An overview of cybersecurity in the healthcare sector

Aurelian Buzdugan
National Nuclear Security Support Center,
Technical University of Moldova
Chisinau, Moldova
aurelian.buzdugan@yahoo.com

***Abstract* — Cybersecurity has become in last decade one of the most discussed subjects in various domains. Besides the traditional IT area of which one would usually think of when discussing about cybersecurity, it has now evolved and is part of almost all other domains using computer technologies. For example, the nuclear domain takes into account the cyber security subject due to the large number and complex infrastructure of computer systems that are now part of nuclear facilities or physical security systems. The recommendations coming from the international level to include cyber security aspects in the nuclear related legislation can now be seen in practice in many countries. For example, the Regulation of Physical Security for Nuclear includes such recommendations and best practices from the IAEA [1].**

However, other evolving domains that heavily rely on computerized systems have not yet fully taken into account the current cyber risks nor included most of these requirements. As for example, the healthcare domain has now a multitude of technologies that are embedded in medical devices for controlling, monitoring the treatment, as well as keeping medical history of patients. Another important aspect of the use of computer technologies is the exchange of medical data such as x-ray images with specialists from other institutions in order to have a timely diagnosis. Such medical technologies can be seen nowadays not only in developed countries, which means global actions are needed to tackle the cyber risks that come along with such technologies.

In this paper, we will discuss over the necessity of actions in order to adjust and update the specific national and international frameworks as a response to the current cybersecurity status in domains that embed computer systems.

***Key words* — cyber security, healthcare, medical imaging, hybrid regulation.**

I. Introduction

A lot of states have already developed or are developing their cybersecurity strategy and respective legal framework. Acknowledging the risks from the cyber space and the potential impact for the economy, society or government is one of the first motivators for establishing and maintaining a cyber security status. The definition of cyber security is still debatable among different parties but is linked to the idea of having a certain protection against misuse of electronic data or measures taken to defend against intentional harm [2]. These measures can be taken at different level – such as administrative level, via a policy or guideline up to technical implementation such as systems or controls. All of these have the goal to defend against potential attacks from the cyber space, both intentional as well as unintentional. Cybersecurity was primarily linked to the IT domain or computers before. Today this is also true, however we have to take into account that most of the domains besides IT, such as nuclear/radiological, healthcare, automotive and other have registered a tremendous growth and development mostly due to the opportunities that computers and processing power has to offer. Therefore, the best practices and requirements that normally would apply to the IT domain or software have also to be taken into account by other domains from the moment when computer systems become part of that domain. Unfortunately, this was not always the case and some of the development related to cyber security occurred after certain events. For example, incidents linked to Stuxnet, WannaCry or Petya, which had as target various industrial control systems, have proved that all industries could be impacted by advanced cyber-attacks. If we go back one decade probably not many would think of such risks when developing or using these new computerized systems in these domains. With the tremendous number increase of computer systems due to technological convenience the risks have another dimension in present. Many of these systems in non-IT domains have not been designed taking cyber security into account, and rather focusing on functions and automation.

In this paper we want to argue the necessity of standardizing cyber security requirements among all domains within a country and having a strong horizontal cooperation at the national level. We will take the healthcare domain as an example, as we believe this domain has developed recently and offers a lot of new technologies that are based in entirety or rely partially to computer systems, and therefore create new risks for this domain [3]. This paper is a **tentative** to extend to other fields of the analysis presented at the 3rd International Conference on Health Technology Management from 2016 [4].

II. Cybersecurity in Healthcare

Most of us have realized the commodity offered by an electronic patient record, so that each time we go to a clinic the practitioners would have access to all our medical data. Many of the medical devices such as X-rays, MRIs store the output in a digital format and could be automatically be saved to our electronic medical record. Most of these systems have been designed and implemented in order to use computers for managing day-to-day activities in healthcare, as this was and is considered to be innovative. Unfortunately, the cyber security risks and lessons learned from other domains, such as nuclear and radiological have not been taken into account until recently in healthcare. The same statement can also be true about other domains that make use of computer chips and programs to improve or offer new features.

If we look at the usual healthcare institutions – these usually have a relative large IT network with a high number of connected devices, few IT staff and the priority being data availability. Unfortunately, this statement can be true for a large number of healthcare institutions, especially for countries where there is no clear cyber security framework which would define the responsibilities for ensuring cyber security. The healthcare IT case becomes even more complex with the introduction of wireless networks, public facing websites or interconnectivity with other institutions. Comparing this to a traditional organization with an IT infrastructure it can be easily stated that the footprint of all these technologies is large and requires a lot of resources to ensure these systems are kept up to date and properly configured. In addition, the traditional IT systems used in most of organizations that have acknowledged already the cyber security risks, such as in finance sector, still lack a proper vulnerability management or asset control. The financial domain is one of the leaders in the use and implementation of technologies and policies in order to ensure the security of the data, due to the high value of this data. However, the data generated and used in the healthcare domain, such as electronic patient records, is also valuable as it could be used for a large number of scenarios. Unfortunately, most of such medical data has inadequate security controls applied for protecting it and monitoring its use. It can also be the case that basic authentication or authorization controls might be missing. Furthermore, the security culture in this domain can be assessed as low, therefore usual type of attacks such as sending spear phishing emails could offer easy control for an attacker to find and misuse the data from healthcare institutions. The WannaCry ransomware attack from 2017, which encrypted user's data and asked for a ransom for the decryption code, has also affected healthcare sector [6]. The impact of having data unusable in healthcare domain can have disastrous consequences. It goes without saying that any deviation in the radiation dose used, misfunction of vital sign monitoring systems or lack of previous medical history could have an imminent impact on people's life.

III. Conclusions

If we refer to the regulatory frameworks in place, it is necessary to mention that there has to be more horizontal cooperation than now at the national level. Looking at the nuclear and radiological domain, where cyber security aspects have been included as part of ensuring a nuclear security regime, as well as technical requirements for operators in handling sensitive data or implementing physical security systems, it can be observed that some cyber security aspects could be performed by the regulatory body from the IT domain. We would like to reiterate the necessity of cross cooperation between domains that use IT technologies and cyber security specialists in order to properly define and evaluate such technical controls, due the specific knowledge needed. This was a recommendation for the specific case of nuclear/radiological domain and cyber security, however could be applied as well for healthcare [5]. Many of the cyber risks could be minimized nowadays if cyber security would be included as a requirement from the design of such systems by the vendors. Such requirements can also be set at the issuance of a license or authorization, as well as at the accreditation process for medical institutions. One solution would be the hybrid regulation for authorization, licensing or accreditation, that would be done by the respective regulatory body, for example from the healthcare domain, supported by the institution which can provide subject matter expertise and regulation from the cyber security domain.

An important role in the development and implementation of cyber security in other branches, such as healthcare, has to be taken by the educational institutions as well. For example, the Computers, Informatics and Microelectronics Faculty from the Technical University of Moldova could offer specialized cyber security courses for other faculties, due to the links this topic has with other domains. Therefore, enabling national and international organizations to come with cyber related requirements and best practices is a key action to be seen in all domains. The complexity of nowadays IT infrastructure is so high as it connects the majority of devices from various domains, many of which were not developed and designed to resist against cyber attacks. Therefore, cooperation and actions taken at a national and international level are the key towards including cyber security aspects in other regulatory frameworks

References

[1] Government Decision no. 1268 from 23.11.2016 - On Regulation on physical security on nuclear and radiological activity. Official Monitor of the Republic of Moldova no. 415, 29 November 2016.

[2] English Oxford Living Dictionaries https://en.oxforddictionaries.com/definition/cybersecurity

[3] Cybersecurity in the Healthcare Industry http://resources.infosecinstitute.com/cybersecurity-in-the-healthcare-industry

[4] Au. Buzdugan, Role of cyber security along with nuclear and radiological safety in medicine, 3rd International Conference Health Technology Management, ICTHM-2016, October 6-7, 2016, Chisinau, Republic of Moldova, Book of Abstracts, p.102, Ed. Prof. Victor Sontea.

[5] Aurelian Buzdugan, Artur Buzdugan - "The interplay between cyber and nuclear security domain in Republic of Moldova", 9th International Conference on Microelectronics and Computer Science, 2017

[6] Healthcare IT Systems: Tempting Targets for Ransomware, https://spectrum.ieee.org/riskfactor/computing/it/healthcare-it-systems-tempting-targets-for-ransomware