAKERS

It is hoped that the results and findings of this research feed into the policy discussions within participating countries to help shape, inform, and provide evidence points for domestic programs and postures as well providing opportunities for the sharing of good practice in areas of maturity and collaboration in areas of mutual challenge. Given the complexity, pace of change, and universality of the cyber threat and risk landscape, it is true to say that collective action and collaboration is the most efficient, effective, and expedient approach to reducing the threat surface area while also setting the conditions from which the promise of the digital revolution can be realised across the healthcare sector.

3.5. SCOPE AND METHODOLOGY

The scope of this research paper covers seven core areas of inquiry, namely:

1. Clinical outcomes alignment
2. Cyber response readiness and recovery
3. Understanding of the strategic threat
4. Cyber resilience and business continuity and disaster recovery (BCDR)
5. Budgetary and investment proportionality and effectiveness
6. Governance, culture, and leadership
7. Supply chain resilience and security

These seven areas have been mapped back to a number of international standards and best practices including, but not limited to, NIST 800, ISO27001, and COBIT 5. Against each of these areas is a question set which each participating country completed and provided evidence for in order to justify their assertions. This enabled the triangulation of results across qualitative and quantitative inputs leading to more informed and nuanced analysis and ultimately recommendations. Nearly half of GDHP participants provided input into this research paper which provides a solid representation of the membership and helps drive the reliability and validity of the results. It should be noted that the questionnaire and underlying framework is scalable and designed so that multiple iterations of this research can be run to capture information regarding the maturity position of new participants (as well as existing but not yet participating members). This will serve to increase the importance of the research and also supports the accuracy of the results and actionability of the recommendations.

4 DEVELOPMENT OF THE FOUNDATIONAL CAPABILITIES FRAMEWORK

At the New Delhi Summit of the Global Digital Health Partnership (GDHP) in February 2019, the Cyber Security work stream launched the white paper *Securing Digital Health: initial reflections for steering global cyber security efforts in health*. The white paper outlined and reinforced the need to recognise cyber security as a continuous activity that generates value for healthcare organisations. It also provided a strategic framework and model that participant countries could adopt and refine to meet their individual structures, legislative regimes, and healthcare priorities.

It was recognised that the strategic framework was just a starting point in the cyber security journey. In order to further the objectives, aims, and intended outcomes of this strategic framework, the Cyber Security work stream subject matter experts (SMEs) have developed a Foundational Capabilities Framework (FCF). This framework is based on internationally recognised best practice, standards (including NIST 800 series, ISO27001 & ISO31000, ISF Good Practice for Information Security, COBIT 5, and the Carnegie Mellon Cyber Security Maturity Model), and the experiences of participants. Figure 2 provides the high-level overview of the Foundational Capabilities Framework.

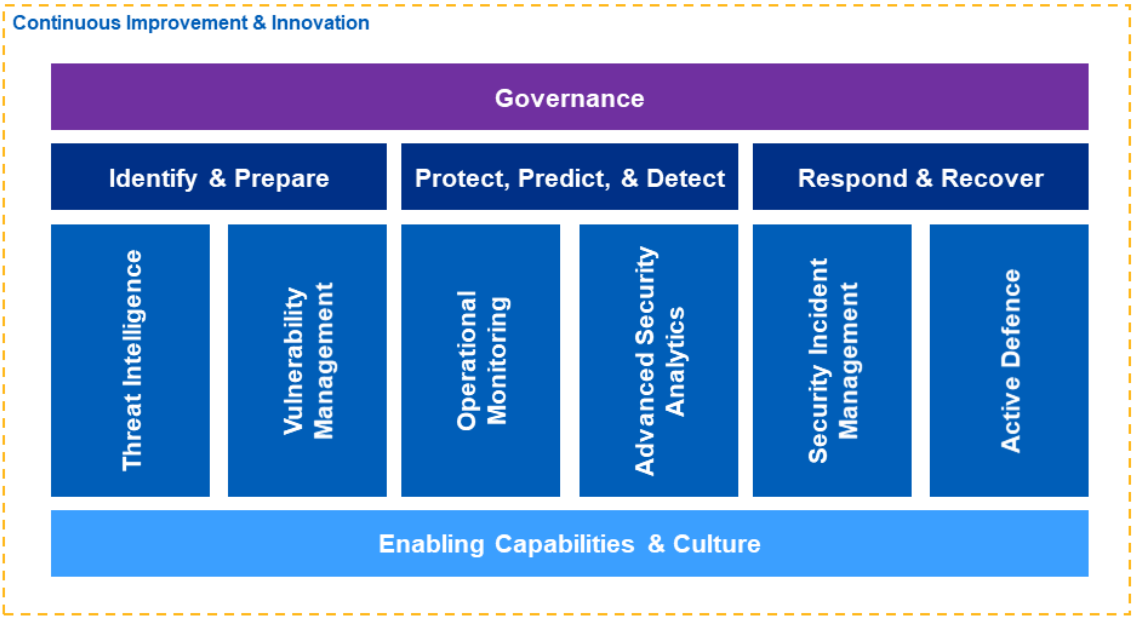

Figure 2: Level-one Foundational Capabilities Framework

In order to make this framework targeted and specific for health care, the Cyber Security work stream devised a targeted questionnaire that 11 participants completed. This questionnaire comprised seven key categories[1], namely:

1. **Clinical outcomes alignment:** how aligned is the cyber program to the wider healthcare strategy and "business" objectives?
2. **Cyber response readiness and recovery:** how far does the country evaluate its ability to react and respond to a cyber security breach?
3. **Understanding of the strategic threat:** how far does the country explore the alignment of its security strategy and program with the threat landscape?
4. **Cyber resilience and business continuity and disaster recovery (BCDR):** how far does the country understand the threat landscape and how does it use it to "design for resilience" so as to limit the impact of cyber-attacks?
5. **Budgetary and investment proportionality and effectiveness:** how does the country consider the allocation of funding across its cyber security program, threat landscape, and clinical objectives?
6. **Governance, culture and leadership:** how well defined is the country's cyber security RACI (Responsible, Accountable, Consulted, Informed), culture, performance, and chain of command structures and mechanisms?
7. **Supply chain resilience and security:** how effective, efficient, and comprehensive – in terms of coverage – is the country's security program across the supply base and the healthcare organisation's wider ecosystem?

These seven categories were then mapped to the Foundational Capabilities Framework shown in Figure 2. It is necessary to do this because a number of the seven categories are applicable to multiple elements of the Foundational Capabilities Framework. This is shown in Figure 3.

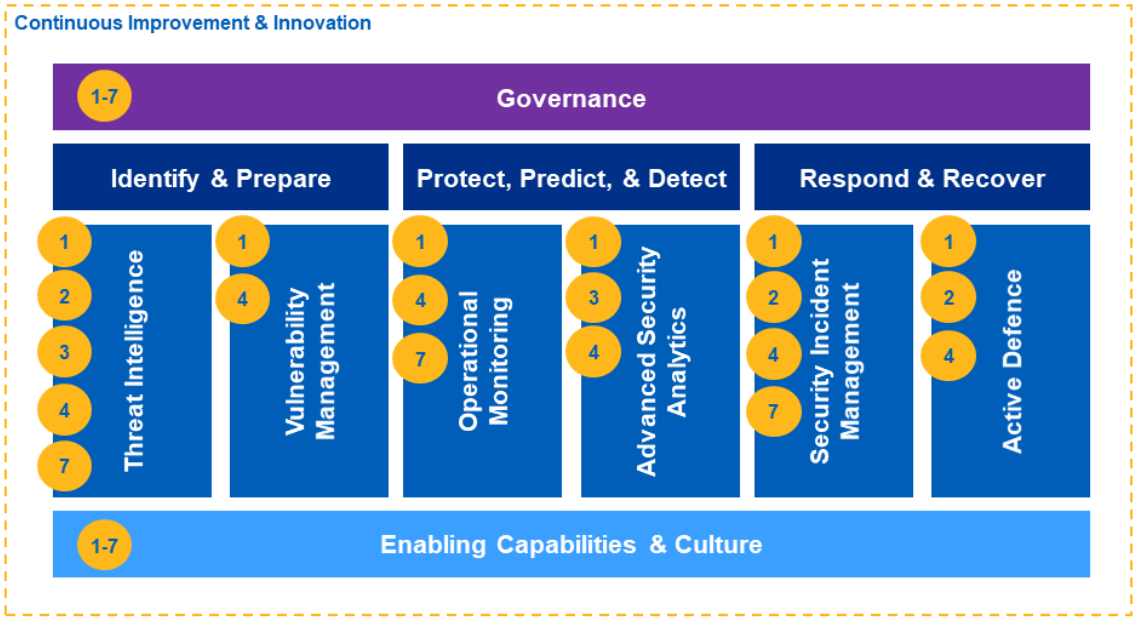

Figure 3: The seven categories of the questionnaire mapped onto the Foundational Capabilities Framework

[1] This was tailored from the NHS England Strategic Cyber Security Management Framework.

The answers to the questionnaires provided the subject matter experts with qualitative and quantitative data and outputs which were the basis for the analysis and findings outlined below. Based on these findings, coupled with subject matter expert inputs, the recommendations were formulated.

The results detailed below not only provide a view of maturity across the membership, but they also identify common challenges and opportunities for improvement which were explored and discussed at the Hong Kong Global Digital Health Partnership Summit in October 2019.

5 BUILDING A FOUNDATION OF RESILIENCE

Given the importance of the digital health agenda and the potential the digital revolution presents to health care globally, there is a need to ensure that cyber security postures are commensurate with the risks that our systems face. GDHP participants are diverse, but the cyber risks we face are broadly universal. While this presents a collective challenge, it also represents an opportunity to identify and understand areas of collaboration, cooperation, and the sharing of best practice – from which we can all benefit. In order to achieve this, there is a need to establish a common baseline of understanding and taxonomy as well as an initial view of "what good looks like" based on best practice. The Cyber Security work stream has analysed and leveraged internationally recognised definitions and concepts to derive an initial set of standardised concepts, terms, and maturity definitions. These are outlined in the section below. While this attempts to provide universality across key concepts, it does not currently take into account local, national, and regional nuances.

A key element to building a foundation of resilience is the need to have a common definition of maturity levels that participants can assess themselves against when answering the questions.

Table 1: Definition of maturity levels

Maturity Scores	Definitions
0	**No current defined capability:** the question area is achieved via ad hoc means that are undocumented
1	**Initial:** approach to meeting the intent of the question area. Not a complete set of practices to meeting the full intent of the question area.
2	**Managed:** simple, but complete, set of practices that address the full intent of the question area
3	**Defined:** uses organisational standards and tailoring to address question area and work characteristics
4	**Quantitatively managed:** uses statistical and other leading quantitative techniques to understand performance variation and detect, refine, or predict the question area to achieve enhanced outcomes

Maturity Scores	Definitions
5	**Optimising:** defined as world/industry-leading practices – uses statistical and other quantitative techniques to optimise performance and improvement to achieve quality and process performance objectives

Each participating country has answered a series of questions that are grouped into seven key categories:

1. Clinical outcomes alignment
2. Cyber response readiness and recovery
3. Understanding of the strategic threat
4. Cyber resilience and business continuity and disaster recovery (BCDR)
5. Budgetary and investment proportionality and effectiveness
6. Governance, culture, and leadership
7. Supply chain resilience and security

The questions for each category can be found in Appendix A. The remainder of this section provides an overview of each area of the Foundational Capabilities Framework and provides an initial view of good practice.

5.1. CLINICAL OUTCOMES ALIGNMENT

This is about the effectiveness of aligning the cyber program to the wider healthcare strategy and clinical business objectives. This category focuses on how effective a country is at aligning security threats and risks to clear clinical outcomes.

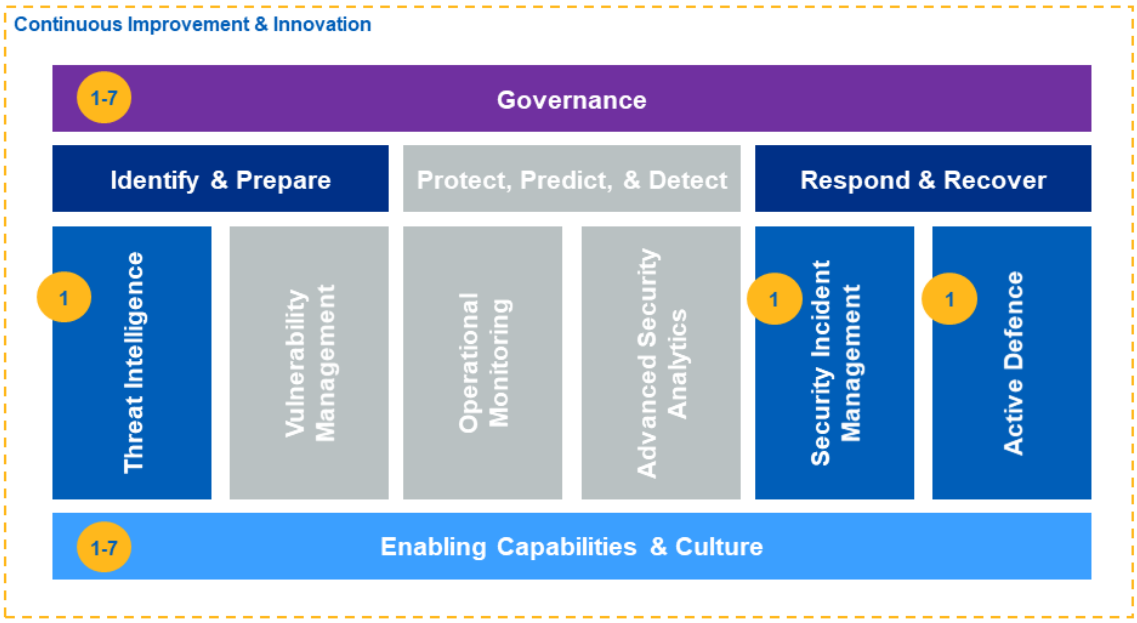

Figure 4: Mapping of the Clinical Outcomes Alignment section of the questionnaire onto the Foundational Capabilities Framework

Good practice will have a consistent approach across health care to identify high-value assets and business processes. The country will have mature key performance indicators (KPIs) and metrics that monitor the relationship between these high-value assets/processes and the threats/risks impacting them. Incident planning and testing should be used to test the validity of these outcomes and use this to influence and inform the cyber security strategy.

5.2. CYBER RESPONSE READINESS AND RECOVERY

This is about evaluating the country's ability to react and respond to a cyber security breach and monitoring the level of readiness to respond to threats and incidents against the ecosystem. This includes a national incident plan on how to manage the recovery from a cyber security breach.

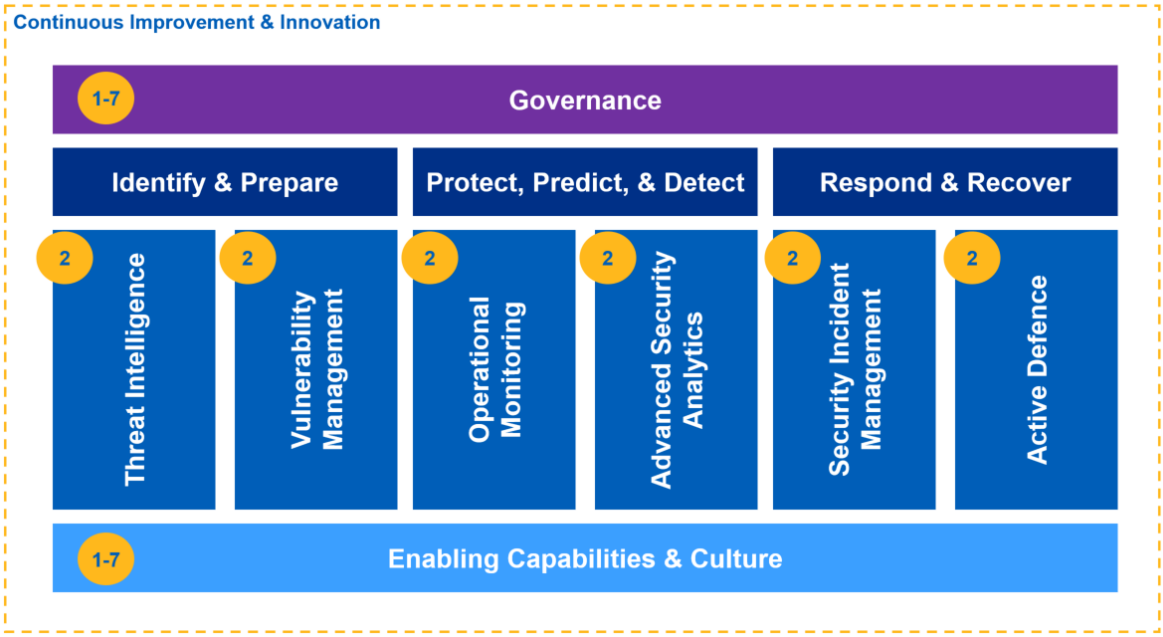

Figure 5: Mapping of the Cyber Response Readiness and Recovery section of the questionnaire onto the Foundational Capabilities Framework

Good practice includes a detailed national response and recovery plan with clear escalation paths in the event of a cyber security incident. The country should have a regime in place to test these plans and escalation paths. Critical to this category is a clear and tested incident communication plan that provides clear routes of communication and the right messages delivered to key audiences in the event of a breach.

5.3. UNDERSTANDING OF THE STRATEGIC THREAT

This category is about the identification of current and potential security threats, trends, and environment, specific to health care. It focuses on how far the country explores the alignment of its security strategy and program with the threat landscape – identifying, contextualising and monitoring threats against the healthcare sector.

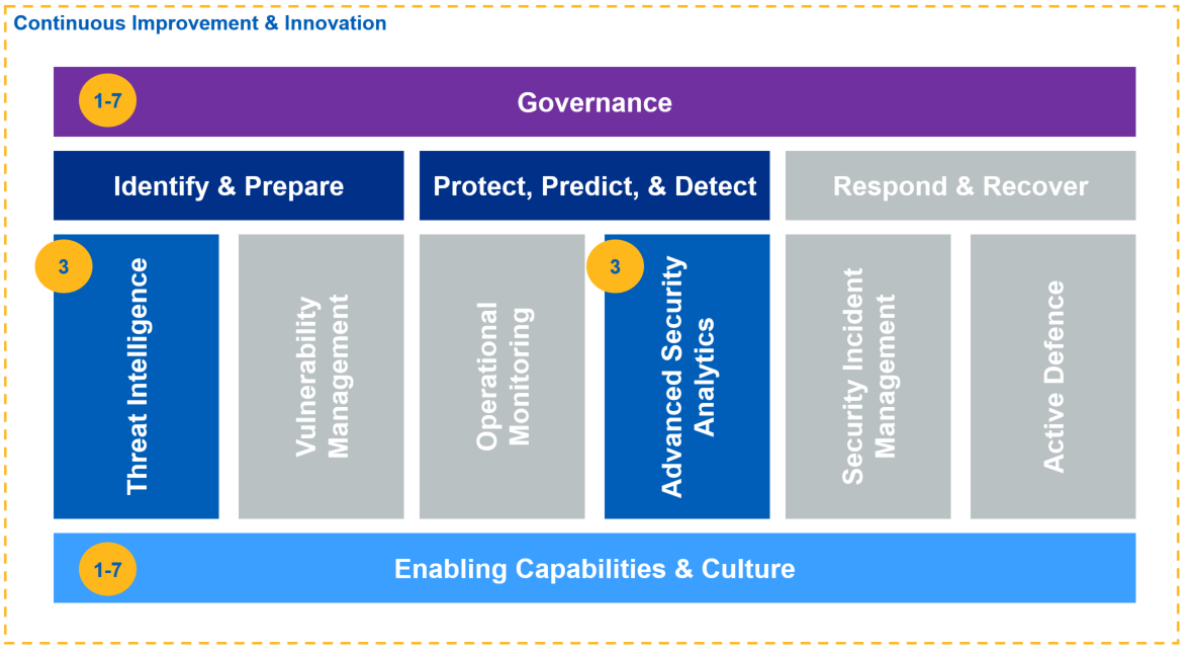

Figure 6: Mapping of the Understanding of the Strategic Threat section of the questionnaire onto the Foundational Capabilities Framework

Good practice will have a consistent process for identifying and contextualising threat and threat vectors specific to the healthcare sector. The country will have effective relationships between relevant intelligence agencies to gather and share threat intelligence and strategic threat vectors. This should be supported by robust advanced security analytics to actively monitor the threat landscape.

5.4. CYBER RESILIENCE, BUSINESS CONTINUITY AND DISASTER RECOVERY

This category covers how far a country understands the threat landscape and how it uses this knowledge to 'design for resilience' with the objective of limiting the impact of a cyber security incident. It involves critically assessing the effectiveness and efficiency of the ability to respond to and recover from a security incident or near miss.

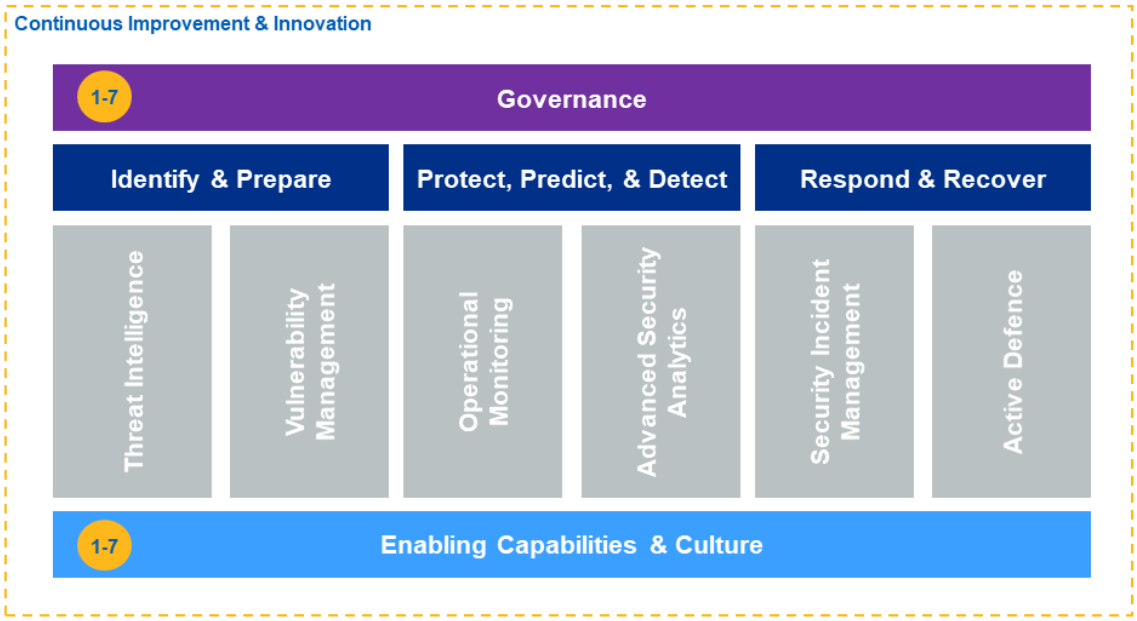

Figure 7: Mapping of the Cyber Resilience and Business Continuity and Disaster Recovery (BCDR) section of the questionnaire onto the Foundational Capabilities Framework

Good practice for this category defines a mature, secure methodology and regime that maintains resilience by design. The approach to resilience should be proportionate to the threat landscape so that this drives investment in the most effective and efficient sections of the healthcare sector.

5.5. BUDGETARY AND INVESTMENT PROPORTIONALITY AND EFFECTIVENESS

This category is about effectively and efficiently allocating funding across a country's cyber security program, threat landscape and clinical objectives. Expenditure and investment should be directly related to increasing cyber security posture and resilience across the whole ecosystem.

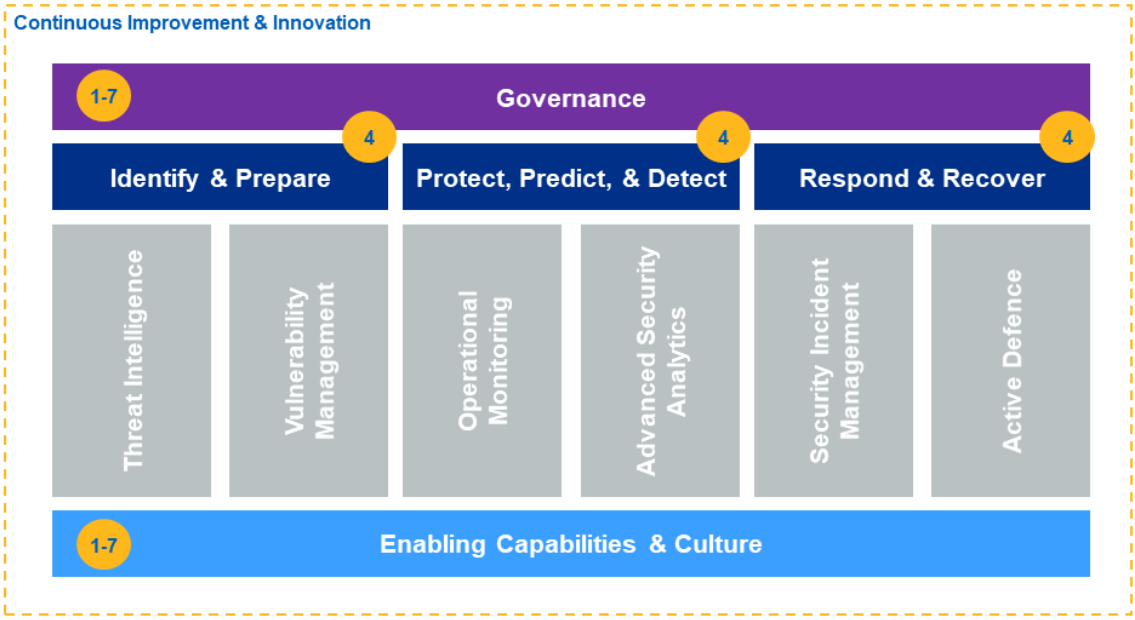

Figure 8: Mapping of the Budgetary and Investment Proportionality and Effectiveness section of the questionnaire onto the Foundational Capabilities Framework

Good practice should include robust financial metrics for cyber security and a regime of key performance indicators that tracks the effectiveness of this investment. Investment should be directly related to the risk and threat landscape and ring-fenced for the healthcare sector nationally and locally.

5.6. GOVERNANCE, CULTURE AND LEADERSHIP

Top-down structured support of security-conscious behaviours reinforced through a proportionate and effective governance structure. This category focuses on how well defined are the country's cyber security RACI (Responsible, Accountable, Consulted, Informed), culture, performance, and chain of command structures and mechanisms for health care. It is important because appropriate leadership drives the right behaviours and culture that impact all stages of the Foundational Capabilities Framework.

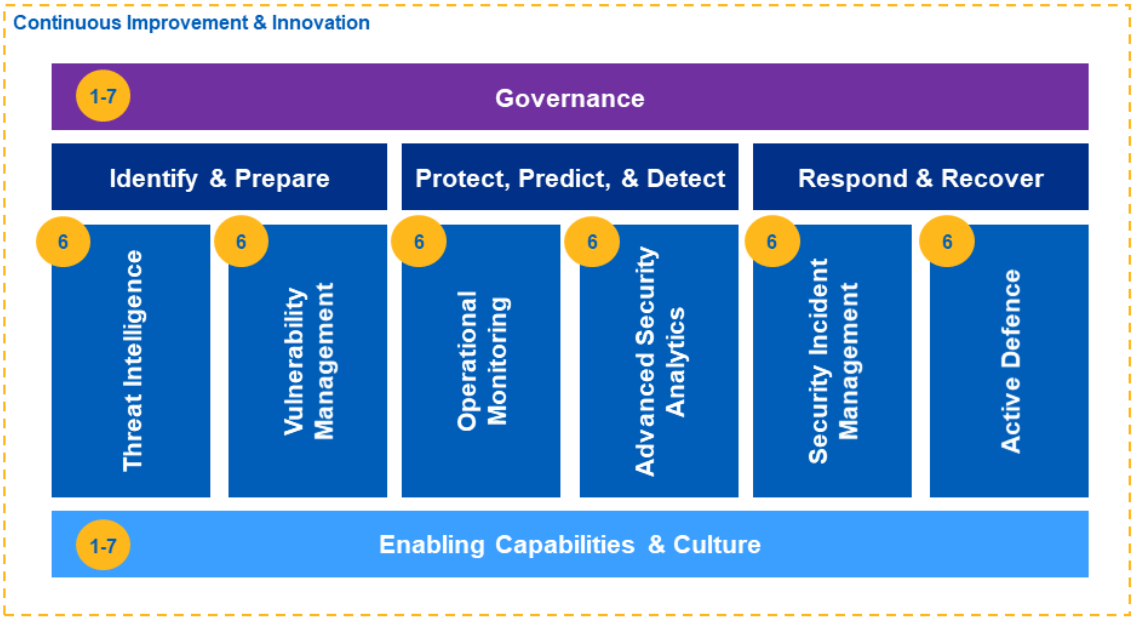

Figure 9: Mapping of the Governance, Culture, and Leadership section of the questionnaire onto the Foundational Capabilities Framework

Good practice will have a clear RACI for the chain of command for cyber security in health care with appropriate reporting and escalation channels defined for both business-as-usual and security incidents. This is supported with a clear governance structure, appropriate objectives for leadership, and delegated authority to enable agile responses to threats.

5.7. SUPPLY CHAIN RESILIENCE AND SECURITY

This category describes how effective, efficient, and comprehensive – in terms of coverage – is the country's security program across the supply base, and across the individual healthcare organisation's wider ecosystem. It is aimed at providing confidence in the security practices of partners, third parties, service providers and employees.

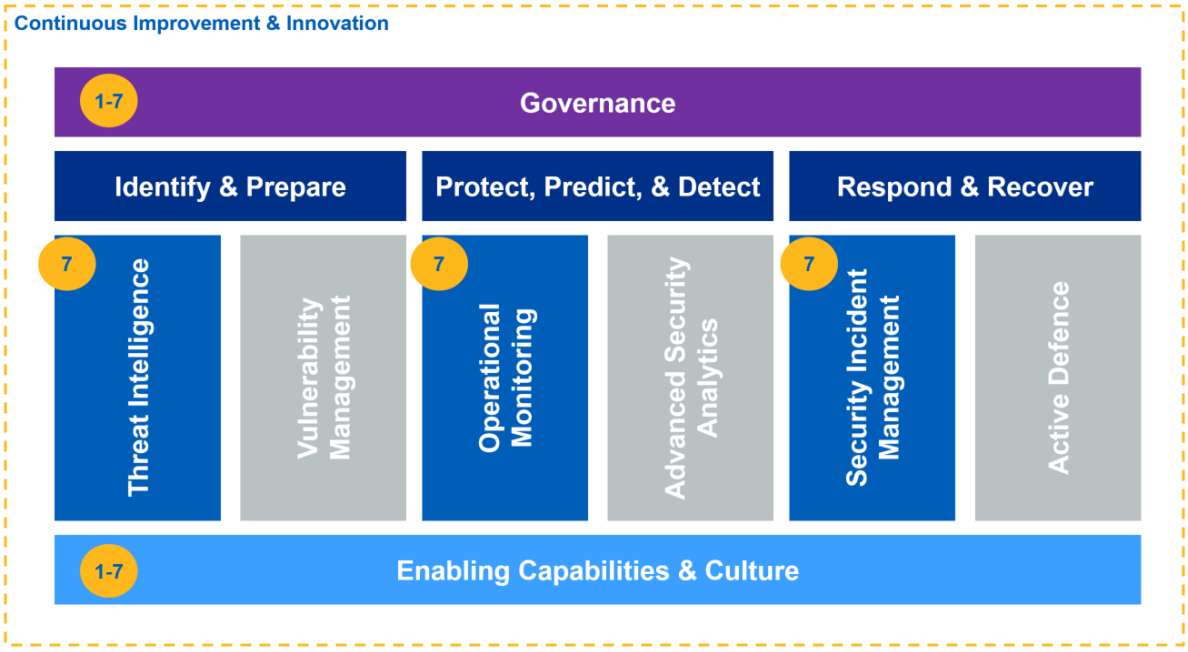

Figure 10: Mapping of the Supply Chain Resilience and Security section of the questionnaire onto the Foundational Capabilities Framework

Good practice has a holistic approach to the wider healthcare supply chain and ecosystem. The country should have proportionate systems in place to influence the supply chain and enforce penalties and punitive/corrective action with respect to cyber security incidents.

6 KEY FINDINGS FROM THE SURVEY

6.1. INTRODUCTION

The targeted questionnaire enabled participants to self-assess their maturity across the seven key categories. The questionnaire featured 59 targeted questions across the seven key categories and asked each participant to provide the following for each question:

1. Self-assess the current maturity against the question based on the common maturity model (0-5);
2. Provide a description of the evidence that could be provided to support the self-assessed maturity score;
3. Add any comments to gather qualitative data on each specific area of interest;
4. Estimate a potential maturity score in 18 months;
5. Provide a rationale for the predicted change in the maturity score in 18 months.

In order to account for unconscious bias and to normalise the result set, the framework calculated an average maturity score for each participant country against the seven key areas and used the following methodology to create minimum, mean and maximum values for each area:

- Individual participant country average for area: when no answer was provided for an individual question that question was ignored when calculating the average;
- Minimum value for key category: the minimum value considering the individual average of each participant country removing the lowest outlier (that is, the second lowest score);
- Mean value for key category: mean average of the individual average of each participant country removing 20 per cent of outliers (that is, removing highest and lowest outlier);
- Maximum value for key category: the maximum value considering the individual average of each participant country removing the highest outlier (that is, the second highest score).

6.2. KEY FINDINGS AND RESULTS

The results provided insight into both the current foundational capabilities and the focus of improvements for participants over the next 18 months. The key findings are:

Current maturity:

- The weakest capability categories are ‘Cyber resilience and business continuity and disaster recovery’ and ‘Supply chain resilience and security’. Not only are the mean values the lowest in these categories, the spread between minimum and maximum values for participants are the widest. This provides opportunities for some participants to share the approach in these areas or to form a joint collaborative approach. The supply chain can cross borders between participants, providing an opportunity for an international approach that builds on existing GDHP deliverables such as, the Code of Conduct, to help participating countries with more challenging scores accelerate their maturity in these spaces.

- The leading category is 'Understanding the strategic threat' with many participants using existing national capability and experience to accelerate the maturity of the healthcare sector. This also has the lowest spread between minimum and maximum values suggesting that all participants are at a similar level of maturity. This provides an opportunity to accelerate a threat intelligence sharing program between GDHP participants. With the delivery of the Threat Information sharing platform that has been delivered by the Cyber Security work stream, good progress has already been made. There is an opportunity over the next 18 months to embed, industrialise, and augment the operationalisation of this Threat Information sharing platform.

Planned maturity in 18 months:

- Very minimal improvement predicted in 'Cyber resilience and business continuity and disaster recovery'. This is critical for the availability of services in health care and needs to be a focus area for the GDHP.
- Significant improvement predicted by all participants in 'Supply chain resilience and security'. This provides an opportunity to combine approaches between participants to enable some to focus on other key areas.

6.3. CURRENT MATURITY

Figure 11 provides an overview of the current cyber security maturity across the participating countries. It provides an anonymised graphical representation of those that scored the highest and lowest by each area as well as providing an average score.

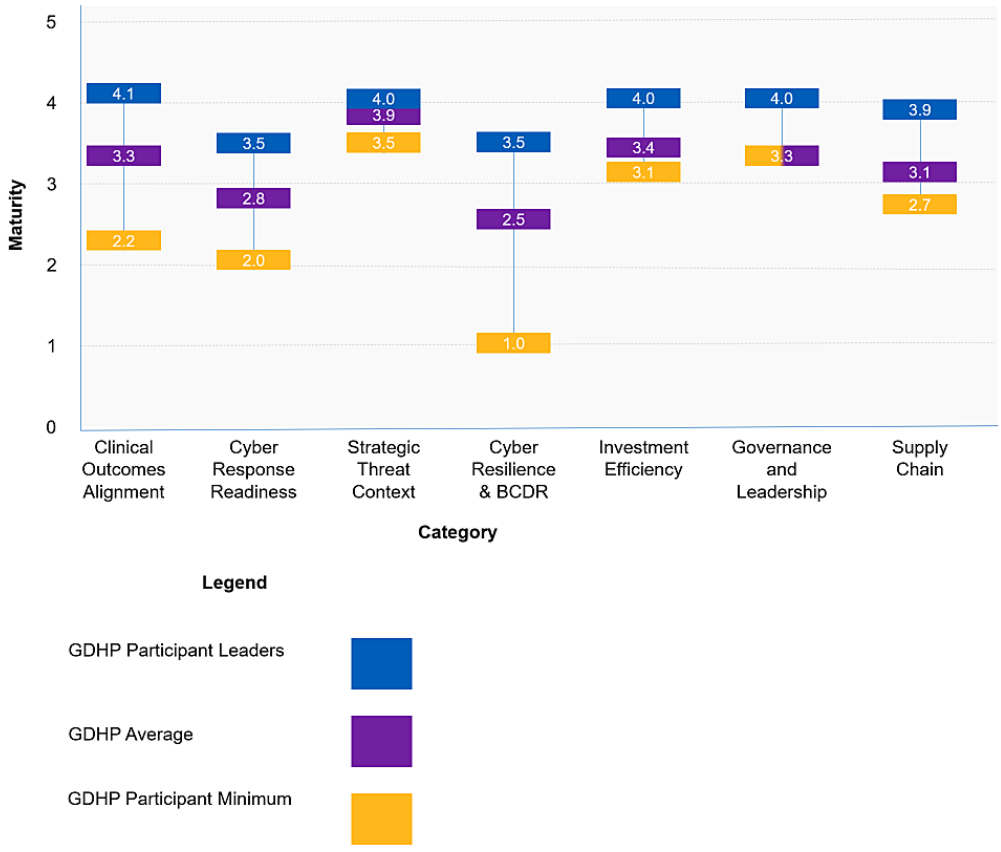

Figure 11: Overview of the current cyber security maturity of GDHP participant countries for each area of the questionnaire

A high-level overview of the underlying drivers and key observations for each area of inquiry found in Figure 11 is provided below.

1. Clinical outcomes alignment

- The use of security management processes that are specific to healthcare environments which help identify critical clinical assets and systems. This allows for a risk-led prioritisation of asset and network hardening, security control application, and risk mitigation.
- There are significant challenges in relating security threats effectively to clinical outcomes. This is driven by the difficulty in participating countries being able to translate and disseminate threat information and insights into actionable intelligence at both the technical and strategic levels and in a timely manner.
- There are significant challenges in ensuring security is seen as an enabler of clinical outcomes rather than just a pure IT risk. There is additional education and awareness needed across senior leadership to help them understand that cyber security risk is a genuine strategic business risk that, left untreated, can lead to catastrophic outcomes and the inability to deliver against core business objectives – in this case, the delivery of patient care and outcomes.

2. Cyber response readiness and recovery

- Defined escalation paths and incident escalation paths and plans are common across participating countries. The degree of testing and validation of these plans and paths does vary relatively widely even though review cycles appear to be comparatively consistent.
- Primarily only ad hoc testing for major incidents occurs rather than regular/periodic testing of either the whole incident response process or key elements of it.
- The structure of a number of incident response plans and processes follow, or are based upon, existing IT incident response rather than being cyber security-specific.

3. Understanding of the strategic threat

- Dedicated threat intelligence teams for the healthcare sector are common across participating countries which enables more targeted and specific intelligence to be created and disseminated to targeted recipients.
- While robust threat intelligence is in place across a majority of the participant base, there is a meaningful maturity gap between those participating countries that are able to contextualise the intelligence and those that are unable to do so at pace and scale. This means that a strategic and accurate view of the threat is not always available in a number of lower scoring participating countries.
- Support from agencies and law enforcement and cross-industry advisory groups is common across participants but the nature and depth of cooperation varies from participant to participant.

4. Cyber resilience and business continuity and disaster recovery

- Increased regulation (for example, European directives) is not directly improving capability and, in some cases, has the unintended consequence of driving a "tick box" culture of compliance rather than a cultural shift required to address a strategic business risk.
- There was generally less evidence produced for this section which implies that a number of the participating countries take an ad hoc approach to cyber resilience, business continuity and disaster recovery, and secure-by-design capabilities and obligations.
- Where evidence was provided by participating countries, it was strong on the whole and represented a secure-by-design and holistic approach to lifecycle design and implementation.

5. Budgetary and investment proportionality and effectiveness

- Participating countries tend to have a dedicated healthcare cyber security budget, but this isn't always distinct from IT budgets, thereby leading to overly technology-orientated investment profiles which leaves out the key people and process elements.
- In some participating countries, the cyber security budget and investment is controlled outside of health and is subject to a third-party government department control. While this allows for greater pooling of financial resources to some extent, it does reduce flexibility and control for healthcare authorities.
- Establishing a Return on Investment (RoI) metric and Key Performance Indicator (KPI) regimes to measure financial performance and efficiencies are a nearly universal challenge. This is unsurprising given that it is notoriously difficult to provide meaningful key performance indicators or metrics for return on investment for events that don't happen or are prevented.

6. Governance, culture and leadership

- There is some cross-over of responsibilities between the health sector and other government departments or law enforcement which leads to confusion or lack of clarity in terms of decision-making and risk ownership. There is a common theme of opportunities to further develop the system-wide and national-level operating model for cyber security within health care and ensuring that it complements and integrates with wider national cyber security structures and capabilities as appropriate.
- Generally speaking, chains of command are well-defined for national level incidents and events.
- An emerging trend of appointing chief security officers has emerged, but this needs to be further supported by board-level training and system-wide awareness regimes. System-wide awareness could be achieved through the development of a security policy which could feature access controls, audit controls, data integrity, authentication and transmission security.

7. Supply chain resilience and security

- Regulations such as the EU's General Data Protection Regulation are having the effect of increasing cyber security obligations in the supply chain. However, there is a lack of standardised wording and drafting of clauses and contractual

obligations which has the effect of introducing inconsistencies and, in some instances, absolving the supplier of liabilities and obligations.

- There is a lack of third party and vendor risk management standards and frameworks which are applied across ecosystems. This means that organisations are unable to fully understand their risk exposure across their supply base and external ecosystem.
- Contractual clauses and obligations as well as implementations of protections are primarily driven by data privacy rather than by cyber security concerns and obligations.

6.4. PLANNED MATURITY IN 18 MONTHS

Alongside the assessment of the current state, the questionnaire also asked participating countries to provide an initial assessment as to how they will score in the next year and a half. This was then evidenced to justify the prospective maturity scores. According to the result, the maturity of participants will increase from a score of 2.2 out of 5 to 3.2 average over the 18-month period. While this is ambitious, it is also eminently achievable and it highlights that the GDHP participant countries are not only taking cyber security seriously as an enabling concept, but they are also committing to aggressive improvement plans to tight timescales as they understand the changing nature and importance of the problem space.

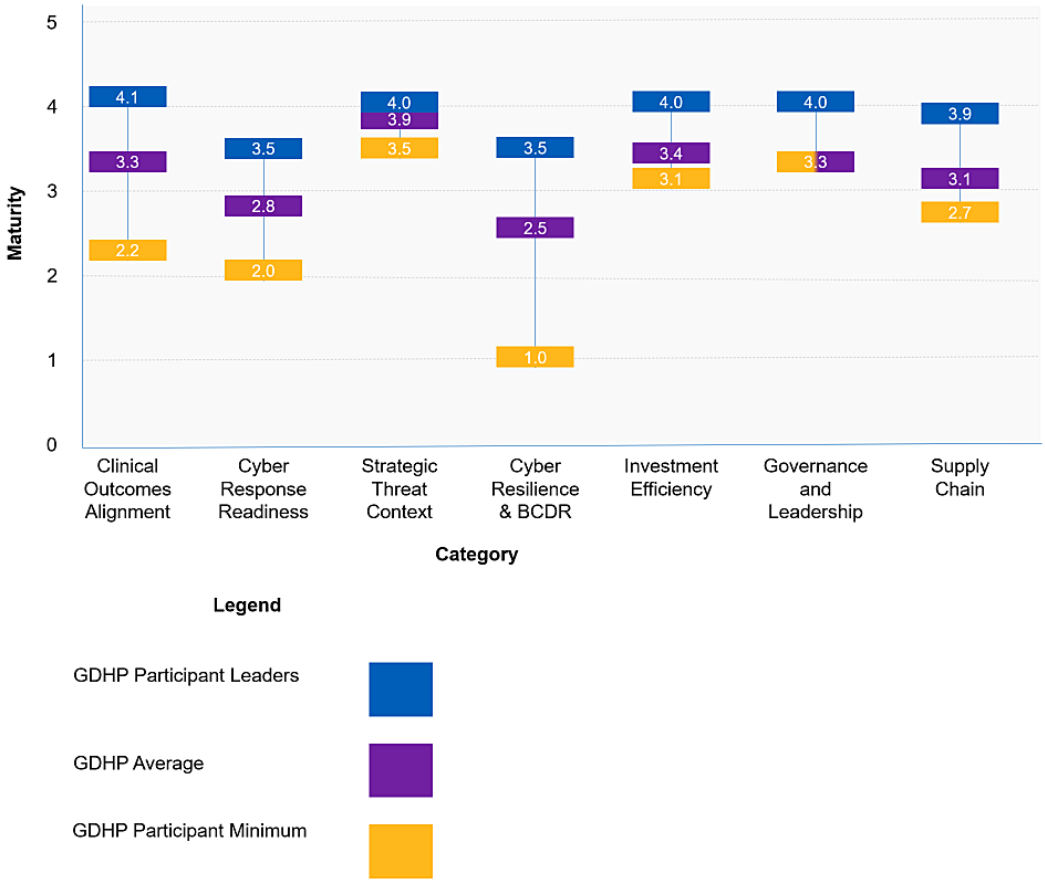

Figure 12: Overview of the planned cyber security maturity in 18 months of GDHP participant countries for each area of the questionnaire

A high-level overview of the underlying expected improvements and enhancements is provided below by category.

1. Clinical outcomes alignment

- Participants are updating and testing continuity plans and risk assessments to improve maturity and move towards performance measurements that align to clinical objectives and reflect criticality of clinical systems and services.
- Some participants that self-assessed lower scores did not provide an 18-month outlook providing an opportunity for leading participants to share approach to continuity planning and risk assessment.
- Significant efforts will continue to develop appropriate risk and performance regimes relating to cyber security and clinical/business outcomes. This includes a greater focus on automation and a providing appropriate information / data to different reporting groups to include (but not limited to): strategic and technical (current) towards tactical and operational decision makers.

2. Cyber response readiness and recovery

- Improvement scores relating to communications, protecting clinical assets, and test regimes did not increase as rapidly as other areas of the questionnaire. This indicates that either participating countries are not investing/concentrating in this space as much over the next 18 months or there is a lack of confidence in translating investments in these areas into meaningful maturity gains.
- Nearly half of the respondents did not provide answers to this section and some participants stated national security interests for not providing a self-assessment. This indicates an opportunity to create a secure environment for participants to share knowledge and information.
- A number of the responses indicated that there were planned renewal and updating exercises and efforts scheduled to be held within the next 18 months. This is encouraging as it demonstrates that the cyber security capabilities of a number of the participants will evolve over time to meet the changing business, technology, and threat environments.

3. Understanding of the strategic threat

- Some 70 per cent of respondents did not provide an 18-month outlook. The reason for this could be that participants have national threat intelligence programs that are wider than just health care or that participants are comfortable with the level of capability they currently have.
- The lowest scoring question is related to threat monitoring relevant to health care, providing an opportunity to build on the existing GDHP threat sharing platform specific to health care by forming additional standard operating procedures to drive uptake and collaborative usage.

4. Cyber resilience and buisiness continuity and disaster recovery

- Minimal improvement is forecast by participants and the spread between outliers in maturity is maintained, indicating weak confidence in this key category. The rationale is not immediately clear, but a working hypothesis is that business continuity and disaster recovery will continue to be “owned” and driven by traditional IT processes. Meanwhile, build and engineering standards

and processes will have cyber security and resilience addressed within the lifecycle, but not necessarily explicitly. The danger of this approach is that cyber security will continue to be seen as a "choke-point" within the design and build phases of development. Therefore, it will be susceptible to work-arounds and/or being avoided completely to ensure adherence to functionality, budget, or time.

- Secure-by-design consistently scores low in current state and outlook. This will become an increasing issue as the scale, importance, and interoperability requirements of new products, services and medical devices rapidly increases over the next 18 months and beyond.

5. Budgetary and investment proportionality and effectiveness

- Financial metrics and key performance indicators for cyber security are forecast to continue to score low. There is opportunity for outlier participant countries to share, as appropriate, relevant metrics for return on investment, regimes for key performance indicators, and reporting methodologies with the wider GDHP membership to help drive up the maturity score in a consistent and sustainable manner.
- Investment is not closely aligned to risk analysis. This creates the risk that investments may not be made in the highest risk areas and that investments will not be able to adjust in an agile way to adapt to the changing risk landscape.

6. Governance, culture and leadership

- Consistent improvements are predicted across all participants. The key improvements are focused on the establishment on new roles and chain of command for cyber security.
- A number of participating countries will bolster their cyber security operating model at a system-wide level to ensure that RACIs (responsible, accountable, consulted and informed) are aligned, clear, and known, which will drive operational efficiencies and effectiveness across cyber operations, delivery programmes, and risk management spheres.

7. Supply chain resilience and security

- Legacy contracts and products continue to cause a challenge, but participants are concentrating on ensuring new contracts and renewals are passing the correct obligations to the supply chain with appropriate penalties in place.
- The lowest maturity is in the area of medical device quality assurance regimes. Participants are relying on new international standards and regulations rather than developing/adapting existing standards and frameworks, given the changing definition of medical device (increasingly including software and firmware as well as the traditional hardware). This means that participants are not proactively addressing legacy connected medical devices in a systemic or sustainable manner. This is important given that many of the new standards and regulations do not have a retrospective/retroactive obligation within them and therefore only apply to devices procured and developed after the adoption date of the regulation. There is an opportunity to significantly shape this space through the GDHP via the Code of Conduct and other potential deliverables.

7 RECOMMENDATIONS AND NEXT STEPS

The results and findings of the Foundational Capabilities questionnaire have provided invaluable insight into the maturity of cyber security across the healthcare sector as well as identifying areas of significant opportunity and challenges that can be addressed. As part of the analysis, the research team identified a number of recommendations and next steps that were presented and discussed at the Hong Kong round of the GDHP and are outlined below in Table 2.

Table 2: Recommendations and next steps

#	Recommendation	Action/Next Step
1	To explore the concept of a pandemic and epidemic incident command centre for cyber security incidents that could leverage existing analogous structures from organisations such as the World Health Organization.	To have a further discussion with the GDHP cyber security work stream membership to scope the opportunity further so as to avoid accidental mission creep.
2	Set up working groups aligned to each of the inquiry categories under the questionnaire to establish and ingrain collaboration and accelerate knowledge sharing.	Leverage existing communal platforms already in use by the GDHP and refine them to enable "peer-to-peer" working across a variety of topics.
3	Collectively focus on maturing business continuity and disaster recovery capabilities and postures across GDHP participants so as to reduce the gulf between the poorest and strongest performers in this space.	Outlier participating countries to share – as appropriate – business continuity and disaster recovery templates, policy, process, and exercise examples.
4	Establish a common framework of key performance indicators and metrics to enable accurate, precise, and timely information from which decisions can be made and priorities agreed.	The GDHP Co-Chairs to identify and agree the lead participating country to own this action.
5	To build on the success of Internet of Things-enabled medical devices Code of Conduct and replicate it for the healthcare supply chain.	To explore the feasibility of designing a high-level conceptual framework from which a Code of Conduct for the supply chain can be developed and explored further.

Ultimately, it was acknowledged that not all the problem areas could be addressed through the GDHP, but it was agreed that three areas represented significant opportunity and collective benefit – threat information sharing; incident response; and management. These items have been added to the Cyber Security work stream's deliverable schedule and will be tracked as part of the GDHP initiative.

The activities resulting from the findings of the Foundational Capabilities questionnaire represent the next phase of GDHP's development in the cyber security domain insofar as they are evidence-based and specific to the GDHP community. The delivery of these actions and recommendations will provide significant benefit for GDHP participant countries, but it is also hoped it will act as a further proving of the benefit of this collective approach and encourage more countries to participate in this exciting, dynamic, and important work stream and initiative.

8 APPENDIX A: SAMPLE OF RESEARCH QUESTIONS

The table below shows a sample set of the questions used in the research.

#	Category	Example Question
1	Clinical Outcomes Alignment	How comprehensive is the identification of high-value assets?
2	Cyber Response Readiness	How mature is your country's defined cyber security incident escalation path?
3	Understanding the Strategic Threat Context	How mature is the country's ability to contextualise threats?
4	Cyber Resilience and Business Continuity and Disaster Recovery (BCDR)	How mature is the country's cyber security programme with respect to designing for resilience?
5	Budgetary and Investment Proportionality and Effectiveness	How mature is the KPI regime for investment in cyber security?
6	Governance, Culture, and Leadership	How mature is the country's reporting structure for cyber security for health and care?
7	Supply Chain Resilience and Security	How mature is the country's medical device quality assurance regime with respect to cyber security? (secure-by-design and testing standards for example)

9 GLOSSARY OF TERMS USED IN THE STUDY

Term	Definition
BCDR	Business continuity and disaster recovery
Continuity plans	A business continuity plan is a plan to help ensure that business processes can continue during a time of emergency, threat or disaster.
Cyber incident communications plan	A plan for how to disseminate, handle and respond to communications during a cyber incident.
Cyber incident response plan	A cyber incident response plan is a systematic and documented method of approaching and managing situations resulting from cyber security incidents or breaches. It is used to identify, respond to, limit and counteract cyber security incidents as they occur.
Cyber resilience	Cyber resilience is the ability to continuously deliver the intended outcome in the event of a cyber security incident.
Cyber response readiness	Cyber response readiness is the ability to respond rapidly and effectively to a cyber security incident.
Cyber security incident	A breach, or near miss, of the security rules for a system or service – most commonly: • Attempts to gain unauthorised access to a system and/or to data; • Unauthorised use of systems for the processing or storing of data; • Changes to a system's firmware, software or hardware without the system owner's consent; or • Malicious disruption and/or denial of service.
Delegated authority	Delegated authority is authority obtained from another entity that has authority. It is the division of authority and power downwards to the subordinate.

Term	Definition
Healthcare landscape	The totality of all elements that deliver or are integrated into the delivery of health care, including supporting services, integrated third-party suppliers, supply chains and frontline health services.
High-value assets	Any asset that has a high financial or resource impact if that asset was damaged, destroyed or misused.
Key clinical assets	Any asset that is critical to providing health care. If the asset is damaged, destroyed or misused this would significantly damage the quality and/or reliability of clinical care.
Key performance indicator	A key performance indicator (KPI) is a performance measurement that demonstrates how effectively an organisation is achieving a key business objective.
RACI	Identification of responsibilities of participants/stakeholders in the completion of an activity/task. Identifies who is Responsible, Accountable, Consulted and Informed.
Secure-by-design	The approach to software and hardware development that seeks to make systems as free of vulnerabilities and threat vectors as possible by considering security throughout the full design and development lifecycle.
Security obligations	Legal and/or regulatory security requirements that an organisation must adhere to.
Threat vector	A threat vector is the technique by which a vulnerability or threat is exploited.

GLOBAL DIGITAL HEALTH
PARTNERSHIP