Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren
Conférence des directrices et directeurs cantonaux de la santé
Conferenza delle direttrici e dei direttori cantonali della sanità

Factsheet

Study of Global Digital Health Partnership Cyber Security

Initial situation

The Global Digital Health Partnership (GDHP) was founded in 2018. It is a cooperation of different countries and their authorities, as well as the World Health Organization (WHO). Switzerland participates in this partnership. The aim of this partnership is to establish an exchange on best strategies and practices for digital health services and thus generate knowledge for the provision of better digital health services for the participating countries. Within the framework of this cooperation, white papers have been produced on various key topics, such as "interoperability", "cyber security", "evidence and evaluation" and "access by citizens to their health data".

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. Since the launch of this paper, the GDHP Cyber Security work stream participants have worked together to develop a Foundational Capabilities Framework (FCF).

This factsheet summarises the main findings of the 2020 report on cyber security[1]. The comments, facts and arguments belong to GDHP.

Aim of the research

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.

The primary aim of this research is to identify and understand common areas of opportunity and challenge. This research also provides participating countries the capability framework itself (FCF), which 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.

[1] Global Digital Health, *2020 Global Digital Health Partnership Launches White Papers*, https://www.gdhp.org/gdhp-whitepapers, accessed on 21st August 2020.

GCA
August 2020

Schwarzenburgstrasse 157
CH-3003 Bern

www.e-health-suisse.ch

ehealthsuisse
Kompetenz- und Koordinationsstelle von Bund und Kantonen
Centre de compétences et de coordination de la Confédération et des cantons
Centro di competenza e di coordinamento di Confederazione e Cantoni

The scope of this research paper covers seven core areas of inquiry. The questionnaire features 59 questions across these categories. 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.

Key Findings

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

Current maturity: The weakest capability categories are 'Cyber resilience and business continuity and disaster recovery' and 'Supply chain resilience and security'. GDHP recognise the needs to support countries with more challenging scores by encouraging international exchanges. 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. GDHP provides a Threat Information sharing platform, which has already enabled good progress and has the opportunity to support international exchanges.

Planned maturity in 18 months: 'Cyber resilience and business continuity and disaster recovery' do not stand in the center of preoccupation of the participating countries. Yet it is critical for the availability of services in health care. In the other hand, significant improvement are predicted by all participants in 'Supply chain resilience and security'.

1. Clinical outcomes alignment

Security management processes help to identify critical clinical assets and systems. Their use allows for a risk-led prioritisation of asset and network hardening, security control application, and risk mitigation. The main challenges are linked to security threats in the healthcare environments. This is due to the difficulty to disseminate threat information and insights into actionable intelligence at both the technical and strategic level in a timely manner. Other challenges lie in building education and awareness 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 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 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. Testing also tend to occurs after major incidents rather than being led regularly.

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, some do not possess a strategic and accurate view. 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. A number of the participating countries approach cyber resilience, business continuity and disaster recovery, and secure-by-design capabilities and obligations with specific questions.

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 others, 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.

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. 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.

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.

Contractual clauses and obligations as well as implementations of protections are primarily driven by data privacy rather than by cyber security concerns and obligations

Planned Maturity in 18 Months

Cyber security remains a sensitive subject. Planning, expectations, and evidences for the next 18 months are not shared easily by member states. However, they all expect to improve their competencies in clinical outcomes, risk assessments, and particularly their governance. The key improvements are focused on the establishment of new roles and chain of command for cyber security.

Finances, cyber resilience and disaster recovery are the weak points in future developments. For the latest, 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.

Finally, 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