1228556

Cybersecurity in Health

Towards a Global Agenda on Cybersecurity in Health

February 2021

KPMG

Dear sir/madam,

It is my pleasure to present the next level IoT Security initiative to shape a Global Agenda for Cybersecurity in Health.

Cybersecurity in Health is a major global challenge for this and the next decade. While solutions have already been developed in some places, still in many cases cybersecurity is not a priority. The need for a global healthcare cybersecurity agenda is evident to raise awareness, formulate major challenges, understand new technology and identify good practices.

Stakeholders need to collaborate on the major challenges identified by the global agenda to develop and amplify scalable solutions, and to accelerate the adoption of good practices.

Our call to action is to shape a Global Agenda to support the increase of cybersecurity in Health over the next years. Afterall, Cybersecurity is a shared responsibility. All stakeholders need to work together to increase safety for the patients.

Kind regards,

Annemarie Zielstra

Partner Cyber
KPMG Advisory N.V.

Contents

Towards a Global Agenda

History

Cybersecurity Solutions Progressing

Roadmap towards a Global Agenda

Point of Contact

Towards a Global Agenda

Cybersecurity in Health

The Covid-19 pandemic underscored and accelerated the transformation of our societies towards more cyber-dependencies. The good news is that many people continued working from home, that international operations continued at a much lower cost by reducing travel costs and carbon footprint, and faster adoption of new ways of working. But the bad news is that we are further increasing the attack surface for cyber criminals. The first fake vaccines were offered on the Dark Web in April 2020 and as vaccination programs are implemented it will be very difficult to distinguish the real from a fake. Cyber espionage with regard to vaccination information about the pharmaceutical industry has been a major challenge. While the hospitals were simultaneously put on edge because of the enormous number of patients. Combined with cyber attacks on hospitals in the recent past where sensitive data was leaked, for example during the SingHealth attack in Singapore, the GGD data breach in the Netherlands, or where hospitals were taken hostage by ransomware around the world.

The cybersecurity challenges of the next wave are being imposed by more and more medical devices connected to the internet, the so-called medical IoT devices.

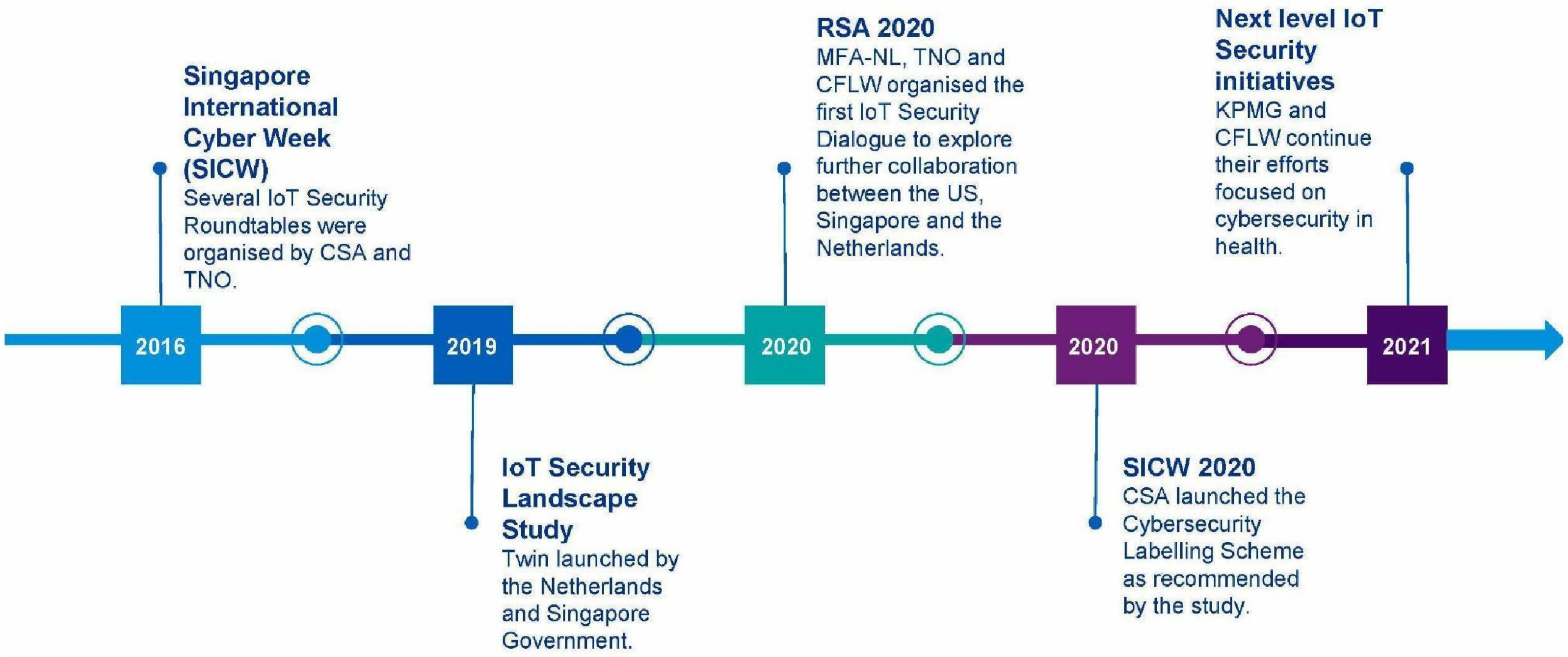
A global challenge

Although we have learned from the recent past that security is usually an aftermath of the device manufacturers targeting the time- to-market.

Cybersecurity in Health is a major global challenge for this and the next decade. While solutions have already been developed in some places, still in many cases cybersecurity is not a priority. The need for a global healthcare cybersecurity agenda is evident to raise awareness, formulate major challenges, understand new technology, and identify good practices.

Solving the cybersecurity challenges in healthcare is not just a matter for hospitals, insurance, the pharmaceutical industry or medical device manufacturers, but it is a shared responsibility of all stakeholders for these complicated matters.

History



2016

Singapore International Cyber Week (SICW)

Several IoT Security Roundtables were organised by CSA and TNO.

2019

IoT Security Landscape Study

Twin launched by the Netherlands and Singapore Government.

2020

RSA 2020

MFA-NL, TNO and CFLW organised the first IoT Security Dialogue to explore further collaboration between the US, Singapore and the Netherlands.

2020

SICW 2020

CSA launched the Cybersecurity Labelling Scheme as recommended by the study.

2021

Next level IoT Security initiatives

KPMG and CFLW continue their efforts focused on cybersecurity in health.

World Economic Forum identified lack of cybersecurity as one of the “key threats of the next decade”

Global Risks Report 2021

KPMG

Cybersecurity Solutions Progressing

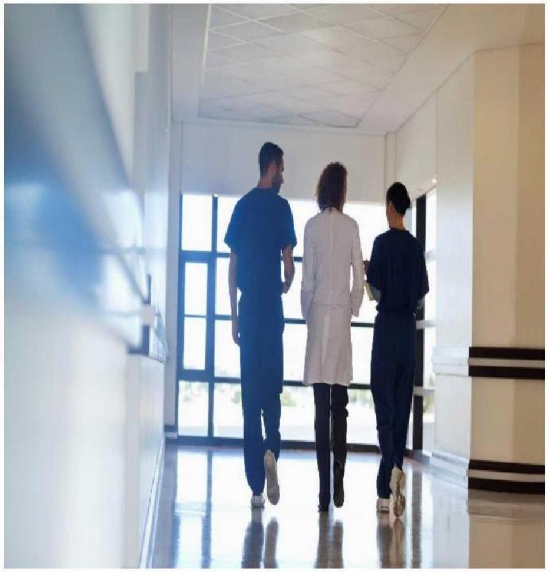
Security challenges in clinical

Simple malware like WannaCry and NotPetya made it painstakingly clear that even the regular IT in the administrational side of the medical world is already very vulnerable. To such an extent that hospitals globally had to delay intake or even move patients to other facilities. This is also confirmed when we perform security testing on medical facilities.

Unfortunately, if we move to the clinical network the cybersecurity problems get more serious and life threatening. Why is that?

It appears that till now the focus at medical devices was on availability and functioning, with easy to reset/configure functionality, and more and more connectivity. That came with a price, we uncovered during security testing, as we were able to modify or disrupt the functioning of critical (e)ICU equipment, (wireless) patient monitors, various imaging equipment, drugs storage and HIS interactions.

Also don't forget medical dispatch and comms systems; a code blue that goes unheard due to a cyberattack also costs valuable time; time that might be fatal.



Approach for security testing

Together with the Clinical Engineers, KPMG determines which devices can be tested on the Clinical Network, which in the simulation lab, and which should be tested standalone.

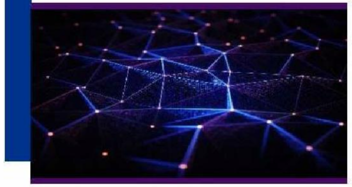
As the security of the devices is only as strong as the weakest link, it is important to assess the security of the clinical network as a whole. A device on its own might be 'secure', but when it communicates with the central console it might expose weak communication. Or as some hospitals have good procedures, and wipe and restore the firmware after each ICU use, what if the central firmware image is compromised? Suddenly all ICU devices are non-functioning.

KPMG uses for the clinical world the same methodology as in use for testing critical industrial environments of our international clients. Depending on the criticality of the environment this includes full packet logging, local firewalls, rate limiting, and a very experienced team in close contact with the clinical engineers. For every test we complement contextual reviews, with manual inspections of the device, as well as security testing on the hardware and the underlying communication (both ends).

Roadmap towards a Global Agenda

Multi-stakeholder Ecosystem

Together, we create a trusted network of public and private organisations, so we can address and push the limits of what's necessary.



IoT Security Dialogue

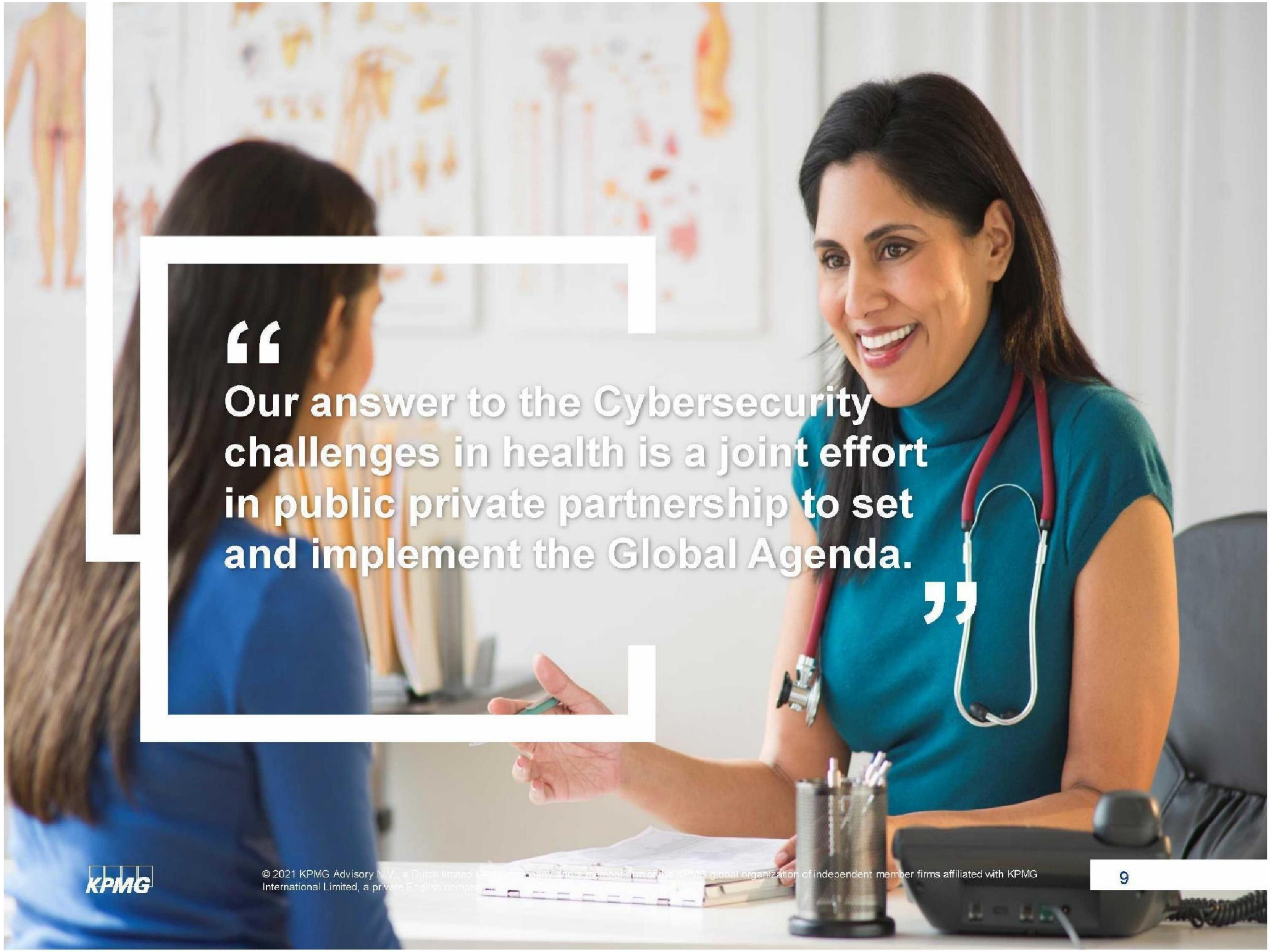
The IoT Security Dialogue will focus on understanding and making recommendations on addressing the cybersecurity challenges.

Report with recommendations

A report will be published with concrete recommendations to implement the cybersecurity agenda in healthcare. Our ambition is to create high-level co-ownership for this report, preferably with the World Economic Forum.

A Global Agenda

Together, we're creating a global agenda, so we can challenge the different cybersecurity threats in health.



> “Our answer to the Cybersecurity challenges in health is a joint effort in public private partnership to set and implement the Global Agenda.”

Point of Contact

5.1.2e

5.1.2e

5.1.2e

5.1.2e

5.1.2e

5.1.2e

5.1.2e

5.1.2e