ULUSLARARASI SAĞLIK YÖNETİMİ VE STRATEJİLERİ ARAŞTIRMA DERGİSİ
INTERNATIONAL JOURNAL OF HEALTH MANAGEMENT AND STRATEGIES RESEARCH
Cilt/Volume : 4 Sayı/Issue : 2 Yıl/Year : 2018 ISSN -2149-6161
Usaysad Derg, 2018; 4(2): 150 -167 (Araştırma makalesi)

SAĞLIKTAKİ SİBER-TEHDİTLERİN ETKİLİ YÖNETİMİ İÇİN BÜTÜNCÜL GÜVENLİK MİMARİSİ

HOLISTIC SECURITY ARCHITECTURE FOR EFFECTIVE MANAGEMENT OF HEALTHCARE CYBER THREATS

Dr. Ahmet EFE
Yıldırım Beyazıt Üniversitesi
aefe@ankaraka.org.tr
https://orcid.org/0000-0002-2691-7517

Elif ÇALIK
Karabük Üniversitesi Sağlık Bilimleri Fakültesi
elifcalik@karabuk.edu.tr
https://orcid.org/0000-0002-9203-7550
Makale gönderim-kabul tarihi (05.06.2018-11.08.2018)

Abstract

Cyber security has become one of the top priorities for healthcare systems, due to the fact that the healthcare information security and personal privacy are major concerns for patients, healthcare providers and governments. The information that is incrementally available in the health records has a much longer shelf life and is a fertile and invaluable source for identity theft. The stagnant social security numbers cannot be easily canceled and medical and prescription records are permanent in the systems. Furthermore, healthcare information has a higher value than credit card information in the underground market in the dark web. There is a huge market for health insurance fraud and abuse, which may be more profitable than selling the records honestly in the forums. There are common but seriously increasing threats, which can be exploit healthcare information, is becoming compromised or stolen outright, when patient health records are being digitized. The abuses of health data such as DNA information is the most critical since it can be used for possible targeted biological weapons or certain targeted artificial diseases. The aim of this study is to provide a framework for future research by identifying concept of security and cyber threats in the healthcare systems.

Key words: Healthcare, cyber security, e-government, EHRs, COBIT-5

Özet

Sağlık bilgisi güvenliği ve kişisel mahremiyet, hastalar, sağlık hizmeti sağlayıcıları ve hükümetler için önemli kaygılar olduğundan, siber güvenlik sağlık sistemleri için en önemli önceliklerden birisi haline gelmiştir. Sağlık kayıtlarında artmakta olan bilgiler çok daha uzun bir raf ömrüne sahiptir ve kimlik hırsızlığı için verimli ve paha biçilmez bir kaynaktır. Statik sosyal güvenlik numaraları kolayca iptal edilemez ve sistemlerde tıbbi ve reçete kayıtları kalıcıdır. Ayrıca, sağlık bilgisi, karanlık ağdaki yer altı pazarındaki kredi kartı bilgisinden daha yüksek bir değere sahiptir. Sağlık sigortası dolandırıcılığı ve suiistimali için büyük bir pazar var, bu da reklâmların forumlarda dürüstçe satılmasından daha karlı olabilir. Hasta sağlık kayıtlarının sayısallaştırıldığı durumlarda, istismarın artmasına neden olabilecek sağlık sorunlarının tehlikeye girmesi ya da çalınması sonucu ortaya çıkan yaygın ve ciddi tehlikeler vardır. DNA bilgisi gibi sağlık verilerinin kötüye kullanılması, olası hedefli biyolojik silahlar veya belirli hedeflenmiş yapay hastalıklar için kullanılabilecek en kritik durumdur. Ayrıca hastalara ait

ULUSLARARASI SAĞLIK YÖNETİMİ VE STRATEJİLERİ ARAŞTIRMA DERGİSİ
INTERNATIONAL JOURNAL OF HEALTH MANAGEMENT AND STRATEGIES RESEARCH
Cilt/Volume : 4 Sayı/Issue : 2 Yıl/Year : 2018 ISSN -2149-6161

tanı verileri ilaç firmaları açısından da paha biçilmezdir. Bu çalışmanın amacı, sağlık sistemlerinde güvenlik ve siber tehditler kavramını tanımlayarak gelecekteki araştırmalar için bir çerçeve sağlamaktır.

Anahtar Kelimeler: Sağlık, siber güvenlik, e-devlet, EHRS, COBIT-5

INTRODUCTION

Cyber security concerns are becoming more severe in lots of reports published about cyber security issues in e-government sites particularly on e-healthcare systems (Ponemon, 2016). According to 2016 Healthcare Information and Management Systems Society (HIMSS) Analytics - Healthcare IT Security and Risk Management Study, it was reported that the number of health records were affected by hacking (breaches) attempts. Similar surveys conducted in 2017 concluding similar results(HIMSS, 2016). This survey reveals several gaps in the current state of healthcare cybersecurity such as IT budget is not allocated enough (0-3% of total) to IT security, 20% of respondents comply with key mandates, 50% of survey respondents are only beginning to address medical device security, and medical device manufacturers are not mandated to incorporate cybersecurity features in their products. Moreover, medical identity theft (77%) is most common reason for health information based cyber-attacks, and the top three that vulnerability of cyber security are respectively e-mail, mobile devices and internet of things (SANS, 2016). Also, the major subject of cybersecurity concerns estimated by providers as ransomware (69%), phishing attacks (61%), advanced persistent threats attacks (61%) in the future. In 2016, the other report shows that ransomware, malware, and denial-of-service (DOS) attacks are the major cyber threats facing healthcare organizations (HIMMS, 2017).

Unless security prevention and controls are in place, data might not be under protection. A network attack can be passive that data is monitored by attackers or active that data altered with intent to corrupt by the unauthorized person. As recently reported by McAfee Labs [Figure1.], frequently network attacks are denial of service (33%), browser (25%), brute force (18%) and the others (23%).

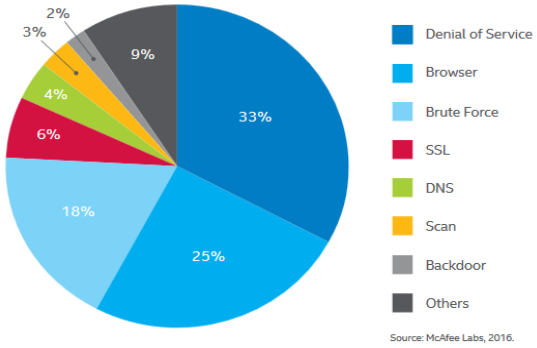


Figure 1. Representation of Frequently Network Attacks 2016 (McAfee, 2016)

1. Method

In this study is conducted search on PubMed (MEDLINE) by using keywords such as healthcare, cyber security, cyber threats. The inclusion criteria in this research have published in the last three years and access to full text.

Our approach to the healthcare data security has three pillars. The methodology of handling healthcare data should be built on capacity building approach.

ULUSLARARASI SAĞLIK YÖNETİMİ VE STRATEJİLERİ ARAŞTIRMA DERGİSİ
INTERNATIONAL JOURNAL OF HEALTH MANAGEMENT AND STRATEGIES RESEARCH
Cilt/Volume : 4 Sayı/Issue : 2 Yıl/Year : 2018 ISSN -2149-6161

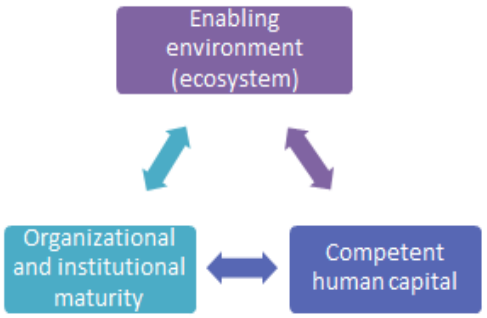


Figure 2. The trinity of capacity development

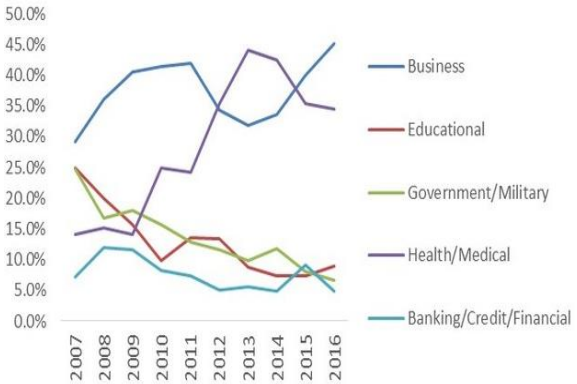
As shown on the diagram above, capacity building on this issue has three branches that are interacting and feeding each other that are enabling the ecosystem, institutional and organizational maturity and developing the human capital.

2. Definition of problem Statement

With the rapid grooving e-government applications and services that aim to provide health services more efficient and time saving by electronic and automated platforms. This growing tendency makes health information more vulnerable. Nearly all of countries and local authorities try to use e-government services for healthcare needs. With the establishment of a European E-Health Network, the European Union would like to improve citizens' health by making life-saving information available using E-Health tools, to make E-Health tools more effective, user friendly, and widely accepted by involving professionals and patients in strategy, design and implementation of the network, and to increase healthcare quality and access by making E-Health a part of the European health policy and managing cross national political, financial, and technical strategies on E-Health. ENISA has been working to guide, government agencies and hospitals for cyber-smart hospitals (ENISA, 2017).

Day by day the health data is growing in the concept electronical healthcare records (EHRs). Confidentiality, integrity and availability, also known as the CIA triad, is the basic principles of information security. In any case, EHRs should be designed and communicated in accordance with this CIA triad. According to this term, confidentiality is a group of rules that restricts access to data, integrity is the guarantee that the information is reliable and correct, and availability is an assurance of secure access to the data by privileged users (Cryptome, 2013).

EHRs are included very important information about patients such as age, gender, diagnostic results, treatment, and test results, so on. Also according to universal standard they should be under the patients' consent. In 2016, there was diverse of data breaches that face to face healthcare providers can be seen in Table 1.



ULUSLARARASI SAĞLIK YÖNETİMİ VE STRATEJİLERİ ARAŞTIRMA DERGİSİ
INTERNATIONAL JOURNAL OF HEALTH MANAGEMENT AND STRATEGIES RESEARCH
Cilt/Volume : 4 Sayı/Issue : 2 Yıl/Year : 2018 ISSN -2149-6161

Figure 3. Type of data breaches in 2016 (McAfee, 2016)

According to fig 3, healthcare data breaches will continue to develop a great interest for cyber attackers because stolen data in EHRs usually includes personal, health situation and financial information. That information is very valuable for some illegal companies, advertising and black markets (Zeadally S. et.al, 2016).

According to recent web based study results in Taiwan that sharing EHRs is not important for contributors, and system security design is not important for most of contributors, but they also do not satisfied with the existing security design (Rau H.H. et al, 2017). Also a study conducted in Canada shows that an application uses MD5 and SHA-1 algorithms in encrypting complex text from personal patient information can be used to produce one-way encrypted identification number any patient and serves data security during sharing the data (Mohammed E.A. et al., 2016).

In a similar study, a patient-controlled attribute-based encryption is proposed, which enables a patient to control access to health data and reduces the operational burden for the patient, simultaneously (Eom J., et al., 2016). Another study that stated in USA proposes the Hippocratic Database approach to secure EHRs records. In the other study, a probabilistic data mining algorithm is used to detect anomalous events and takes appropriate response in real-time and proposed system detected 15 unusual connections which were undetected by a commercial intrusion prevention system on real-world hospital network data consisting of incoming network connections for a 24-hour period (Faysela M.A., 2016). In additionally, there are number of review about healthcare cyber security that they are guiding our study Also they have information of general steps and general status of cybersecurity in healthcare because of new trend (Kruse S.C., et a., 2017) (Abbas A., 2014) (Lopes P., 2015) (Gope P., et al, 2016).

Dr Helen Wallace, director at GeneWatch UK, says there is a risk of commercial exploitation. "*Many companies want to calculate your health risks from your medical records and DNA and use this information for personalized marketing of medicines, foods, supplements and skin creams,"* she says. Governments could also use the data to track citizens. "*In the future, the government and commercial companies may be able to identify you and your family and again access to your health education, social care and tax records through your DNA*," says Wallace (Bioterror, 2012). Furthermore, weapons can be developed targeting a specific DNA group. The problems with health data breaches are not only related with its abuse for economic ends but also for its possible usage for some kind of biological weapons. A report, Biotechnology, Weapons and Humanity II, warns that construction of genetic weapons "is now approaching reality". Such "genetic bombs" could contain anthrax or bubonic plague tailored to activate only when genes indicated the infected person was from a particular group (Adam David, 2004)

3. Importance of Personal Health Information (PHI)

In the black market, medical information has a higher value than credit card information. One reason for the discovery of medical data by thieves is that they have more permanent values than other types of information. When the bad guys go to their hands, it is hard for the victim to do anything to protect her. While a stolen credit card can be canceled and objectionable for fraudulent charges, the process of resolving medical identity fraud is not simple.

Hospitals and insurers usually do not have clear processes to correct mistakes in their health records or to help patients cope with other consequences of identity theft. WhiteHat Security vice-president Robert Hansen told Christian Science Monitor that health information could not be recovered and could be fatal in the wrong hands, as opposed to credit card numbers. "Banks have become increasingly sophisticated by adding more secure transactions and transfers in recent years, security.

In a survey, twenty-one percent of physicians said they were below the average of cyber security, but eight percent of IT staff and 28 percent of managers shared the same view. In a Ponemon Institute

ULUSLARARASI SAĞLIK YÖNETİMİ VE STRATEJİLERİ ARAŞTIRMA DERGİSİ
INTERNATIONAL JOURNAL OF HEALTH MANAGEMENT AND STRATEGIES RESEARCH
Cilt/Volume : 4 Sayı/Issue : 2 Yıl/Year : 2018 ISSN -2149-6161

report, cyber criminals increased their health care attacks by 125 percent, indicating that the industry is paying $ 6 billion a year. Recently, the UCLA Health System data breach affected 4.5 million patients. Extraordinary events were detected in October 2014, and an investigation by the FBI confirmed a breach on May 5, 2015. Filed server names, birth dates, Social Security numbers, Medicare and health plan identification numbers, as well as patient diagnostics and procedures were reveled (INFOSEC, 2015).

Figure 4. Medical Information Theft Predictions

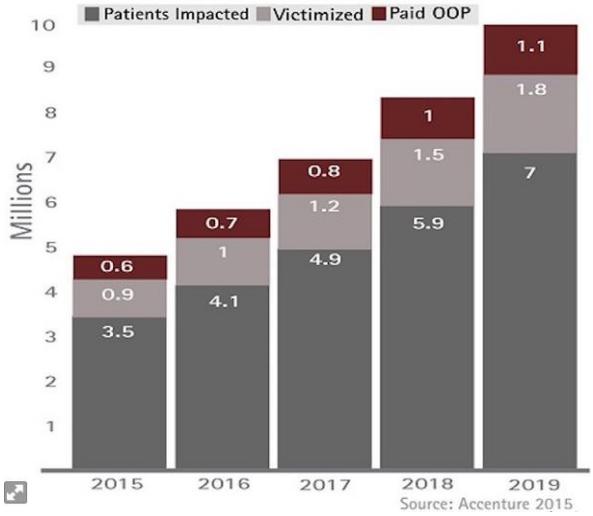


Fig. 4 shows the scale of cyber breaches of healthcare systems in 2015 and the table 1. Below show how dramatic increase in numbers it has shown just in a couple of companies.

Table 1. Cyber Breaches in some of critical companies

Company	Numbers	Data stolen
Anthem Blue Cross	78.8 million	Personal data, including social security numbers
Primera	11 million	Bank account data, personal data, clinical records
Excellus Health Plan, Inc.	10 million	Some credit card details, financial transactions, personal data
University of California, Los Angeles Health	4.5 million	Medical records, personal data
Medical Informatics Engineering	3.9 million	Full range of PHI
Banner Health	3.62 million	Financial data, personal data, clinical Information
Newkirk Products, Inc.	3.5 million	Personal data

21st Century Oncology	2.2 million	Financial data, personal data, medical records
CareFirst BlueCross BlueShield	1.1 milion	Some personal data
Valley Anesthesiology Consultants, Inc.	882,590	Financial data, personal data, medical records
Anthem Blue Cross	78.8 million	Personal data, including social security numbers

3.1. Healthcare data specifications

Cybercriminals often pursue electronic health records (EHR) held in health care facilities. Electronic health records include personal health data recorded during medical applications. This data can be accessed by special electronic health records management programs used in health care facilities.

Electronic health records include birth date, health insurance number, social security number, identity card number and various financial data related to the individual. Besides, the doctor's information about the person involved in the registration, the life style of the person, the medical history of the family, the drugs used, the health bill and the results of the examination are also very important data.

513 thousand 811 health institutions in the United States are receiving incentive premiums for the elderly and the poor within the scope of health benefits and insurances. The amount of premiums distributed is around 35 billion dollars. Therefore, the data flow in the health sector also includes serious financial data (Mayra R. F., 2017).

3.2. How is the stolen data transformed?

The captured health data contains enough information to create false identity, driver's license and insurance policies. Cybercriminals can create false identities in this way and use it in various activities.

For example, they are fraudulent in the creation of false identities and social insurance data, as well as fake prescription and drug discovery. The same amendment can also be made in the area of tax refunds and insurance payments.

EHR data is much different than credit card data and the danger is that it contains completely personal and unchangeable information. Hence, cyber attackers who acquire this information can use this data in much more serious operations as they have much more vital data. In addition, everyone wants to have this information in underground markets where the cyber attackers share what they have stolen because they are unchangeable data.

Cyber attackers are getting financial income by selling healthcare products that they obtain from underground markets. For example, a complete database of patients seized can be worth as much as $ 500,000. For example, a package that contains all personal and health data, or a health insurance number that belongs to a person, can cost up to $ 5 to $ 5. Driving license information is $ 170, with a database containing identity information, it can be sold for up to a thousand dollars (Mayra R. F., 2017).

3.3. Healthcare software and attacks against them

Healthcare institutions use many health data management programs. To give an example from the programs in America; PrognoCIS, NueMD, McKesson, Allscripts, Cerner, Praxis EMR, Athena Health, GE Healthcare, eClinicalWorks, and SRS EHR. Globally, Allscripts Healthcare Solutions, Inc., Athena Health, Inc. Programs such as Cerner Corporation, CPSI, Epic Systems, eClinicalWorks, GE

Healthcare, Greenway Health LLC, Medical Information Technology, Inc., McKesson Corporation, NextGen and OpenMRS are widely used (Mayra R. F., 2017).

These programs and infrastructures are sometimes used in closed networks in the enterprise and sometimes on cloud networks. Cyber attackers can access multiple databases with attacks on cloud networks.

SQL injection is a method used intensively in this area. This is the generic name given to the process of adding data, including intervening SQL queries. In web applications, dynamic SQL statements are generated with data entered by users. The intervention of these codes when they are created constitutes the basis of this process.

Cross site scripting (XSS), computer security is another kind of attack. This attack is defined as the ability to run the requested client-based code on a user's browser by embedding client-based code in HTML code.

In 2015, the health data of 300,000 users were leaked in an attack on Smith's PrognoCIS cloud-based EHR software. This attack was carried out through malicious software infected to the main server of the program.

At the same time, a web-based EHR software named Nomore Clipboard was hacked in 2015, causing 3.9 million users to leak data (Mayra R. F., 2017).

Another threat in the health sector is the open spots created by Internet-connected devices used at various points in infrastructures and the risk of infiltration of cyber attackers from these points. A questionnaire on Shodan, a search engine that lists Internet-connected devices, reveals that many networks and medical devices in the healthcare industry are vulnerable to attack.

4. Protection of the healthcare sector in the US

There are also some legal regulations in the US that health institutions must follow to protect these electronic data. (The Health Information Technology for Economic and Clinical Health (HITECH) Act). In addition, according to the Health Insurance Portability and Accountability Act (HIPAA) applied in the US, SSL security standards must be used for transactions involving health data. This includes corporate e-mail systems and all internet-based platforms.

Again, according to a survey conducted by the Healthcare Information and Management Systems Society (HIMSS) in the USA, 68.1 percent of the hospitals and less than half of the medical practitioners say that they encrypt the data on the move. 61.3 percent of the hospitals say they encrypt the data they store. 48.4 percent of medical application providers coded data they stored. The risk of data being shared or sent without data encryption is very high (Mayra R. F., 2017).

5. Numerous healthcare sector's cyber security and major attacks

Since February 2017, connected device search engine Shodan's data exposed to the attacked 240 million 933 thousand 715 connected devices, 101 thousand 394 are used in the health sector. Looking at the first squad of the attacked devices, it is seen that 52.6 percent are used in Canada, 35.62 percent in the US and 1.83 percent in Japan.

418 attacks against the operating systems used in health services are seen. Of these attacks, 53.83 percent are Windows Server 2008 R2, 11.72 percent are Windows 7 and 8, 8.85 percent are PIX OS 7.0.x, and 8.13 percent are Linux 3.x operating systems. However, software support is still being used in many hospitals and public institutions in Windows XP, which is finalized.

According to Verizon's 2016 data leak review reports (DBIR), many companies need third party services to block data breaches. According to forecasts, cheaters for hospitals, clinics and doctors are

causing more than $ 6 billion annually to the American healthcare industry. The damage to these hospitals by these attacks is an average of $ 2.1 million.

In July 2016, the Banner Health Company was attacked by peppers and leaked health care data of 3.6 million people. Newkirk Products' cheerleaders attacked 3.4 million people health care related data came out. In Florida, 21st Century Oncology Holdings' 145 cancer treatment centers in the case of the pepper attack, 2.2 million patients came out of the data. In 2016, a total of 876 data related to health services in the UK have been leaked. In a statement made by the Australian Health Minister in October 2016, data from close to 3 million patients were leaked due to a breach in the Medicare system (Mayra R. F., 2017).

6. International Regulations

The data confidentiality of the patient has been mainstreamed by a number of regulatory frameworks and laws which are either concerned with this issue or are included as a separate area. Two examples of this are:

General Data Protection Directive (GDP): Even if this regulation is derived from the EU, GDP has a broad impact. Any organization that handles the data of an EU citizen or employee of the EU will be under the aegis of GDP for data confidentiality. GDP also specifies certain data classes and assigns special considerations for specific data classes. This includes determining health benefits. There are some exemptions in the protection of the privacy of health data in GDP, particularly in the area of its use for scientific research (EC, 2018).

Health Insurance Portability and Accountability Act (HIPAA). The HIPAA Security Rules, Privacy Rules and Application Rules are used to provide privacy and protection of health data. HIPAA has been expanded to force organizations to comply with the same rules, not only that they are enforcing their own rules, but that all business partners who operate the same data (HHS, 2018).

GDP and HIPAA play an important role in what is to be protected, how and in some case how to prioritize it. However, it is often difficult to assess the situation when an organization approaches the situation for health data privacy for the first time.

7. The standards and frameworks

Relatively large number of frames and standards exist and reports report that there is a potential for confusion between data controllers. In addition, the direction of self-assessment of conformity mechanisms led to concerns about generally welcome audits because they provided "enforcement inspection".

Following existing standards have been identified:

- Knowledge Management Team (IG Toolkit)
- CESG Cyber Basic Information
- Cyber Essentials 'PLUS' Service Network - Connection Code (PSN CoCo)
- ISO / IEC 27000: 2013 (Information Security Management)
- COBIT-5 for Cyber Security
- Good Practice Standards for the Information Security Forum (ISF SoGP)

Regarding health and social care activities, it has often been found that organizations are overwhelmed by very detailed standards such as ISO / IEC 27001 and ISF SoGP. When included in the cost of licensed documentation and related support, these standards might not be seen as appropriate for sector-wide implementation. However considering its coverage of both business and IT structure according to stakeholder needs, COBIT-5 for cyber security emerges as the best solution that can be tailored according to business needs and security requirements aligned with risks and resources.

ULUSLARARASI SAĞLIK YÖNETİMİ VE STRATEJİLERİ ARAŞTIRMA DERGİSİ
INTERNATIONAL JOURNAL OF HEALTH MANAGEMENT AND STRATEGIES RESEARCH
Cilt/Volume : 4 Sayı/Issue : 2 Yıl/Year : 2018 ISSN -2149-6161

8. Threats and perceptions

Given the fact that the value of a single health record is almost 10 times higher than a stolen credit card number and that the idea of health care (drug and device development, billing process, maintenance processes, etc.) it is not surprising that they are increasingly targeting health care providers over time.

There is a huge obstacle to the safety of patient data in health service providers. On the one hand, while the informatics sector is rapidly evolving and people are adapting to their use, on the other hand institutions face serious challenges and inadequacies in putting central security policies into effect.

In a report prepared (ICIT, 2016) in 2016 by the Institute for Critical Infrastructure Technology (ICITECH) According to the health sector, the area that is at the most risky but most prepared for the cyber-attack in the US. Both service providers need to allocate a significant portion of the resources of the payment institutions for this hunger. The approach of managing government and healthcare institutions' complex information systems infrastructure to various layers with gaps is providing access to vulnerable people. Also, most of the time, manufacturers do not continue to support the technology, and this poses more threats. In June 2015, the US Office of Personnel Management system security breach, which threatened the knowledge of 4 million federal employees, shows how this is used by malicious people.

Experts who prepare the report also point out that the Internet of Things (IOT) is a major attack surface. At this point, experts advise that medical devices should not be subject to mandatory penetration testing before and after submission to the market. This means that innovation will not thrive often, that potential threats will be recognized, and that greater opportunities will be created for patch creation.

On the other hand, according to a new survey conducted in the USA, (Veracode, 2018) the loss of patients due to ill-intentioned people whose health leaders are unaware of the greatest fears of cyber security regarding systems or medical devices. According to a survey conducted by HIMSS on Veracode, an application software security company, healthcare executives are increasingly concerned about the damage to healthcare brands, the costs of government departments and the cost of security breaches. More than two-quarters of the participating hospitals and healthcare leaders participating in the survey said their main concern was that hackers used tools such as electronic health record systems and clinical practices in the Web and cloud environment.

According to the survey, leaders in health care are increasingly aware of the responsibilities of security vulnerabilities. 55% of respondents stated that spending on safety assessments is increasing. By contrast, 56% stated that they had added material to their contract with their third party vendors and added about 50% to the SANS Institute Center for Internet Security *(*CIS) Security Controls.

Participant inclinations in the survey:

- 56% said that the biggest worries were "phishing" attacks on employees and bad intentions within the organization,
- 54% budgeted more resources for cyber insurance,
- 44% say they want insistent managers to defend their information security policies in all units,
- 65% say they allocate money for the government's political regulations,
- 51% stated that they are investing to educate department leaders in the field of cyber security.

The authors state that healthcare institutions are facing security risks from web and mobile applications and that money and time are invested to understand these risks that cyber-attacks will face.

As a result, cyber security centered culture; requires manufacturers to develop safer devices, to ensure that the healthcare industry as a whole is confidential, and that policy makers should implement legislation to provide a safer and technologically accessible future.

9. Turkish National Regulatory compliance program for Electronic Health Records (EHR)

A regulatory compliance program requires some central coordination. It supports the collection of audits and the testing of information, the development of a set of common control objectives and the

ULUSLARARASI SAĞLIK YÖNETİMİ VE STRATEJİLERİ ARAŞTIRMA DERGİSİ
INTERNATIONAL JOURNAL OF HEALTH MANAGEMENT AND STRATEGIES RESEARCH
Cilt/Volume : 4 Sayı/Issue : 2 Yıl/Year : 2018 ISSN -2149-6161

coordination of efforts to comply with more than one regulation. Typically, new or updated regulatory or other requirements (such as PCI compliance) follow new institutional and departmental policies and procedures. As a result, this policy and procedural documentation begins to overlap and results in a separate HIPAA policy and a separate PCI policy addressing the same inspections and requirements, increasing complexity and confusion. For example, it is more practical to create an Access Control Policy or a Password Management Policy that meets both HIPAA and PCI requirements.

Electronic health record systems are designed to store data accurately and capture a patient's condition over time. It removes the need to track a patient's previous medical records and helps ensure that the data is accurate and legible. Because the file is more likely to be up-to-date and the files are just a changeable file that reduces the risk of loss, data can reduce the risk of copying. Some organizations are still examining compliance as audit documentation, documentation and audit practice. However, more mature organizations are aware of the need to adopt a risk-based approach as a way to focus their resources on the highest risk areas. We should also mention that the health sector may be the key focus, but it does not always turn into safe environments. The newly revised HIPAA Security Guidelines require vendors to evaluate the security of databases, applications, and systems that contain patient data against a list of 75 data security controls. These controls include certain precautions that may be in place to protect PHI (Saglik, 2017).

In Turkey, cyber security is a very critical new issue for healthcare information technologies. Strategically and political infrastructure studies, which started at the Ministry of Health level in 2003, is constituted the basis of the viewpoint of healthcare information systems of all health care units located in central and peripheral units. New approach is that EHRs' cyber security is as important as data storage, processing, and sharing by using internet. There is new announced study area about cyber security in healthcare by announced department of Information technology at Ministry of Health. However, except for reports covering the last three or four years of cyber security, it has been observed that there is no visible concrete study. When the reports are reviewed that cover serious general perspective of information security in the last one or two years, that shows it is a new topic for Turkey. Although this is the weakness, it presents the advantage for new improvement areas and offers the new perspective about cyber security of EHRs (Cert, 2017).

Recently in 2017 a new regulation called "Processing And Privacy of Personal Health Data Regulation" was issued by the Ministry of Health in line with requirements of "Personal Data Protection Act" 6698 numbered. As a requirement of this legislation a new commission called "Personal Health Data Commission" has been established under the Ministry of Health. The Commission has been established to assist in the determination of the Ministry policy, to resolve the disputes, to evaluate the applications for data transfer, to examine the complaints and to carry out the necessary inspections in accordance with the principles set by the Law No. 6698 and Personal Data Protection Board (RG, 2016). A new provision for processes of the commission has been issued for implementation of tasks of the commission by the Ministry (Saglik, 2018). This demonstrates the willingness and institutional capacity of Turkish government in the protection of personal healthcare data.

One of the most important measures in this regulation was a new establishment at directorate general level as "General Directorate of Health Information Systems" under "Personal Health Data Commission". Main duties of this DG are set out as such:

a) Establishes a central data system for the holding of personal health data,

b) All public and private health institutions and health professionals who provide health services to be sent by the service providers to the central health data system It provides,

c) Making the necessary technical arrangements for the integration of all systems,

d) The storage of all kinds of data on health status and health services nationwide; and determine the standards related to the information systems which are possible to transfer,

d) The access of third parties to whom they are entitled establish a personal health record system that provides,

e) High-level security to prevent unauthorized access to or from systems ensure that measures are taken,

f) Publish documents related to the management and organization of the systems on the internet page and when necessary, conducts training and orientation work on this issue,

g) An internet page where informative content is included in all matters related to this Regulation they are ready,

h) Establishing a call center to solve the technical problems that may arise in the use of the systems

or establish and support the internet .

Significant progress has been made in the health practices carried out in our country, the health informatics technologies used and the health service coordination, execution and supervision mechanisms. It is also seen that these mechanisms are in an innovative and competitive position, and they want to be sampled by many countries. Thanks to innovative applications in the field of health information, all health information and even internet policies of health institutions can be centrally coordinated and audited.

The increasing use of health technologies and technology for health today means that the healthcare sector, which is considered one of the 6 critical sectors in the world, will be more vulnerable to attack, now that cyber-attacks have become uncontrollable. In addition to the Cyber Security Strategy and Strategy Supporting Cyber Safety legislation, the Ministry of Health also takes care of information security issues and establishes health information legislation in accordance with the legislation of the country. Two law essential to Turkey's cyber security legislation No. 5809 Electronic Communications Act and the public on the Internet, known as the Act of 5651 Internet Environment Regulation of Publications and Via These Issues are processed Law on Combating Crime.

5809 and 5651, regulations, circulars, communiqués and directives are supported. The Ministry of Health also carries out the legislation-related regulations and directives in this direction. All institutions and organizations affiliated to the Ministry of Health in accordance with the law numbered 5651 are obliged to keep the internet access records belonging to the sub-organizations that the central internet service providers and to use the filtering system for internet content access. In this case, all Public Hospitals Association (KHB) General Secretariats providing central internet service in the direction of Health Information Network Project are obliged to keep all the access registration details of each computer in the hospital, polyclinic or health center they serve. The points that were ambiguous in the legislation in this respect were abolished with the Regulation on Internet Public Use Providers dated April 11, 2017.

9.1. Assessment of Content Filtering Liability

The widespread use of technology for health and the increasing number of devices and software of health technology makes it possible to transfer all data between institutions even if it is via VPN cloud and make the Ministry of Health network which is one of the biggest networks of the country to be threatened and attacked.

There is a National Black List for the ICTA, which is responsible for the coordination of national cyber security practices in our country, to provide clean and secure internet.

ULUSLARARASI SAĞLIK YÖNETİMİ VE STRATEJİLERİ ARAŞTIRMA DERGİSİ
INTERNATIONAL JOURNAL OF HEALTH MANAGEMENT AND STRATEGIES RESEARCH
Cilt/Volume : 4 Sayı/Issue : 2 Yıl/Year : 2018 ISSN -2149-6161

The use of the National Black List provided by the relevant public authority ICTA, in accordance with the Law No. 5651 and related legislation of the Internet access records and the protection of critical information infrastructures within the scope of the national security strategy of our country, the objective of managing the cyber security risks at a manageable and acceptable level as a unique list that can be credited for providing. This list, which can only be used by BTK's approved content filtering products under the 5651 law, is updated daily by BTK.

Non-BTK-approved solutions do not use the National Black List, but filter content with commercial blacklists produced in different countries. It is seen that the only way for healthcare organizations to ensure public information security and ensure compliance with legal cyber security legislation is to use products approved by the BTK, the direct law enforcement agency.

9.2. Assessment of Registration of Access Records

Information indicating the use start and end times and the unique network device number (MAC address) of the computers using these IP addresses, the destination IP address, the ports of one or more IP addresses the user must include the actual IP and port information allocated to the user in the internet access service provided by the method of sharing with the users via the Internet and the records should be stored for two years by the center providing the internet usage.

Since the VPN infrastructure established within the Health Information Network conducted by the Ministry of Health is structured at the Layer 3 level, it is not possible to obtain MAC address information from the hospitals, outpatient clinics and health centers affiliated to the KHB General Secretariat, which should be taken to the General Secretariat of the KHB as required by Law No. 5651 and the Layer 2 level information. the need for a solution to support the product of network security is emerging.

The statements regarding the compliance of the cyber security solutions on the market with the law No. 5651 are entirely their own assertions and any document received from the international testing and certification bodies does not guarantee compliance with the law No. 5651. As a matter of fact, in order to fulfill the requirements of Law No. 6551, they have to construct a security wall for every point connected to the KHB General Secretariat

In addition to the country's cyber security legislation, the BTK-approved network security solution, which is specialized in the field of Health Informatics, ensures that the needs of the healthcare sector are achieved in a legal and effective manner. The Antikor Integrated Cyber Security System is a BTK-approved solution that provides effective content filtering solutions with a large database that integrates both national blacklists and international blacklists.

9.3. Assessment of data confidentiality aspect of healthcare cyber security

The Law KVKK on the Protection of Personal Data entered into force as of October 2016. It is one of the important issues to get consent and stay connected to certain rules especially when the person belongs to the family. The foundation of the law also requires this. He describes the change in the EU countries in 1995 when the legislation was not enough, and goes on: "In 2018, there will be a regulation on general data privacy called GDPR (General Data Protection Regulation). Even these are discussed in Turkey. Can we issue a series of regulations and circulars taking into account the legislation to be issued in the framework of the law, GDPR, and legislation with stricter rules? There are two regulations on the agenda regarding personal benefits. One of these is the record-keeping regulatory responsibility. According to this, the establishment of a record account like a trade account is on the agenda, and those who process personal data may be registered here.

If the law sees what it brings; doing personal data definition; Any kind of information we can associate with the person says personal data. It also defines the definition of personalized personal data; health

ULUSLARARASI SAĞLIK YÖNETİMİ VE STRATEJİLERİ ARAŞTIRMA DERGİSİ
INTERNATIONAL JOURNAL OF HEALTH MANAGEMENT AND STRATEGIES RESEARCH
Cilt/Volume : 4 Sayı/Issue : 2 Yıl/Year : 2018 ISSN -2149-6161

care, biometric data, religion and sect, and political thought. Last but not least, personal data refers to the conditions of processing. Personal data outside of health and sexual life can be processed without consent in cases where it is foreseen in its blood. It is an issue that concerns insurance companies. The personal data received for financial support was actually an exception. This includes hospitals, for example, or health care or health care providers.

As the mandate in a number of banks in Turkey, was held personal data responsible assignment. But in general there is a gap. He is also afraid of his criminal and administrative sanctions because he is also hesitant to take responsibility for who is going to be responsible, who does not know who will have the ball from fire. If there is a clear consent from the data owner about the proper processing of the personal data that you collect after that, you must obtain express consent if you are going to use something other than exceptions. How are you going to get the open order? Is it paper or electronic? How will you prove that you have taken this open ration; when did you receive, in which environment did you take.

Health is actually a third subgroup in the KVKK. There are personal data, personal data of a special nature, and even if it is not specified as an item in the data relating to health and sexual life, you cannot process it without explicit consent, It's in the insurance sector, but it's not our job because it's health insurance. We made correspondence with the Under-secretariat of Treasury, Ministry of Health, KVKK about this matter. As a result, regarding the regulation of the Ministry of Health, we learned that the first order is already changing and the new order will change. We have learned that the insurance industry is not subject to that directive. The regulation is only the Ministry of Health and the health institutions operating in the presence of SGK. As the insurance sector, we are not subject to the regulation of the Ministry of Health. But it does not exempt us from explicit consent. We are in touch with KVKK for this. So healthcare can only be handled properly in the insurance sector (Saglik, 2018)

Even the technical staff sometimes does not attach much importance to the issue. Cyber safety comes first after the defense plan comes to mind first. But health information security in information, cyber security is much more important than defense. The 'Health Information and Management Systems Society' report, which expresses its importance, is in the forefront. The report says that in 2016, 80 per cent of health care institutions were exposed to a pyrotechnic attack.

The main problem is who uses health applications for what purpose, and the importance of developed health information technology to include software that will keep user records on this issue. The General Directorate of Foundations opens 260 information sharing environments to stakeholders, software support and municipalities. What question do you ask the authority, when did you enter, what did you do, whose data? Have you looked at a patient's data that you were an important politician or were not obliged to look after? All of these are recorded and directly reported if there is a discrepancy between them. They can be implemented and audited for every software application.

CONCLUSION AND RESULTS

The amount of increase in violations of health data shows that medical industry must adopt cyber safety precautions and standards to identify, detect and prevent security vulnerabilities. Nearly 90% of healthcare IT specialists are expressed in reports on cybersecurity last year, where it has become a higher business priority for organizations and about 67% of organizations have experienced a "major security incident" in the recent past.

With the large increase in the cybercriminal industry, the health sector is a potential target for hungry hackers. Patient safety may not be directly related to data security, but includes everything from personal health information, address, private medical records, and credit card information.

In healthcare systems, using mobile technology and cloud computing, which increase risks such as denial of service or data breaches is increasing day by day, because of their time and cost effectiveness. Currently available healthcare cyber security precautions are not capable of counteracting cyber threats.

ULUSLARARASI SAĞLIK YÖNETİMİ VE STRATEJİLERİ ARAŞTIRMA DERGİSİ
INTERNATIONAL JOURNAL OF HEALTH MANAGEMENT AND STRATEGIES RESEARCH
Cilt/Volume : 4 Sayı/Issue : 2 Yıl/Year : 2018 ISSN -2149-6161

To avoid exposure to cyber-attacks, firstly adequate budget should be allocated for cyber security, and secondly end users should be educated about preventive attitude.

Integrating healthcare objectives with security concerns and resources using a wisdom model is of crucial importance for hospitals and regulatory agencies for health sector (Efe, 2016, Efe, 2017). In addition to this, using a comprehensive framework such as COBIT-5 to have an integrated and holistic approach of both governance and management of health and IT services and measurable processes will provide an infrastructure for effective management of health data and information (Efe, A. 2015,).

The national regulations alongside with international rules and regulations exist in the stage but usage of a holistic framework that covers both business processes and IT governance alongside with cyber security is lacking in implementations. Without proper strategic alignment of organizational strategies, business processes and risk&resource optimization prudent response to cyber threats and infringements of privacy cannot be addressed and mitigated. We have found COBIT-5 to be competent and apt comprehensive framework for healthcare information security.

RECOMMENDATIONS:

Recommendations can differ for organizations, hospitals, users and vendors. But in general these recommendations can a list of generally known measures. These measures can be detective, preventive, corrective, deterrent, recovery and compensating controls. These types of controls can be defined according to needs, resources and risks.

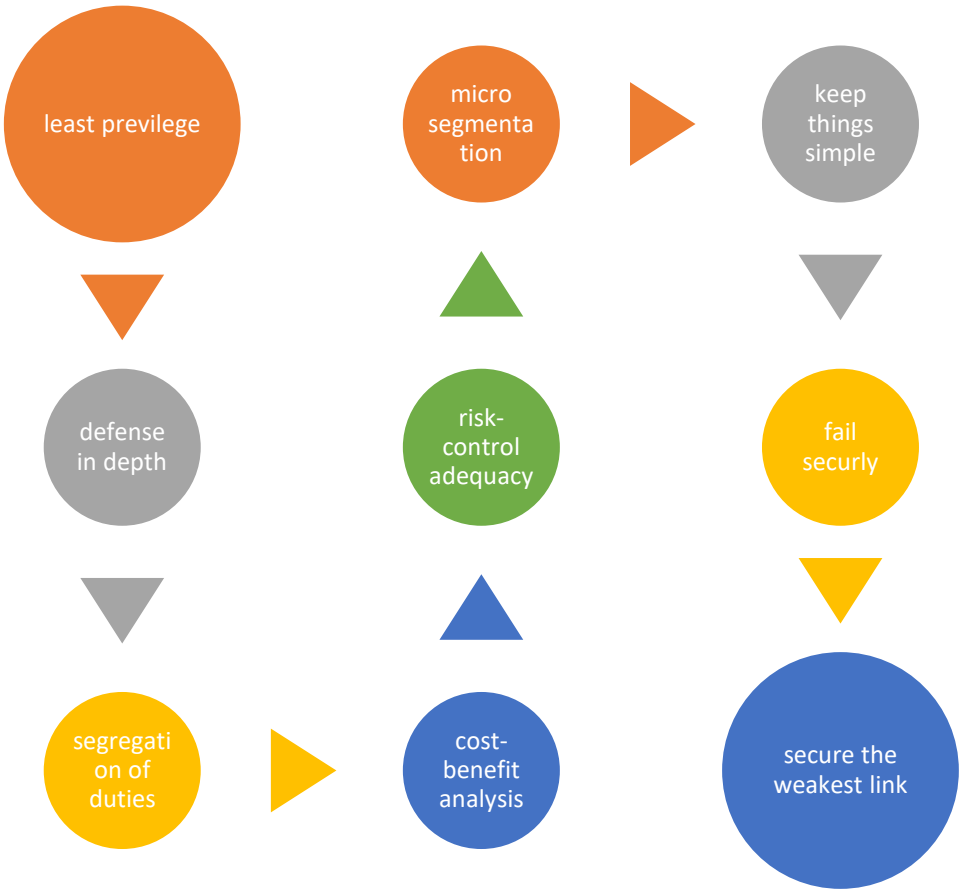


Figure 5. Information Security Fundamentals

As is shown in the fig. 5, recommendations can be made according to information security fundamentals.

Precautions for End users:

- A strong password that contains letters, numbers, and symbols that are eight characters long and does not share a password with anyone.
- Using an official computer only without authorization.
- Use it securely using a bookmark URL instead of writing to the URL or clicking on any link.
- Use the secure exit button
- Verifying extraordinary requests for verification of legality rather than following instructions.
- You are not using an insecure connection path to access the Internet.
- Do not use personal devices to transfer, share or store official data.

Management Measures:

- Developing a policy to manage threat events that take into account national and international cyber security standards, policies, agreements, guidelines and annual reports, and are kept up to date.
- Be prepared for any cyber-attack, keep data backup and restore strategies current and functional.
- Preparation of safety awareness training programs for all users.
- Simulate real-world threats to assess whether training and awareness programs that enhance defense capabilities are effective.

Precautions for Technical Staffs:

- When setting up or rebuilding the system, universal standards such as Health Level Seven International (HL7), Digital Imaging and Medical Communication (DICOM) should be considered and always up to date.
- Using malware-free hardware and software technologies to disable cyber-attacks.
- Back up data at predetermined regular intervals to monitor security posture and test restoration capabilities.
- Use network security devices to enforce and enforce network segmentation, which can provide network traffic between segments of networks with different security profiles.
- It is given at the level that it can make the powers of the users possible, and can reduce the effects of the cyber-attacks the least. For example, doctors can read and write patient prescriptions, but nurses can read the patient's prescriptions.
- It will reduce the effect of cyber-attacks on the basis of minimum authority for file access control on the servers.
- Restrict administrator-level authorization as much as possible and also administrators can use manager account when necessary, otherwise they should use normal account.
- Obtaining a professional certification is an important asset. A healthcare information security and privacy practitioner (HCISPP) is a certified professional who earned his/her certification from the International Information Systems Security Certification Consortium (ISC). The certification identifies these professionals as having expertise in the chief areas of knowledge on privacy and security of healthcare information. (ISC) is a non-profit organization that is the largest IT security organization in the world (Infoesec, 2017). Cyber Security Nexus (CSX) is also another certification for cyber security professionals.

Precautions For organizations:

For organizational level of security there should be a security framework which is integrated with organizational strategies based on stakeholder needs. This kind of a framework should take into

ULUSLARARASI SAĞLIK YÖNETİMİ VE STRATEJİLERİ ARAŞTIRMA DERGİSİ
INTERNATIONAL JOURNAL OF HEALTH MANAGEMENT AND STRATEGIES RESEARCH
Cilt/Volume : 4 Sayı/Issue : 2 Yıl/Year : 2018 ISSN -2149-6161

consideration risks, resources and corporate values aligned and optimized on business and IT related processes. This is a requirement due to changing structure, scope and types of threats and risks.

We have found COBIT-5 framework as the best framework that encompasses all business processes of both IT governance and management. Without a holistic, integrated and end-to-end process management of all business and IT processes, it is impossible to tackle with issues like health data breaches in ever changing and unpredictable business environment and innovative technological advancement.

An organization is less likely to block every possible IT security incident without effective utilization of holistic frameworks such as COBIT-5. Healthcare organizations should not only try to protect data but also implement an incident response plan when a disruption is detected at the same time as a result of COBIT-5 security management processes. Because of violent or malicious actions, employees often violate health care. Therefore, employee awareness and response training should be applied. Electronic health record specialists also provide remote storage and data backup systems. This provides security for healthcare organizations against natural disasters that can destroy files, although they are not as powerful as data breaches as a defense against hackers and data encryption.

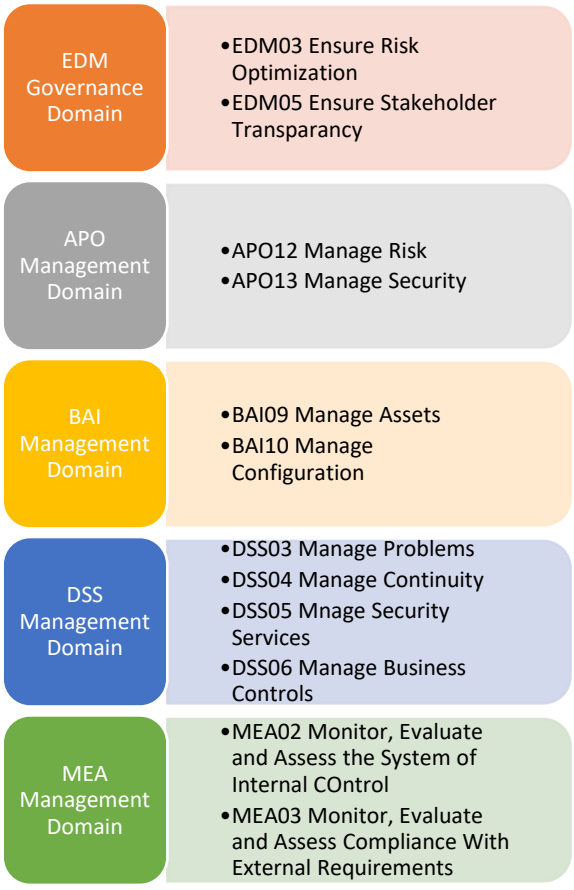


Figure 6. COBIT-5 Process for Healthcare Data Protection

Fig. 6 above shows COBIT-5 domains and man processes that can be used for healthcare information protection. These processes have sub processes, process targets, critical activities and input for and outputs from other processes. These are called as enabling processes objectives that are shaped from

organizational objectives, stakeholder needs and environmental factors (ISACA, 2018). Implementation of these critical processes can be taken into deep examination by another study.

REFERENCES

Abbas A., Khan US., (2014), A Review on the State-of-the-Art Privacy-Preserving Approaches in the e-Health Clouds, IEEE Journal of Biomedical and Health Informatics, Vol. 18, No. 4, July

Adam David, (2004), https://www.theguardian.com/science/2004/oct/28/thisweekssciencequestions.weaponstechnology, last accesed on 25.06.2018

Bioterror, (2012), https://sites.google.com/site/bioterrorbible/BIO-WEAPONS/RACE-SPECIFIC-BIO-WEAPONS, last accesed on 10.05.2018

Cert, (2017), https://www.certtr.com/Iletisim.aspx, (Access Date: 28/05/2017).

Cryptome, (2013), https://cryptome.org/2013/09/infosecurity-cert.pdf, (Access Date: 28/05/2017).

EC, (2018), http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf, last accesed on 35.03.2018

Efe, A, (2015), COBIT-5 Framework As A Model For The Regional Development Agencies. *International Journal of Ebusiness And Egovernment Studies*, 33-43.

Efe, A. (2016), Unearthing and Enhancing Intelligence and Wisdom Within the COBIT 5 Governance of Information Model. *ISACA Journal*.

Efe, A. (2017), A Model Proposal for Organizational Prudence and Wisdom within Governance of Business and Enterprise IT. *ISACA Journal*.

ENISA, (2017), http://old.cimt.dk/wp-content/uploads/2017/04/Dimitra-Liveri-ENISA-Cybersecurity-in-hospitals.pdf last accesed on 15.05.2018

Eom J., Lee DH., Lee K., (2016) Patient-Controlled Attribute-Based Encryption for Secure, J Med Syst 40: 253, DOI 10.1007/s10916-016-0621-3

Faysela M.A., (2015) Evaluation of a Cyber Security System for Hospital Network, MEDINFO 2015: eHealth-enabled Health, I.N. Sarkar et al. (Eds.), IMIA and IOS Press, doi:10.3233/978-1-61499-564-7-915

Gope P., Ruhul Amin R., (2016), A Novel Reference Security Model with the Situation Based Access Policy for Accessing EPHR Data, J Med Syst 40: 242, DOI 10.1007/s10916-016-0620-4

HHS, (2018), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html, last accesed on 11.04.2018

HIMMS, (2017), http://www.himss.org/sites/himssorg/files/081516_CybersecurityCheckup.pdf, (Access Date: 29/04/2017).

HIMSS, (2016), Cybersecurity Survey, Sponsored by FairWarning, www.himss.org

ICIT, (2016), http://icitech.org/wp-content/uploads/2016/01/ICIT-Brief-Hacking-Healthcare-IT-in-2016.pdf, last accesed on 10.05.2018

Infoesec, (2017), What Is The HCISPP? Healthcare Information Security & Privacy Practitioner http://resources.infosecinstitute.com/category/certifications-training/cissp/cissp-concentrations/hcispp/, last accesed on 17.06.2018

INFOSEC, (2015), http://resources.infosecinstitute.com/hackers-selling-healthcare-data-in-the-black-market/#gref, last accesed on 15.05.2018

ISACA, (2018), http://www.isaca.org/Knowledge-Center/Research/Documents/COBIT-Focus-The-Failed-VASA-COBIT-5-Governance-and-the-Seven-Enablers-Part-3_nlt_Eng_1014.pdf, last accesed on 15.05.2018

Kruse SC., Frederick B., Jacobson T., Monticone DK., (2017), Cybersecurity in healthcare A systematic, Technology and Health Care 25 1–10, DOI 10.3233/THC-161263

Lopes P., Silva L.B., Oliveira J.L. 2015, Challenges and Opportunities for Exploring Patient-Level Data, Hindawi Publishing Corporation, BioMed Research International, Volume, Article ID 150435, pp:11, http://dx.doi.org/10.1155/2015/150435

Mayra R. F., (2017), https://www.trendmicro.com/content/dam/trendmicro/en/security-intelligence/research/reports/wp-cybercrime-&-other-threats-faced-by-the-healthcare-industry.pdf, last accesed on 15.06.2018

McAfee, (2016), Threats Report,https://www.mcafee.com/au/resources/reports/rp-quarterly-threats-sep-2016.pdf (September 2016), ss. 49 (Access Date: 29/04/2017).

Mohammed EA., Slack JC., Naugler CT., (2016), Generating unique IDs from patient identification data using security models, Journal of Pathology Informatics, 7: 55, DOI 10.4103/2153-3539.197203

Ponemon, (2016), Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, Research Report Sponsored by ID Experts Independently conducted by Ponemon Institute LLC

Rau HH., Wu YS., Chu CM., Wang FC., Hsu MH., Chang CW., Chen KH., Lee YL., Kao S., Chiu YL., Wen HC., Fuad A., Hsu CY., Hung-Wen Chiu WH., (2017), Importance-Performance Analysis of Personal Health Records in Taiwan: A Web-Based Survey, Journal of Medical Internet Research, vol. 19, iss. 4, e131, p.1

RG, (2016), http://www.resmigazete.gov.tr/eskiler/2016/10/20161020-1.htm, last accesed on 15.05.2018

Saglik, (2017), https://bilgiguvenligi.saglik.gov.tr/ , (Access Date: 28/05/2017).

Saglik, (2018), http://sbsgm.saglik.gov.tr/TR,15220/kisisel-saglik-verileri-komisyonunun-teskili-ve-calisma-usul-ve-esaslari-hakkindaki-yonerge.html, last accesed on 15.05.2018

SANS, (2016) State of ICS Security Survey, https://www.sans.org/reading-room/whitepapers/analyst/2016-state-ics-security-survey-37067, (Access Date: 29/04/2017).

Veracode, (2018), https://info.veracode.com/whitepaper-state-of-web-and-mobile-application-security-in-healthcare.html, last accesed on 15.06.2018

Zeadally S., Isaac JT., Baig Z., (2016), Security Attacks and Solutions in Electronic Health (E-health) Systems, J Med Syst 40: 263, DOI 10.1007/s10916-016-0597-z