ESSEC
BUSINESS SCHOOL

STATE OF CYBERSECURITY & CYBER THREATS IN HEALTHCARE ORGANIZATIONS

Applied Cybersecurity Strategy for Managers

Aurore LE BRIS, Walid EL ASRI

Introduction

Cybersecurity has become a crucial issue for many organizations but also for private individuals. As well as for "regular" crime, anyone may become a target of ill-intentioned people, exploiting the vulnerabilities of information systems (IS) in any possible way. Healthcare organizations are some of the entities we trust the most and that hold the most sensitive information about us: name, date and place of birth, medical records, social security details, etc. Suffering from many flaws (low budget, lack of IT organization, excessive use of legacy systems…), healthcare actors have become easy targets for hackers, facing more and more pressure and threats from them.

This article aims at depicting the current state of cybersecurity in healthcare organizations as well as at understanding the main cyber threats they face and how these last ones could be addressed.

First of all, the stakes and risks associated to the healthcare environment will be presented. The different types of assets likely to be targeted will be reviewed as well as the profile of the potential attackers/threats and their objectives.

Then, examples of attack scenarios - that occurred in real life or pentests – will be studied in order to highlight the consequences they may have on healthcare IS.

Finally, the current state of cybersecurity in healthcare facilities will be portrayed and possible measures to enhance it will be discussed.

1. Stakes and risks in the healthcare environment

Healthcare organizations are sensitive infrastructures due to their criticality for people's well-being and safety. Hospitals, health plans, research labs handle unique and valuable assets that digitization, systems interconnectivity, etc. make more and more exposed to cyber threats.

In order to assess health sector cyber risks, it is paramount to understand the systems to be defended, their key assets and the impacts a successful attack may have on them. In addition, potential adversaries also need to be identified along with their intentions and capabilities. That way, threats can be better evaluated as well as healthcare systems vulnerabilities.

This part of the report first provides an overview of healthcare facilities' assets. Then, it outlines the threats faced by the medical sector and their evolution.

1.1. Key assets

In its research study report on securing hospitals (2016), the firm ISE (Independent Security Evaluators) identifies the primary assets found in the healthcare ecosystem.

The most critical one is patients' health that can be affected in many ways by perpetrators. Indeed, patients can be permanently or temporarily injured through direct actions such as performing inadequate medical acts or turning off critical active medical devices; but their health may also be affected by indirect actions aiming at disrupting care. In fact, altering patient health records, compromising medicine inventory systems or cutting off power supply in operating rooms are likely to have dramatic consequences on the health of the patients involved.

The second most important asset in hospitals is patients' health record. This record contains valuable information including personally identifiable information (PII) such as social security number, health care provider information, credit card information, name, address, date of birth, etc. They also include

protected health information (PHI) - like patient physical or mental health condition, provision of health care, etc. – that identifies or can be used to identify the patient. Nowadays, most of these records are electronic (EHR) and so exposed to cyber threats. According to Ponemon institute (2016), "the most lucrative information for hackers can be found in patients' medical records" (p.5) as EHRs are on average valued at 50$ on the black market. Thus, patients' health records are adversaries' primary target for the purposes of identity theft and other insurance fraud opportunities. Furthermore, attacks on EHRs may have consequences on patients' health when they compromise their integrity whether by altering or destroying sensitive information (blood group, medical history...).

The availability of healthcare services is also a major asset of medical facilities. They are divided into two distinct categories: critical services & administrative services. The first ones ensure continuity of care, including, among others, active/passive medical devices, medicine delivery systems and surgery equipment. The disruption of these services may have a devastating impact on patients' health. The administrative services are dedicated to the smooth hospital workflow. Systems handling work orders, medicine inventories, prescriptions, bills or appointments are part of these services. Their unavailability is however less critical as long as their downtime remains of short duration.

Furthermore, some healthcare facilities host research labs. In this case, they house intellectual property assets such as experimental procedures for surgery, test and studies results, test subject information or drug formulas. This data has high value for the research team conducting the work but may also be of interest to third parties like researchers or pharmaceutical companies of competitor countries. Hence, they are possible targets of cyberattacks. In the event of the theft of such data, work years could disappear along with the money invested in it. The alteration of these assets can have even more serious consequences as it may mislead researchers and in the worst case scenario, results in harm to patients (e.g. during clinical trials).

Finally, the reputation of the facility and their physicians is also a non-negligible asset. Indeed, as they place their health (and even their lives) in the hands of the medical staff, patients need to know they can trust them and that the facility is safe. A cyber-attack - regardless its nature - will harm the institution credibility if it is disclosed to the public. In addition, if the identity of specific medical staff is used to perform the attack (impersonation, credential theft, etc.), it may damage their reputation and career.

1.2. Threat landscape

Crime as a business

According to Ponemon institute (2016), "healthcare organizations are in the cross hairs of cyber attackers" (p.2) that grow increasingly frequent. Indeed, its report showed that on average US healthcare facilities have been victims of one cyber-attack per month over the past 12 months and that half of them "have experienced the loss or exposure of patient information during this same period (26% of the other half is unsure)" (p.2).

This phenomenon can be explained by the combination of two factors: on the one hand, the high value of healthcare facilities' assets and on the other hand, the ease in which they can be compromised. In fact, according to KPMG (2015), "the healthcare industry is behind other industries in protecting its infrastructure" and its data. Therefore, it constitutes a prime target to adversaries offering them high rewards at low costs.

Typology of the threats

Cyber threats on health care facilities can be divided into two categories: the untargeted attacks and the targeted attacks (ISE, 2016, p. 19).

The untargeted attacks do not discriminate between assets. Therefore, adversaries choose the targets that maximize their gain/cost ratio first. For example, in the case of an EHR theft, the selection of the targeted facility is based on both the number of EHRs available and the difficulty to access them. That way, a high profit is generated with the least effort. Untargeted attacks could also be directed against patients. Indeed, a terrorist organization planning a massive cyber-attack on active medical devices, is likely to choose its target evaluating the gain/cost ratio of its different alternatives.

On the other hand, targeted attacks have specific assets in the crosshairs. In this case, adversaries have precise objectives and are willing to mobilize the required resources to reach them. For instance, blackmailing a specific target using information from his/her EHR, generates gains much greater than the sale of a random EHR on the black market. Therefore, the attackers will deploy significant means to obtain it and will be less likely to give up if encountering difficulties to penetrate the system.

Thus, the adversaries' motivation is the fundamental difference that exists between the two types of attacks presented above. This implies that health care facilities cannot defend themselves against targeted and untargeted attacks the same way. Indeed, while limiting security breaches may be enough to prevent untargeted attacks from happening, a more advanced security policy is required to effectively respond to targeted attacks.

Evolution of the healthcare environment and threats

Over the past decade, the medical field has experienced a massive digitalization. As mentioned by KPMG (2016), EHRs have appeared, clinical systems have been automated. As a result, workflows in healthcare facilities have evolved and brought new and increasing security challenges. Systems are now interconnected, mobile devices extensively used as well as remote accesses and data sharing. Thus, key assets of healthcare facilities are exposed to greater cyber-risks: their new nature in particular, makes their impact much higher than in the past (p.2).

Furthermore, the cyber threats faced by healthcare organizations have also evolved. In recent years, the value of personal data – including EHRs - has increased on the black market. Because of this increased potential financial gains, adversaries are now more numerous and better-skilled. As a result, they tend to move away from traditional attack patterns that physical security, training and digital perimeter defenses (firewall, intrusion detection systems) protect facilities against. Therefore, generally speaking, new cyber-risks in hospitals are both more probable and difficult to detect.

This trend of increasing cyber-risks criticality in healthcare facilities will continue. In fact, according to KPMG (2016) "interconnectivity of data in healthcare holds huge promise for health outcomes – improving both quality and efficiency of medicine." (p.2). Therefore, interconnectivity in healthcare will keep developing and consequently the attack surface and the exposure of the assets will keep growing. Cyber-attack opportunities will be more numerous and as adversaries become more skilled, cyber threats in hospitals will probably continue to multiply and become more complex.

Adversaries profiles

In its report, ISE (2016) identified the most likely adversaries faced by healthcare facilities (p.22-24). However, not all of them face the same threats. "For instance, a small healthcare facility in an unpopulated area may not be concerned with nation state or terrorist threats, while a metropolitan area hospital could be" (p.22). Understanding the profile, motivation and sophistication of the actual adversaries is therefore paramount to adopt the appropriate security policy.

The following paragraph gives an overview of the most likely adversaries faced by healthcare facilities as well as their intentions regarding the key assets (in particular, patient health and patient records).

Individuals and small groups of hackers constitute a first category of attackers. They are mainly motivated by profit and notoriety. Hence, they usually choose their targets according to opportunities and make use of unsophisticated means.

Then, political groups and paparazzi represent another type of threat. They are motivated by hacktivism but also political and financial gain. They most often aim at embarrassing, discrediting, blackmailing or selling information about high profile individuals.

As for criminal organizations, they are motivated by financial gain and more broadly criminal activities such as extortion, blackmail, coercion. They may aim at obtaining medical records about target individuals, threatening them or causing physical harm to them. They may also profit from the exploitation of untargeted EHR in volume.

Terrorists, for their part, are motivated by inspiring fear and cause harm. Their objective is usually to harm or threaten individuals.

Finally, nation-state attackers are the greatest threat likely to be faced. Indeed, enemy nations may aim at harming or threatening individuals. They also may want to obtain PIIs and/or EHRs of groups of individuals for mass exploitation.

The table below, extracted from ISE's report (2016, p.3)), summarizes the different profiles of attackers and their likely targets.

	Patient Health		Patient Records	
Adversary	Targeted (Specific Victims)	Untargeted (Indiscriminate)	Targeted (Specific Victims)	Untargeted (Indiscriminate)
Individual / Small Group				YES
Political Groups / Hacktivists /			YES	
Organized Crime	YES		YES	YES
Terrorism / Terrorist Org.	YES	YES		
Nation States	YES	YES	YES	YES

FIGURE 1: CAPABILITIES AND MOTIVATIONS OF HEALTHCARE ORGANIZATIONS ADVERSARIES

2. Attack anatomies

2.1. Frequent types of attacks

The situation regarding cybersecurity in healthcare facilities - presented in more detail in the next section - is quite alarming. Indeed, as at July 2013, the health IT security firm Red Spin released a report on the matter (D. Munro, 2014), showing how sensitive this issue has become:

- Almost 30 million patient health records have been affected by breaches since 2009.
- An increase of +137.7% in the number of patient records breached was noticed in 2012-2013.
- More than one third of attacks were due to the loss or theft of an electronic device, raising the question of employees' cyber-awareness (later tackled in this report).
- According to J. Pagliery (2015), more than 4 million records were breached in a single attack in 2014 (and even 80 million in 2015), revealing how massive an attack towards a healthcare facility can be. In fact, hackers can spend a considerable amount of resources to get their hand on extremely sensitive information. The attack was led in September 2014, and was only discovered one month after the breach.
- UCLA claims they block "millions of known hacker attempts each year".
- In 2015, as mentioned by T. Costello (2016), around 100 million health care records were stolen.

One of the most popular types of cyber-attacks mainly targeting hospitals is ransomware. The list of hospitals hit by this type of attacks keeps getting longer and examples of such attacks are flooding the news: in 2015, experts estimated the number of ransomware attacks to be close to 1,000 per day, which is 35% more than the previous year - the number even rose to 4,000 attacks on certain days according to a report published by Symantec (2016).

These attacks are quite similar and usually show the following pattern:

- Hackers gain access to the facility information system using diverse methods: physical presence (e.g. USB drive), exploitation of vulnerable and expired software, theft of staff's mobile devices and even phishing or malicious emails.
- Once hackers have access to the IS, they use a special virus that holds the system hostage by encrypting the data it contains. Therefore, it becomes completely inaccessible and unusable until hackers are paid a ransom - usually in Bitcoin to make it untraceable - as the virus remains in the system and prevents anyone from using it.
- What makes hospitals such easy targets is their time sensitivity. Indeed, without quick access to patients' health record, their care may be delayed, which could result in serious consequences on their health - even death - and so lawsuits for the hospital. Thus, facilities usually do not take any additional risks and they directly pay the ransom.

This type of attack is very popular as it is extremely simple in every way: it is easy to implement (a malicious email opened by a staff member can be enough) and it is an easy way to make cash (perpetrators only wait until the hospital pays the ransom). Finally, as hackers do not need to extract any data from the IS, they barely expose themselves.

Another common attack is the "classical" information theft: hackers manage to get inside the healthcare facility's IS (phishing, stolen portable devices…) and steal as much information as possible. This type of attack is even more dangerous than ransomware but more difficult and time-consuming for hackers. However, it is also more rewarding. Indeed, on the dark web and illegal markets, stolen

credit cards go for $1-$3 and social security numbers are worth around $15, whereas, as previously mentioned, complete health care records are valued $50 each, keeping in mind that one attack can give access to millions of patients' records.

2.2. Are cyberattacks aimed at health sector actors similar?

One of the main issues of the health sector is the multiplicity of actors handling patients' medical record and so the numerous potential targets. Indeed, each entity can be attacked and hackers can get equal profits by targeting different entities. The examples are quite numerous: hospitals (M. Orcutt, 2014), insurance companies (R. Hackett, 2015) and even public health agencies (J. Conn, 2016).

This shows how diversified cyber-attacks can be in the health sector. As detailed before, hackers have multiple choices regarding the way they want to conduct their attack: targeted, untargeted, implement ransomware and hold hospitals hostage, etc. Hence attacks are very diverse, which is one of the reasons why it is so complicated to prevent them from happening. This diversity is effective on several levels:

- Benefiting from the abundance of operators having access to confidential information, but also of the large range of hardware used in these facilities: personal computers, mobile devices, medical hardware, data storage facilities, inventory systems, power supply...
- Picking one hacking method among many: physically targeting and entering the facility IS (L. Vass, 2016), theft of an employee's personal device, remote hacking (through phishing, scams, vulnerabilities exploitation…)
- Choosingthe type of attack: ransomware and information theft, for the most common attacks, but also power shortages, altering patients' results, etc.

We could go on with the different types of attacks and targets hackers can think of, but what is essential here is to understand that defending such an open field is particularly difficult. This is precisely why hackers prey on health care facilities.

As described previously, hackers are nowadays more prone to choose the "easy and lazy way" and launch ransomware attacks. The problem is that the facilities have to protect themselves not only against this type of attack (which is, besides, very difficult to predict), but also against all those quoted in the previous sections. In addition, this list of threats keeps getting longer along with the digitalization and use of mobile devices in the healthcare industry.

3. Current state of cybersecurity in healthcare facilities

In its 2015 report, KPMG pointed out that "the healthcare industry is behind other industries in protecting its infrastructure and electronic protected health information (ePHI)" (p.2). In addition, it revealed a lack of awareness of healthcare facilities managers regarding "the sophistication of hackers and their means to infiltrate confidential patient data networks" (p.2). This translates into a significant and expanding gap between "the magnitude of the threat against health care information that has grown exponentially" (p.2) last recent years and the resources allocated to security –especially cybersecurity- in hospitals.

ISE (2016) investigated a representative range of American hospitals and found out that healthcare facilities do usually have strategies to counter untargeted attacks against patient records. However, they totally disregard the motivations and strategies that would be employed if attackers targeted patient health or precise patient records (p.3).

Indeed, ISE (2016) identified failures in properly addressing modern security threats at three different levels: organizational, technical and physical (p.5). Most of them are security design issues. Thus, they directly affect the way the staff (medical or not) implements security measures.

3.1. Organizational level

At the business level, the main issue is the lack of funding dedicated to Information Security. Currently, the budget allocated to Information Security in the health field, is way lower than in the other industries despite the high value of its assets and so the high level of threat it faces. This is due to the fact that Information Security is not seen as a priority in most facilities. Indeed, in the medical community, protecting patients' health is associated with direct means such as physicians' skills, treatments, medical devices, etc. but rarely with cybersecurity. Thus, the root of the funding problem is the lack of awareness that exists in hospitals, about the critical role of Information Security in ensuring patients' safety.

Besides, most of the other cybersecurity-related problems encountered by hospitals stem from the lack of resources they have in this domain. This is illustrated, among others, by the small size of the Information Security staff in healthcare facilities. According to KPMG (2015), in the USA, "almost one-fifth of healthcare providers don't have a leader solely responsible for information technology security" and "25% of facilities do not have a security operations center to identify and evaluate threats" (p.5). Therefore, security matters are often handled by the IT staff who doesn't generally have the required skills and background to be fully competent.

When the hospital does have an IS staff, an improper organizational structure may prevent them from having the sufficient leverage to define strong security policies. In fact, according to ISE report (2015), the Information Security team is most often integrated into the IT department and so under the control of the CIO. However, IS and IT have diverging guidelines: IT aims first at making systems easy-to-use whereas IS aims at making them secure - that can increase their complexity for users (e.g. 2-factor authentication). As a result, in conflictual situations, IS considerations tend to be discarded in favor of the IT ones.

Then, security policies were often found defaulting in the investigated hospitals. They should define the facility's goals in terms of security and provides detailed requirements on how to achieve them. However, in most hospitals, policies appear to be either not implemented, not enforced or not

auditable as their requirements were not precise enough. For instance, facilities do not always have a network policy to compare their implementation against.

Even when they have well-defined security policies, facilities almost never perform regular audits of their infrastructure to check its compliance with them and assess its vulnerabilities.

Finally, hospitals staff (medical or not) receive no or minimal security training. Hence, most of them are not familiar with the elementary good practices and the common mistakes to avoid. In addition, they show a weak risk awareness and understanding of the threat landscape increasing the hospital vulnerability to cyberattacks.

3.2. Technical level

During its investigation, ISE noticed that most hospitals do not have full knowledge of their IT infrastructure. Indeed, few of them have a precise picture of their network, the devices it is made of, etc. and documents to summarizing this information. This inevitably allows security breaches and vulnerabilities to develop as updates and upgrades are delayed, devices misconfigured and legacy systems kept online although no longer used.

According to KPMG, healthcare facilities also have difficulties in "understanding, tracking, reporting and managing threats effectively. Mature incident and vulnerability management processes are lacking in most organizations, and thus, daily threats aren't even reported" (p.4). This directly stems from the fact that few hospitals log network/system events and even fewer monitor these reports to detect in-progress or past attacks. This data is however paramount to reducing damages done by adversaries and addressing systems loopholes.

Then, most hospitals' networks are designed without taking into account security matters. In particular, their architecture makes difficult or even impossible the implementation of efficient security controls. In fact, most of hospitals 'networks are little or no segmented and implement poor access controls. Thus, systems as diverse as EHR portals, printers, nurse's stations, active medical devices can freely communicate with each other. In addition to facilitating the infection of the network and the leak of data, it makes the access to the devices connected to living patients very easy and so makes patients' health very vulnerable to cyber-attacks.

Finally, healthcare facilities make extensive use of legacy systems. In fact, numerous hospitals still rely on devices that have reached their end-of-life or that are no longer supported. They keep using these systems as they are still operational and that upgrading them would be too costly and/or constraining. However, legacy systems, as they are not maintained anymore, are easy targets for perpetrators. Indeed, their vulnerabilities can indefinitely be exploited since patches are no longer released to fix them.

3.3. Physical level

Physical security is not directly linked to the cyber-threats. However, it cannot be neglected as failure in assuring it can ease the task of cyber-attackers.

Physical access to the hospital network is quite easy in most facilities. Indeed, most patient rooms offer connection to the network as they expose open ports normally used for plugging medical devices. Therefore, attackers can easily create situations allowing them to access these network entry points. This exposure could be mitigated if the network were monitored. However, ISE noticed that often no

security measures are implemented for detecting the connection of intruders to the network – meaning that nothing prevents them from gaining access to it.

Then, in hospitals, many systems such as mobile workstations, unattended terminals, medical devices and wireless access points are within the physical reach of guests. Thus, adversaries could modify or gain control of a device to establish a foothold on the network or harm a patient. Preventing them from physically accessing them devices seems difficult, even unrealistic. However, various technical and organizational measures can be taken to limit the attackers' leverage (e.g. no access to the hardware, systematic logout when leaving a workstation…).

Due to the usual workflow in hospitals, medical staff often has to access information systems in front of patients – exposing each time their credentials. These repeated exposures heighten the chance they are compromised and used maliciously. Therefore, additional precautions should be taken when designing the security of medical mobile systems (use of multi-factor authentication, etc.)

Thus, given the current state of cybersecurity in hospitals, protection against cyber threats cannot be strengthened by solely patching systems. In fact, the manner in which security is understood by the healthcare industry must fundamentally change so that effective security can be implemented.

4. Improving cybersecurity in healthcare facilities

With so many cases of hacked healthcare facilities, threatening both their reputation and their patients' safety, facilities become more and more aware of the strategic importance of developing a thorough cybersecurity strategy.

Indeed, the American Hospital Association (AHA) pushes its members to invest in cybersecurity and has proposed many plans to help them do so. Here are a few procedures that the organization tries to enforce to enhance cybersecurity in healthcare facilities:

- Create a dedicated team, whose first goal would be to study the current settings of the facility's cybersecurity, establish procedures to improve it and reduce its vulnerabilities as much as possible.
- Dedicate a part of the resources to raise awareness, train employees and monitor their activities (macro-management).
- Implement a full cybersecurity plan in case of attack: investigate extensively on the incident (type of cyberattack, diagnosis of the affected equipment, study of the entry points and vulnerabilities, alert and work closely with authorities…), use the assistance of experts if needed and take appropriate disciplinary measures against non-compliant employees.
- As explained by the AHA, hospitals can consider "engaging in regional or national information-sharing organizations to learn more about the cybersecurity risks faced by hospitals" – employees as well as senior managers should be aware of all the risks they face when using their IT and learn how to reduce these risks with a compliant use.

In parallel, other organisms are promoting "smart" cybersecurity programs designed to help healthcare facilities. On the same model as the AHA, these associations offer healthcare actors solutions and plans to enhance their security and raise awareness among both managers and employees:

- HITRUST initiative offers a monthly cyber threat briefing to learn the latest news and best practices regarding defense and response in case of cyber-attacks and helps identifying early warning Indicators of Compromise (IOC) that warn in case of breach.
- NH-ISAC provides a proactive stance on cybersecurity (instead of reactive) by training and raising awareness among healthcare actors, providing security standards and protection policies and assessing the global cyber risks.

Other organizations such as the Food and Drug Administration (FDA) try to coordinate both manufacturers and users of medical devices, in order to improve their use and protection. Indeed these medical devices contain operating systems which are also vulnerable to cyber-attacks, even more since all devices tend to be interconnected with a centralized data treatment.

The main goal here is to identify potential risks associated with their medical devices, and offer the necessary software updates to overcome these vulnerabilities. This cooperation would work both ways:

- Manufacturers would provide appropriate software updates in order to keep the devices secure enough and adapt them to the constantly changing cyber environment. This would also go through an exhaustive study of the device's environment (type of authentication, frequency of use, number of authorized persons…) so as to have a better understanding of what threats they may face on a daily basis.

- Device users have to make sure all software is up-to-date and protected with the right firewalls and antiviruses. Plus, they can also inform the manufacturer with simple reports by monitoring the activity of the device: bugs, unauthorized accesses and intrusion attempts (with full reports on the method and potential success).

Here, the FDA acts as an intermediary whose sole goal is to help both entities enhancing the security of patients. Both manufacturers and users can interact independently or rely on the FDA to convey information and act as a hub. The main idea is that communication between healthcare actors is key and cooperation is the first step to protect both patients' health and privacy.

5. Conclusion

Cybersecurity has become a strategic issue for healthcare facilities. Branded as easy targets with obsolete defenses and poor IS and IT organization, hackers don't hesitate to attack them in order to get any profit they can: paralyzing the systems using ransomware, hacking into hospitals' databases and selling patients' information to the highest bidder, threatening to release private information, cutting off their power supply, etc. These are only a few examples of the numerous cyber-attack types healthcare facilities would have to deal with. This situation comes from an internal double threat: the misuse of IT systems by employees due to their low risk awareness and the lack of proper funding dedicating to Information Security. Simultaneously, the democratization of hacking techniques has also increased the number of potential perpetrators and the variety of their profile.

The multiplication of healthcare facilities hit by such attacks reveals how absolutely necessary the question of cybersecurity is. Thanks to the mediatization of these incidents, concerns now grow among general public and authorities, which trigger more and more initiatives to turn things around: FDA, AHA, HITRUST in the USA, APSSIS in France. Finally aware of the alarming state of cybersecurity in healthcare facilities, authorities offer conferences, trainings and presentations but also try to push all health sector actors towards more coordination so as to reduce their vulnerabilities. Furthermore, facilities' staff is essential in solving the hacking issues. Indeed, cybersecurity cannot be improved without training employees to use devices properly, raising their awareness on cyber threats and ensuring their compliance with security policies.

This is the first step toward an efficient holistic "firewall" against cyber threats, but won't be sufficient against sophisticated hackers and organized groups that are more and more resourceful. In fact, the real question is how healthcare facilities can implement sustainable procedures and a real strategy to defend themselves and be able to protect their assets on a long term basis. This also raises the question of our personal information and its protection: Who has access to it? Is it securely held? What can we do, as patients and clients, to ensure resources are dedicated to the protection of our private data? Many questions that we tend to forget to ask, leaving the industry dealing with it the way it wants, and not the way we need it to.

References

Conn J. (2016), *Data Breach Affects 12,000 Patients in New Mexico Substance-abuse Program,* Available at: http://www.modernhealthcare.com/article/20160523/NEWS/160529984 [Accessed 3 May 2016].

Costello T. (2016), *Hacking of Health Care Records Skyrockets,* Available at: http://www.nbcnews.com/news/us-news/hacking-health-care-records-skyrockets-n517686 [Accessed 07 June 16].

Hackett R. (2015), *Anthem, a Major Health Insurer, Suffered a Massive Hack,* Available at: http://fortune.com/2015/02/05/anthem-suffers-hack/ [Accessed 22 May 2016].

ISE - Independent Security Evaluators (2016), *Securing Hospitals*.

KPMG (2015), *Health Care and Cyber Security: Increasing Threats Require Increased Capabilities.*

Munro D. (2014), *Cyber Attack Nets 4.5 Million Records From Large Hospital System,* Available at: http://www.forbes.com/sites/danmunro/2014/08/18/cyber-attack-nets-4-5-million-records-from-large-hospital-system/#6740d5cd18bc [Accessed 04 June 16].

Orcutt M. (2014), *2015 Could Be the Year of the Hospital Hack,* Available at: https://www.technologyreview.com/s/533631/2015-could-be-the-year-of-the-hospital-hack/ [Accessed 14 May 2016].

Pagliery J. (2015), *UCLA Health Hacked, 4.5 Million Victims,* Available at: http://money.cnn.com/2015/07/17/technology/ucla-health-hack/ [Accessed 16 May 2016].

Ponemon Institute (2016), *The State of Cybersecurity in Healthcare Organizations in 2016*.

Symantec (2016), *Healthcare Internet Security Threat Report*, Vol 21.

Vaas L. (2016), *Hospitals Vulnerable to Cyber-attacks on Just About Everything,* Available at: https://nakedsecurity.sophos.com/2016/02/26/hospitals-vulnerable-to-cyber-attacks-on-just-about-everything/ [Accessed 29 May 2016].

Williams N. (2015), *Big Healthcare Breaches Affected Millions Before Anthem's Hack,* Available at: http://www.modernhealthcare.com/article/20150210/blog/302109995 [Accessed 6 May 2016].

Yadron D. (2016), *Los Angeles Hospital Paid $17,000 in Bitcoins to Ransomware Hackers,* Available at: https://www.theguardian.com/technology/2016/feb/17/los-angeles-hospital-hacked-ransombitcoin-hollywood-presbyterian-medical-center [Accessed 17 May 2016].