Original Article

The cyber-risk in cardiology: towards an investigation on the self-perception among the cardiologists

Daniele Giansanti[1], Lisa Monoscalco[2]

[1]ISS, Centro TISP, Roma, Italy; [2]Università di Tor Vergata, Roma , Italy

Contributions: (I) Conception and design: All authors; (II) Administrative support: None; (III) Provision of study materials or patients: All authors; (IV) Collection and assembly of data: All; (V) Data analysis and interpretation: All authors; (VI) Manuscript writing: All authors; (VII) Final approval of manuscript: All authors.

Correspondence to: Daniele Giansanti. ISS, Centro TISP, Roma, Italy. Email: gianslele@gmail.com; daniele.giansanti@iss.it.

Background: The strong demand for health data by cybercrime exposes hospital structures in particular to IT risks. The greater connectivity to existing IT networks has in fact exposed Administrations to new IT security vulnerabilities, as healthcare is an extremely interesting target for cybercrime for two fundamental reasons: on the one hand, it is a source rich in valuable data and on the other, very often, the defenses are weak.

Methods: The general purpose of the study was to investigate the cybersecurity in cardiology, a strategic field of the health care. The specific purpose of the study was: (I) to perform a first overview in this field; and (II) to investigate the opinion on the cyber-risk in cardiology directly interviewing the actors working in this field, using a properly designed questionnaire submitted using mobile technology.

Results: Fifty seven cardiologists participated in the study and filled the proposed questionnaire on their smartphone/tablet. From a global point of view the output of this work allowed to highlight some important issues related to the perception of the cybersecurity specifically on the actors working in the field of the cardiology as for example their opinion on the received and/or needed training.

Conclusions: A properly designed questionnaire has been: (I) proposed to investigate the perception of the cybersecurity among subjects working in cardiology; (II) successfully submitted to 57 cardiologists highlighting some critically important issues.

Keywords: Cybersecurity; e-health; medical devices; cardiology

Received: 25 September 2019; Accepted: 18 January 2020; Published: 20 April 2021.

doi: 10.21037/mhealth.2020.01.08

View this article at: http://dx.doi.org/10.21037/mhealth.2020.01.08

Introduction

Cybersecurity in health care

Cybersecurity in the healthcare faces four main aspects in the cyber-system that can be either a complex medical device (1-12) and/or a complex interoperable and heterogeneous system embedding different components with informatics, mechanics, electronics, networks (13-15).

The data preservation

It is the need to ensure that digital information of prolonged value remains accessible and usable.

The data access and modification

Refers to those typical activities such as storing and recovering data stored in databases or other archives. For the execution of these actions, functions such as authentication and authorization are fundamental.

The data exchange

Data exchange can be carried out either internally (for example by involving two or more parties belonging to the same health institution) or externally (for example involving multiple stakeholders belonging to different health institutions, possibly present in different countries).

The exchange of data should take place in compliance with predetermined security requirements and provide for the implementation of adequate information protection measures.

The interoperability and compliance

Interoperability allows you to establish to what extent systems and devices are able to exchange data and interpret shared information. In order for two systems to be interoperable, they must be able to exchange data and subsequently present that data so that it is understandable by a user. Compliance, on the other hand, refers to the adoption of the same standards, as well as compliance with the regulations (both nationally and internationally) relating to the use of health data.

The risks of cyber-attacks in healthcare

The strong demand for health data by cybercrime exposes hospital structures in particular to IT risks. The greater connectivity to existing IT networks has in fact exposed Administrations to new IT security vulnerabilities, as healthcare is an extremely interesting target for cybercrime for two fundamental reasons: on the one hand, it is a source rich in valuable data and on the other, very often, the defenses are weak. Data breach violations can be caused by accidental events (e.g., loss of a USB stick or unregulated access to data) or malicious, and can result in the theft of health information, attacks of ransomware to hospitals (13-15), denial of service attacks and attacks on implanted medical devices [such as pace-makers (7-12) or artificial pancreas (1-6)] which can reduce patient confidence, paralyze health systems and threaten human life. Ultimately, cyber security is critical to patient safety, but has often been underestimated. This requires cyber security to become an integral part of patient safety through changes in human behavior, technology and processes as part of a holistic solution. Also because we must not forget that the health system is a complex system in which multiple factors, heterogeneous and dynamic, interact, including the plurality of health services, specialist skills and professional, technical-health and economic-administrative roles and the heterogeneity of the processes and results to be achieved. All the elements of the system must integrate and coordinate, to respond to the patient's care needs and ensure the best possible care, as threats and safety hazards that can come to have can also be hidden between the folds of this dynamism and heterogeneity. Reflections on the "Clinical risk" (i.e., the possibility that a patient suffers involuntary damage or discomfort, attributable to health care) related to this are strongly needed. Indeed the clinical risk may cause an extension of the period of hospitalization, a worsening of health conditions or even, in extreme but possible cases, death (for example, think of a computer attack that hides, cancels, alters or exchanges patient information, effectively preventing the provision of adequate care). Of course, threats and vulnerabilities cannot be completely eliminated, so reducing security risks is particularly challenging. Furthermore, specific regulations are continuously evolving in this field, as in USA and Europe (16,17).

Purpose

The general purpose of the study was to investigate the cybersecurity in cardiology, a strategic field of the health care for the very high technological content both of the medical devices and the components of the care-systems.

The specific purpose of the study was:

(I) To perform a first overview in the field of the cardiology and;

(II) To investigate the opinion on the cyber-risk in cardiology directly interviewing the actors working in this field, using properly designed questionnaires delivered by means of the mobile technology.

Methods

The overview was conducted through the WEB and publication databases. The investigation of the opinion of the actors working in cardiology was performed by means of properly designed questionnaires. These questionnaires faced all the aspects of the cybersecurity that an actor working in this field can meet. The proposed questionnaires were therefore specific for the heart-care. They were rearranged starting from a previous version proposed at the Medicon 2019 (18); were developed using the software Microsoft-Forms and submitted to 57 cardiologists using WhatsApp to send the internet pointer.

Results and discussion

The overview to the cyber-risk in cardiology

In the challenge that sees doctors and administrators engaged in improving care in cardiology it is essential that the professionals and patients can securely exchange

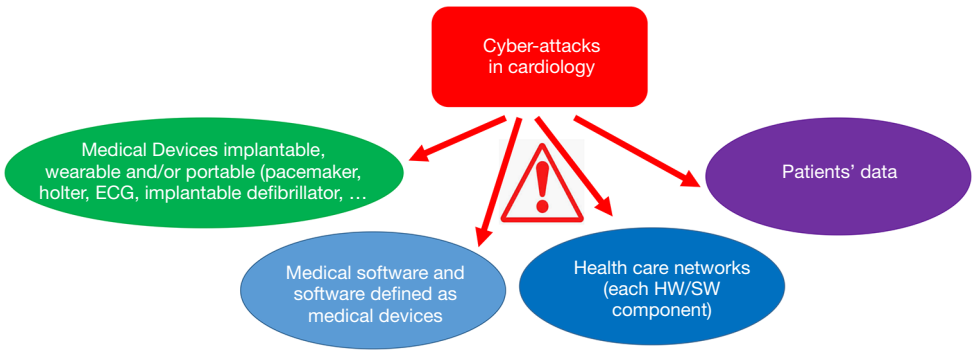

Figure 1 Sectors of the cardiology affected by the cyber-attacks.

reliable health information. The set of information and communication technologies (ICT) that allow remote processing and exchange of information in digital format is constantly evolving and cardiologists are among the main ones users: the use of remote monitoring, remote consultation, Apps is already a reality in cardiology. The recent discussions in cardiology have given a great importance to *m-Health* & *e-Health* recognizing that these technological revolutions will have a major impact on patients' lives and the way people work. The use of these new technologies, of course, cannot be separated from people's rights, in particular from those related to the protection of personal data, for example in Europe in view of the new European Regulation on the "Date Protection" (privacy), which specifies responsibilities and penalties for sector operators. Many giant steps have been taken in cardiology regarding technologies since the days of the electromechanical electrocardiogram with nibs. Today cardiology uses exceptional wearable medical devices such as pacemakers, wearable digital holters, implantable defibrillators and other wearable and portable devices. However, all these technologies open cardiology to a whole new set of cyber security risks that were once unthinkable. FDA has shown that there are more than 350 thousand cardiac devices at risk of cyber-attacks (7-12), showing informatic vulnerabilities. Of course, cardiology makes use, as in the case of other disciplines, of all the advantages offered by digital imaging, data networks and new decision support and classification softwares, with the same cyber-risk (13-15). *Figure 1* resumes the sectors of cyber-attacks in cardiology.

The use of the electromechanical electrocardiogram with nibs, although today considered antiquated, did not present risks from cyber attacks.

It has been shown today that for example (7-12):

Digital electrocadiograms can undergo cyber attacks: the display of an electrocardiogram under cyber attack can show untrue traces that lead the clinician to administer incorrect therapy.

Pacemakers, which are now opened to network connections to allow remote re-programming, can be subjected to various types of attacks, from those ones that cause them to drain the battery to those ones that induce an incorrect response.

Both in USA and in Europe the attention is high. Properly regulations have been proposed (16,17) involving also the field of the cybersecurity in cardiology.

The questionnaire

The design

The internet pointer of the questionnaire (QR) developed by means of Microsoft-Forms is the following one:

https://forms.office.com/Pages/ResponsePage.aspx?id=DQSIkWdsW0yxEjajBLZtrQAAAAAAAAAAAAZ__gdk7kpUQ1AxV0xTOUxaM0RLUVIyTUZBSFlESUFYOC4u.

The Quick Response code is available in *Figure 2*. *Figure 3* shows the initial section and the starting of the specialist section of the QR dedicated to the cardiologists.

The output of the submission

Several questions were proposed with graded scores (1= minimum, 5= maximum). The submission to 57 cardiologists, also conducted to verify the robustness of the method did not show criticalities in the distribution and collection on the net. At the moment the sample is growing. Targeted data mining will follow. From a first

Figure 2 The Quick response code associated to the questionnaire.

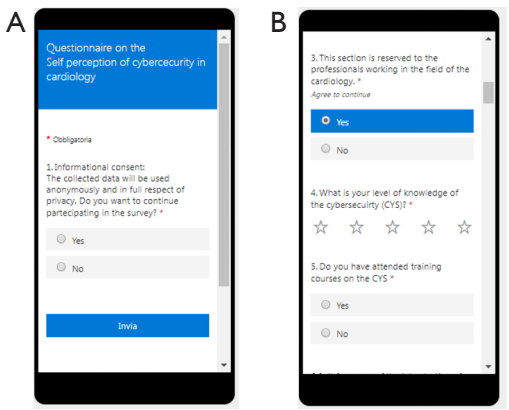

Figure 3 Two print screens from the survey. (A) The initial section of the questionnaire. (B) The starting of the specialist section dedicated to the cardiology.

analysis we highlight: (I) a safety self-perception in one's own environment to 3.58; (II) a desire to invest in training in this area to 4.01. The general knowledge related to cybersecurity received a score of 3.65. Most respondents (93%) say that despite the digitalization of the health sector has brought security problems, the benefits it has brought they are higher than the possible risks; only 33% believe that the initiatives intended to cybersecurity are adequate; only 39% attended training courses and 74% advocate the introduction of specific courses.

Conclusions

The greater connectivity to existing IT networks is exposing the Administrations to new IT security vulnerabilities, as healthcare is an extremely interesting target for cybercrime for two fundamental reasons: on the one hand, it is a source rich in valuable data and on the other, very often, the defenses are weak. The study investigated the cybersecurity in cardiology, a strategic field of the health care. In particular the study performed a first overview in this field and investigated the opinion on the cyber-risk in cardiology directly interviewing the actors working in this field, using properly designed questionnaires designed using Microsoft-forms. Fifty seven cardiologists were recruited in the study and filled the proposed questionnaire. From a global point of view the study allowed to highlight some important issues related to the perception of the cybersecurity in cardiology as specifically perceived by the actors working in the field of the cardiology. The next steps will consider several directions such as:

(I) The investigation on further strategic fields of the digital health such as the digital radiology and the digital pathology.
(II) The involving of a high number of subjects in the study, asking aid to the scientific societies.
(III) The interaction with the stake-holders.

Acknowledgments

Funding: None.

Footnote

Conflicts of Interest: Both authors have completed the ICMJE uniform disclosure form (available at http://dx.doi.org/10.21037/mhealth.2020.01.08). The authors have no conflicts of interest to declare.

Ethical Statement: The authors are accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

References

1. O'Keeffe DT, Maraka S, Basu A, et al. Cybersecurity in Artificial Pancreas Experiments. Diabetes Technol Ther 2015;17:664-6.

2. Doyle FJ, Huyett LM, Bok Lee J, et al. Closed-loop artificial pancreas systems: engineering the al-gorithms. Diabetes Care 2014;37:1191-7.
3. Picton PE, Yeung M, Hamming N, et al. Advancement of the artificial pancreas through the development of interoperability standards. J Diabetes Sci Technol 2013;7:1066-70.
4. Maisel WH, Kohno T. Improving the security and privacy of implantable medical devices. N Engl J Med 2010;362:1164-6.
5. Food and Drug Administration: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices—Guidance for Industry and Food and Drug Ad-ministration Staff. Available online: www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf (ac-cessed March1, 2015).
6. Public Workshop—Collaborative Approaches for Medical Device and Healthcare Cybersecurity, October 21–22, 2014, Arlington VA. Available online: www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm412979.htm (accessed March1, 2015).
7. Baranchuk A, Alexander B, Campbell D et al. Pacemaker Cybersecurity. Circulation 2018;138:1272-3.
8. Muddy Waters Capital LLC. MW is short St. Jude Medical (STJ:US). Muddy Waters Research.2016. Available online: https://d.muddywatersresearch.com/research/stj/mw-is-short-stj/. Accessed February 13, 2018. Google Scholar.
9. Baranchuk A, Refaat MM, Patton KK, et al. American College of Cardiology's Electrophysiology Section Leadership. Cybersecurity for cardiac implantable electronic devices: what should you know? J Am Coll Cardiol 2018; 71:1284-8.
10. U.S. Food and Drug Administration. Cybersecurity vulnerabilities identified in St. Jude Medical's implantable cardiac devices and Merlin@home transmitter: FDA safety communication. U.S. Food and Drug Administration.2017. Available online: https://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm535843.htm. Accessed February 13, 2018.Google Scholar.
11. Kramer DB, Fu K. Cybersecurity concerns and medical devices: lessons from a pacemaker advisory. JAMA 2017; 318:2077-8.
12. Ransford B, Kramer DB, Foo Kune D, et al. Cybersecurity and medical devices: a practical guide for cardiac electrophysiologists. Pacing Clin Electrophysiol 2017; 40:913-7.
13. Kruse CS, Frederick B, Jacobson T, et al. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technol Health CareCW Jobs (Internet). London, UK: 2016. Cyber crime timeline; Available online: http://www.cwjobs.co.uk/careers-advice/itglossary/cyber-crime-timeline. Accessed: 2016-08-09.
14. Coronado AJ, Wong TL. Healthcare cybersecurity risk management: keys to an effective plan. Biomed Instrum Technol 2014;(Suppl):26-30.
15. Loughlin S, Fu K, Gee T, et al. A roundtable discussion: safeguarding information and resources against emerging cybersecurity threats. Biomed Instrum Technol. 2014; 8-17. Available online: 10.2345/0899-8205-48.s
16. Postmarket Management of Cybersecurity in Medical Devices.Available online: http://bit.ly/2nOYGB8
17. The general data protection regulation applies in all Member States from 25 May 2018. Available online: https://eur-lex.europa.eu/content/news/general-data-protection-regulation-GDPR-applies-from-25-May-2018.html
18. Giansanti D, Grigioni M, Monoscalco L, et al. A Smartphone Based Survey to Investigate the Cyber-Risk Perception on the Health-Care Professionals MEDICON 2019: XV Mediterranean Conference on Medical and Biological Engineering and Computing – MEDICON 2019 pp 914-923-IFMBE Proceedings, Volume 76.

doi: 10.21037/mhealth.2020.01.08
Cite this article as: Giansanti D, Monoscalco L. The cyber-risk in cardiology: towards an investigation on the self-perception among the cardiologists. mHealth 2021;7:28.