Security Risks in Healthcare

Ivo Miguel Lopes Pinto
Instituto Superior Técnico, Universidade de Lisboa

***Abstract*—Healthcare systems are essential to society. They handle very sensitive information, but they are often not as protected as one expects of a system of this nature to be. This problem can easily be noticed at the light of recent global events in which, for example, attackers gained access to millions of private health records causing millions of dollars in damages. Portugal may not have yet been victim of such a large scale attack, but this project aims to contribute to avoid it. The generic objective of the project is to contribute to create awareness of cybersecurity risks in the Portuguese healthcare sector. To address our objective, a top 10 of risks was compiled based on a risk analysis of the Portuguese healthcare sector along with two attack demonstrations. This document will provide an overview on the state of healthcare technologies with a cybersecurity perspective. Also, a description of threat modeling and risk assessment methodologies, and some IT-related tops of risk. Next, we present our risk analysis of the Portuguese healthcare sector, including the steps we took to achieve it and how it contributes to the sector. There is a section for our cyber-attacks video demonstrations in which we go in depth into the steps required to achieve them. Lastly, we evaluate our work with three methods that complement each other.**

***Keywords*—Healthcare, Information Systems, Security, Risk Analysis, Cybercrime**

I. Introduction

Healthcare has been around for many years and its importance is indisputable. The goal of healthcare is to maintain or improve the health of a group of human beings. *Information Technology* (IT) has become crucial for the support, sustainability and growth of most businesses [1]. Healthcare has been increasingly adopting IT, making funding channeled to healthcare organizations be used in the development of new technologies, acquisition of new equipment or hiring of extra personnel. These are adequate investment options considering the proven IT value for a business, and the healthcare goal. However, the security of some healthcare assets has been partly neglected over the years. At the light of recent events, exemplified on Table I, we can be sure that security flaws exist in healthcare systems. Flaws can lead to disastrous consequences, specially in systems that manage information so sensitive as patient health information.

From the most simple accident, as losing a laptop computer, to sophisticated malware that ciphers all data of a system, healthcare organizations have been increasingly targeted as time goes by. Even if they are not increasingly vulnerable, the knowledge that healthcare systems are potentially vulnerable to cyber-attacks is out in the open. Media articles such as [2], state that medical record information is currently more valuable than credit card information on the black market. This was exactly the type of motivation attackers needed.

The analysis of *threats* and *risks* has already proven its value, and is currently used thoroughly by multiple sectors. Science has been assessing risk probabilities for years, however, its use in other areas such as business is far more recent. These analysis can in fact save countless of companies resources, by helping in the prioritization of the most important problems over minor issues. Having that in mind, the healthcare industry should use the benefit of having at their disposal tested methodologies of risk and threat analysis to assess its current situation and effectively allocate resources to critical security measures.

Tops are known for their capacity of presenting information concisely as well as improving understanding of a given subject. For those reasons, we will present the results of our research as a *top of risks*. Our top has the intent of creating awareness to this security problem by making known the most important *cyber risks* in the Portuguese healthcare system. For even greater awareness, attack demonstrations will be created.

A. Objectives

This project aims to address the current state of healthcare systems in Portugal motivated by their essential role in our society. The goal is to perform a *risk analysis* on the Portuguese healthcare system, following a reliable methodology, and use it to compile two concrete resources:

- Top 10 of risks: A top summarizing the risk analysis, with improved readability and exposure compared to other approaches. The top ranks ten cyber risks due to the fact that ten is a good threshold for being accurate in the risks affecting the industry but still staying concise, and not losing the readers attention.
- Attack demonstrations: Video demonstrations of possible attacks aiming to create further awareness to this kind of problems.

The results are unusual deriving from the fact that the area of interest, healthcare, is very far from *cybersecurity* and (cyber-)risk analysis. A *top 10* plus video demonstrations allow the creation of awareness to the problem in a comprehensible manner to our target audience.

B. Contributions

This project aims to contribute to raise awareness of the healthcare sector for cybersecurity risks. For this, we developed a *top 10 of cyber risks*. The top does not only describe the ten most severe cyber risks faced by healthcare, but also the threats behind these risks, previous successful attacks, and potential impact. It shows how dangerous these risks can be.

Date	Target	Type of Attack
June 2010	AvMed, Inc.	Theft of two laptops
October 2011	The Nemours Foundation	Loss of property
August 2013	Advocate Health and Hospitals Corporation	Theft of four computers
May 2014	Portuguese Integrated Management of Health	Hacking
July 2014	Montana Department of Public Health	Hacking
August 2014	Community Health Services Corporation	Hacking
March 2015	Anthem, Inc. Affiliated Covered Entity	Hacking
March 2015	Premera Blue Cross	Hacking
May 2015	CareFirst BlueCross BlueShield	Hacking
July 2015	University of California, Los Angeles Health	Hacking
September 2015	Excellus Health Plan, Inc.	Hacking
February 2016	Hollywood Presbyterian Medical Center	Ransomware

TABLE I: Example attacks to healthcare systems and data

Another contribution are cyber attack video demonstrations. Seeing an attack happening is better motivation for this topic than just the description of it, as agreed by professionals in the healthcare sector. These demonstrations are publicly available on YouTube.

II. Background

This section presents an overview on topics we researched prior to starting our work. The first section explains the methodology we later used, *OWASP risk rating*. The second section presents some information about the current state of the healthcare sector in Portugal.

A. OWASP risk rating methodology

Risk rating is the process of estimating and assigning a value/category of severity to a *risk*. There are numerous risk rating methodologies currently in use. These methodologies take part in risk analysis enabling to estimate the severity of a risk to the business. Their importance is supported by the time saved and priorities well defined by having a system able to rate risks.

The OWASP risk rating methodology is adaptable and applicable to most organizations and/or systems [3]. Their approach starts with a risk equation, Equation 1.

$$Risk = Likelihood * Impact \quad (1)$$

The methodology can be broken down into six different steps [4]:

1) Identify Risk
2) Estimate likelihood factors
3) Estimate impact factors
4) Determine severity of risk
5) Decide what to fix
6) Customize risk rating model

The first step consists in identifying a security risk that needs to be rated. Information must be gathered about the *threat agent* involved, the attack that will be used, the *vulnerability* involved, and the *impact* of a successful exploit on the business.

Once the risk has been identified the following step is to estimate its *likelihood*, generally identifying if whether the likelihood is low, medium or high is sufficient. Although there are a number of factors to determinate likelihood, they can be separated in two distinct groups: threat agent factors and vulnerability factors. Each of these factors has a rating number associated from zero to nine. The threat agent factors are: skill level, motive, opportunity, and size. The vulnerability factors are: ease of discovery, ease of exploit, awareness, intrusion detection. The numbers are used to calculate the overall likelihood by simply calculating their average.

Overall Risk Severity				
Impact	High	Medium	High	Critical
	Medium	Low	Medium	High
	Low	Low	Low	Medium
		Low	Medium	High
	Likelihood			

TABLE II: Overall risk severity table [4]

The third step is estimating the impact of a risk. When considering the impact of a successful attack, it is important to realize that there are two kinds of impacts. The first is the technical impact on the application, the data it uses, and the functions it provides. The other is the business impact on the business and company operating the application [4]. As in the step two there are multiple factors rated from zero to nine, which can also be broken down into two separate groups: technical impact factors (loss of confidentiality, loss of integrity, loss of availability, loss of accountability) and business impact factors (financial damage, reputation damage, non-compliance, privacy violation). The overall impact is also calculated using the average of rating in each factor.

In order to determine the *severity of a risk*, the evaluator utilizes the overall impact and likelihood as well as the rating system described on Table II. Scores from zero to two are considered low, three to five are considered medium, and six to nine are considered high.

After the risks have been classified, they must be prioritized. As a general rule, the most severe risks have higher priority. However, sometimes it can be different for specific situations [3].

The sixth step is the customization of the risk rating model.

It is optional, however of great importance. The customization of the methodology to a business is critical for optimal adoption. A tailored model is more likely to produce results that match people perceptions about what a serious risk is [4]. An example of customization could be weighting factors differently, or adding new ones.

B. Portuguese healthcare sector

Portugal has a healthcare sector with a large public participation [5]. The ministry of health has an entity called Serviços Partilhados do Ministério da Saúde (SPMS) which provides guidelines, best practices, and identifies challenges and competencies in the sector. The importance of this entity for our context is high, because it creates the directives about information systems security.

Although Portugal has this transversal entity, SPMS, it does not enforce specific procedures, which leads us to the lack of available information about the sector state of the art. Each local institution (hospitals, clinics) is responsible for their own security. They interpret these guidelines and best practices, and deploy solutions they see fit. In this structure each institution can have different measures and systems in place, and information about which is being used is not public. Also, materials such as risk analysis previously conducted, former vulnerabilities lists, or any other report about cybersecurity are private to the organizations and not available.

There were no regulations in Portugal enforcing the need of publicly communicating breaches or security incidents, unlike other countries such as the U.S. [6]. This changed with the approval of the new data protection regulation in 2016, which enforces the need of communicating such incidents. However, this regulation is only in full effect in 2018.

For the previous reasons information about cybersecurity in the Portuguese healthcare sector are difficult to find. Nevertheless, one can expect the sector to have cyber hygiene measures in place [7], such as controlled use of administrative privileges or inventories of authorized and unauthorized devices. Sectors tend to be somewhat alike, and if considering so, Portugal should also suffer from the vulnerabilities other countries have.

III. Project development

This section is divided into two parts. The first is about the top 10, where we present all the steps we took to achieve it. From the preparation to the result. The second describes the processes behind our cyber attack demonstrations, which represent identified risks by our analysis.

A. Top 10

The following section is divided according to the major steps that we took to achieve our top 10 of cyber risks. The first section covers the preliminary interviews, followed by the scope definition. The third section is the most extensive with the in depth description of our risk analysis. The fourth is the description of another interview round, in which we gathered feedback for the last step, the compilation of the final top 10 of cyber risks.

1) Preliminary interviews: The preliminary interviews were a way to validate our methodology and future plans. We prepared an overview of our thesis, and some open answer questions:

1) Do you consider the presentation of the cyber risk analysis in a top 10 format adequate?
2) Do you think the top 10 of cyber risks is usable in the future by this sector?
3) Do you think the video demonstrations are useful as a extra awareness raising tool?
4) Considering the structure for the video demonstration I presented, any criticism or suggestion?
5) Are there any resources that you could recommend me about the current sector state? e.g. previous cyber risk analysis, previous cyber attack data...
6) Do you recommend me having this conversation with someone else, in order to gather more information before starting the development?

We interviewed three people. Without the permission to reveal names, two of them are part of SPMS, and the other an IT director of a major Lisbon hospital group.

The first question answers were not all identical. Two of the three interviewees agreed to the top 10 format, the other argued that there were still some considerable downsides, such as only referencing ten cyber risks.

In the second question all three interviewees considered the top 10 usable in the future, although one showed some concerns about the methodology used being OWASP.

The third question had unanimous feedback. Every interviewee considered the attack demonstrations a very good way to raise awareness to this matter.

The fourth question also had unanimous feedback, with every interviewee agreeing to the proposed demonstration structure. The only suggestion made, the same by two of the three interviewees, was to make this cyber attack on a real target e.g. a Portuguese hospital, instead of a sandbox environment to motivate the nonbelievers that the threat is real.

In the fifth question no resources were recommended by any of the interviewees. The reason for this is that due to regulations these resources are confidential, and not made available outside these organizations.

For the last question, the interviewees recommended other individuals that were already in our list, so it did not expand our candidate pool.

From these initial interviews we concluded that our plan made sense, and validated our top 10 idea. Also we tried taking in consideration real targets for our attack demonstration.

2) Scope definition: The project started with a scope definition, a very important step as it serves as a base for the risk analysis. In this step we established which assets exist in the industry, which of those assets depend on IT to function properly, possible threats, attacks types, and vulnerabilities. To aid us in the scope definition we used the work surveyed in Section II, but also extra resources such as [8], [9]

a) Assets: Bellow we enumerate the primary assets found within the healthcare sector. Some are patient specific which we consider the highest priority asset to protect, others indirectly affect patients, and there is also assets that do not affect patients in any way but affect the organization. Attacks against these assets can disrupt patient care, affect the organization in financial, reputation or other ways, or even have effects on patients safety.

- Electronic medical devices, both active and passive devices;
- Electronic business devices e.g. servers, computers, power equipment;
- Healthcare personnel, both involved in patient care or in other activities;
- Software applications;
- Service availability;
- Patient health;
- Patient information e.g. electronic health records;
- Intellectual property and proprietary information.

b) Threats: In addition to the identification of assets, it is crucial to identify the adversaries. Although not every healthcare facility may face the same adversaries, bellow we enumerate all the threats we consider to be relevant in this sector.

- Nation states;
- Terrorists;
- Organized crime;
- Internal personnel;
- Individual/groups of hackers;
- Business rivals e.g. other hospitals, clinics;
- Companies e.g. insurers, banks, pharmaceuticals;
- External suppliers.

c) Vulnerabilities: We used data from our related work, and former attacks on other countries to gather a list of possible vulnerabilities that exist on the healthcare sector, from quite an extensive list with over twenty items, we shortened it to ten items by clustering some specific vulnerabilities into bigger categories, and also by abandoning some vulnerabilities that we did not consider relevant enough. Following we present these ten vulnerabilities:

- Physical access to critical hospital assets lack proper control;
- Unauthorized system access;
- Lack of active protection measures;
- Lack of adequate security personnel;
- Mobile devices;
- Compromising medical devices;
- Denial of service and business continuity;
- Lack of training about good security practices;
- Network vulnerabilities;
- Software vulnerabilities.

3) Risk analysis: The methodology we followed to perform this risk analysis was the *OWASP risk rating methodology*, which we already covered in Section II-A. In summary this methodology attempts to rate the severity of risks after they have been identified, based on different factors such as threat, vulnerability and impact factors. We estimate these factor values based on categories, and calculate the result.

However, this methodology is customizable and we took advantage of it. We made some changes to best suite our sector. We removed a factor, *loss of accountability*, from the technical impact factors since we do not think it adds any value to our analysis. We also added one impact factor, *patient health*, in a new category which we created called *patient safety*. These changes in factors altered the way we calculate the overall impact: it is still the average of the technical and business factors but it also uses the patient health factor with a multiplier of 2. The reasons behind this multiplier of 2 are our intent of making our analysis more focused on patient impact than business or technical impact, and the importance of the safety of patients.

The first step to perform our analysis was to cross-reference our vulnerabilities with our threats. However, in this step we encountered our first problem. This cross-referencing was going to produce a massive number of tables. In order to solve this problem we analyzed our threats and decided to use a single threat that we called *skilled and motivated attacker*. Nevertheless, we still reference which specific threats are relevant for each risk, and if the calculations of the severity categories change based on a specific threat we make reference to it.

Based on our previously presented scope, we compiled a list of 10 risks. These risks resulted from the cross-referencing of our identified vulnerabilities with healthcare assets. When we recognize that a vulnerability could have an impact in one or more assets, we identify it as a risk. The lists of vulnerabilities and assets are defined in Section III-A2. The 10 risks are the following:

- Physical access to servers;
- Social engineering;
- Mobile devices;
- Software vulnerabilities;
- Network vulnerabilities;
- Denial of service and business continuity;
- Compromising medical devices;
- Unauthorized systems access;
- Lack of active protection measures;
- Lack of adequate security personnel.

Bellow we are only going to present the analysis of one risk followed by relevant threats, attack types, environments, and calculations for that risk. We present these properties for every risk in the full version of the document. Although, a summary of the analysis is present on Table V.

a) Physical access to servers: The calculations for each level (threat level, vulnerability level, and impact level) are based on the factors value on the two tables presented for each risk (Table III and Table IV for this risk). Threat level is the overall threat, vulnerability level is the overall vulnerability, and impact level is the overall impact. Risk severity is the average of these levels.

A generalized threat, *skilled and motivated attacker*, was used for the calculations. Aside from internal personnel, all threats would produce equivalent overall threat levels and consequently risk severity. Internal personnel have better opportunity. This leads to an increase in threat level to high, however maintaining the same overall risk severity.

Value attribution justification: Regarding threat agent factors, the skill level is very high for our generic attacker (Skill level: 9). The value for motive is justified by the possible good reward of a successful attack (Motive: 7), opportunity is low because gaining physical access to specific parts of a facility is hard (Opportunity: 2). The size factor represents how large is the threat agent group, in this case as large as users with physical access (Size: 4).

This vulnerability is easily discovered by observation (Ease of discovery: 7), also easily exploited due to the lack of technical skills and resources required by this threat agent group (Ease of exploit: 5). We believe the vulnerability is currently hidden, as there is no public discussion of it (Awareness: 4). The intrusion detection is there, in the form of video surveillance or other mechanisms, although it may not be reviewed if there is no sign of alarm (Intrusion detection: 7).

The impact of a successful attempt can lead to confidential data disclosure, although the size may vary (Loss of confidentiality: 6). Loss of integrity can happen, but only on data that does not have a backup, which is less relevant (Loss of integrity: 3). Availability of services can also be affected (Loss of availability: 5). Patients health can be affected by the loss of availability of services (Patients health: 6).

Business impact will also occur. Financial damages to fix the effects of the exploited vulnerability (Financial damage: 3). Reputation damages are a product of both patient safety impact and technical impact, and can lead to a loss of faith in the affected organization (Reputation damage: 5). Privacy violations and non-compliance come from the loss of confidentiality (Non-Compliance: 5 / Privacy violation: 5).

Threat level: Medium (5.5)

Threats: Terrorists, Business rivals, Nation states, Companies, Internal personnel, Organized crime, Hackers.

Vulnerability level: Medium (5.75)

Vulnerability: Physical access to critical hospital assets lack proper control.

Attack types:

- Denial of service
- Hardware/software integrity violation
- Confidential data theft
- Data tampering

Environments:

- Hospitals
- Clinics
- Health centers
- Laboratories

Impact level: Medium (5.3)

Risk Severity: Medium (5.45)

4) Top 10 document: After our analysis, we ordered the ten cyber risks according to their severity and we got this top 10 as a result:

1) Software vulnerabilities
2) Unauthorized systems access
3) Lack of active protection measures
4) Lack of adequate security personnel
5) Compromising medical devices
6) DoS and business continuity
7) Network vulnerabilities
8) Social engineering
9) Physical access to servers
10) Mobile devices

We used this top 10 to write the top 10 document itself, where we explain briefly what is each risk, threat agents involved, possible attack vectors, assets affected, expected impact in case of successful attack, and provide a real past case.

5) Feedback questionnaires: The goal of these questionnaires was to validate our top 10, by asking risk related questions. We developed questions for each of our identified risks, with the intent of verifying if these risks are present in the Portuguese healthcare sector. The questionnaire was closed response, although there was an open field for observations in the end. These questionnaires gave us a more in-depth perspective of the Portuguese healthcare sector and its current state. The target audience was only IT healthcare professionals due to the technical nature of the questions. The number of professionals that answered our questionnaire was 23. All these professionals were chosen because they work in IT areas of Portuguese healthcare institutions.

We begin the questionnaire with a question about the size of the local institution the user is inserted into. This helps us correlating which types of institutions are vulnerable each risk.

The overall results from this questionnaire showed that Portuguese healthcare institutions are vulnerable to the risks in our top 10. Some risks are more frequently present than others, depending on the size of the institution. We did not change the ordering of our top 10, since these results supported our previous analysis results.

B. Attack demonstrations

This section will cover all the steps taken to develop the attack demonstrations. The purpose of such demonstrations is to raise awareness to the cybersecurity problems we identified, in a more graphical manner.

The video demonstrations have the planned structure: visual scheme of the attack for easier understanding, reproduction of the major steps needed to exploit the vulnerability, and a representation of the consequences of such attack.

In order to make these demonstrations we created fictional scenarios. We pretend to follow every attack step like a real attacker would. We record the important steps, and compile them into videos. Lastly, we add a voice-over.

Likelihood								
Threat Size factors					**Vulnerability factors**			
Skill level	Motive	Opportunity	Size		Ease of discovery	Ease of exploit	Awareness	Intrusion detection
9	7	2	4		7	5	4	7
Overall threat:		5.5			Overall vulnerability:		5.75	
Overall likelihood:				5.6				

TABLE III: Physical access to servers likelihood table

Technical impact				**Business impact**					**Patient safety**
Loss of confidentiality	Loss of integrity	Loss of availability		Financial damage	Reputation damage	Non-compliance	Privacy violation		Patient health
6	3	5		3	5	5	5		6
Overall technical impact:		4.6		Overall business impact:		4.5			
Overall impact:				5.3					

TABLE IV: Physical access to servers impact table

Risk	**Threat level**	**Vulnerability level**	**Impact level**	**Risk severity**
Software vulnerabilities	8.0	6.75	6.0	6.8
Unauthorized systems access	8.75	5.75	6.2	6.7
Lack of active protection measures	8.0	6.0	6.2	6.6
Lack of adequate security personnel	8.0	5.5	5.9	6.3
Compromising medical devices	6.5	4.75	6.7	6.2
DoS and business continuity	8.5	6.0	4.8	6.0
Network vulnerabilities	8.0	6.75	4.1	5.8
Social engineering	8.25	5.75	5.3	5.6
Physical access to servers	5.5	5.75	5.3	5.45
Mobile devices	5.75	6.5	1.7	3.9

TABLE V: Summary table of the risk analysis

1) Social engineering: We started by researching how a social engineering attack is orchestrated, without any special resource worth mentioning, this research provided us with a good general idea.

We decided to use e-mail as the attack vector, and distribute a simple malware. The reason behind the e-mail choice was simply the ease of representation in the video versus, for example, physical social engineering.

The first step was to find a target, we chose Serviços Partilhados do Ministério da Saúde (SPMS). They are the higher entity in Portugal in terms of IT in healthcare. The second step was to create a plan, and we did.

We started by researching their company, for instance using their website. Using a tool like Google makes easy the task of finding information about a specific target.

In order to get their e-mail footer, and domain name the attacker would e-mail them pretending to be interested in their recruitment services.

We did not really create any malware, because we have no intent of actually running the attack, only emulating it on a video. Although, in this step an attacker would develop a fully undetectable malware with features of his choosing, for instance data theft, data tampering, damages to availability, among many other possibilities. Other possibility would be to simply download a malware, or even order one on the *dark web*.

Following, the attacker would need a cover story to redistribute his malware. Our story consisted of the information systems director distributing a document of new best practices, because of the incoming legislation about privacy already approved.

To distribute the malware, the attacker just had to use Google or another *crawler*. After having their domain, *spms.min-saude.pt*, he can search for personal e-mails with that extension. The more targets the email is sent to, the higher the success rate.

The video is available on YouTube at https://www.youtube.com/watch?v=1gwPOp9NXmQ.

2) Software vulnerabilities: We started by compiling a network environment with a database, and a web application. The purpose was to simulate a real life network in a small scale. We configured each device with standard specifications.

First the attacker must choose a target. Following this first step, the attacker will want to access confidential data stored in the hospital database server. To achieve that he must find a vulnerability in one of their web applications. For this task he can use one of several automated tools available online, depending on the type of vulnerability he is searching for.

We used *SQLmap*. This tool automatically searches a web application for vulnerable injection points, and presents the results. The attacker discovers three potential entry points. The next step for him is to exploit one of these injection points, and try to extract database information.

After exploiting the attacker can simply dump the contents of the desired tables into a file.

After all these steps the attacker would now have access to confidential healthcare information.

The video is available on YouTube at https://www.youtube.com/watch?v=hF3FH0DyVks.

IV. Evaluation

This section describes the methods used to evaluate our solution. The first two sections evaluate the top 10 following a quantitative and a qualitative approach to evaluate our top, and a third evaluation for our attack demonstrations. The purpose of the quantitative approach is to provide an argument that the top 10 produced is up to date and can be used by the industry to appoint priority to cyber risks. The qualitative approach evaluates what end users think about our work, to make sure we appeal to our target audience. It also evaluates their understanding on the subjects covered, in order to prove the materials produced are comprehensible by the healthcare sector. Lastly, we try to evaluate the content and appearance of our video demonstrations along with their ease of understanding.

A. Qualitative Evaluation

We prepared a questionnaire with nine questions and a open field for observations. To validate the document itself, four questions were prepared about its appearance and content. We also prepared a question about the comprehension difficulty of the document, and a question about the applicability of the top to the current healthcare state. To measure if our target audience was educated to the topic we developed a question about the usage of learned topics in future decision making. As a bonus, we also tried to understand if we motivated these users to further research cybersecurity topics.

We sent the questionnaire along with the top 10 document to many professionals working in Portuguese institutions, and we got fifteen answers. The target audience for this questionnaire was more general than the first questionnaire we conducted. Medical care, IT, and management are examples of areas of the professionals questioned.

Figure 1 shows the results of our questionnaire.

There is a first section has a question about the type of user, followed by a question about his institution. This section helps us understand the profile of the user.

1. What is the area in the healthcare that you work?

We managed to get a very nice distribution of healthcare professionals.

2. What is the size of your local institution, in number of employees?

In terms of organization size, a majority was from big organizations. However, the others were evenly distributed.

The following section has four questions about the top 10 document itself.

3. Rate the appearance of the document.

A majority rates the document appearance high, however there are still votes on an average appearance.

4. Rate the content of the document.

Most people consider the document content of good quality.

5. Rate the difficulty of comprehension of the topics addressed for you.

The comprehension of the topics has a very disperse distribution. However, most votes are positive. This dispersion is because of the several different roles in healthcare that were questioned.

6. Rate utility of the real past cases in the document, as extra means of sensibilization.

Most votes are positive feedback. The real past cases raise awareness to the cybersecurity threat.

7. Did you research more about cybersecurity, for instance the bibliography, after having contact with our document?

We managed to get over 50 % of people to research more about our topic. We consider this to be a victory.

8. Do you consider our top applicable to the Portuguese healthcare sector, having in account the used methodology?

All votes consider the top applicable to some degree. Most consider it fully applicable.

9. Will you take into account information in our document in future professional decisions?

Many of the questioned people claim they will utilize information from our document in future work decisions. We consider it another victory.

1) Results: Fifteen people answered our questionnaire. From the ones that answered we got a good distribution of roles in the healthcare sector. The feedback was good, in terms of appearance, content, and comprehension of the document.

The real cases were considered a good tool for extra awareness.

The top was considered applicable by everyone to the Portuguese healthcare sector, and most say they will utilize the information in future professional decisions.

We also managed to get the attention of a few people to further investigate these topics.

Overall, we managed to get the results we wanted. The document is comprehensible by healthcare professionals, and raises awareness to the cybersecurity problem. On top of that we managed to make some healthcare professionals more informed for future decisions.

B. Quantitative Evaluation

This evaluation method consisted in gathering information about past events in the healthcare industry, categorizing them, and lastly comparing these to our top. The goal of this evaluation was to prove our top was up to date on cybersecurity risks.

Due to the nature of the healthcare industry in Portugal, data about cybersecurity events is private. This is not the case in other countries, for instance, in the United States of America. We took advantage of this, and used their U.S. Department of Health and Human Services Office for Civil Rights breach portal [6] to gather intel. However, this portal only shows breaches that affect privacy, and more than 500 affected users. Any attack that targets integrity, or availability is not shown. Neither are attacks with less than 500 affected users. Without any other reputable resource to use, this evaluation method will only validate the ordering in risks that affect privacy.

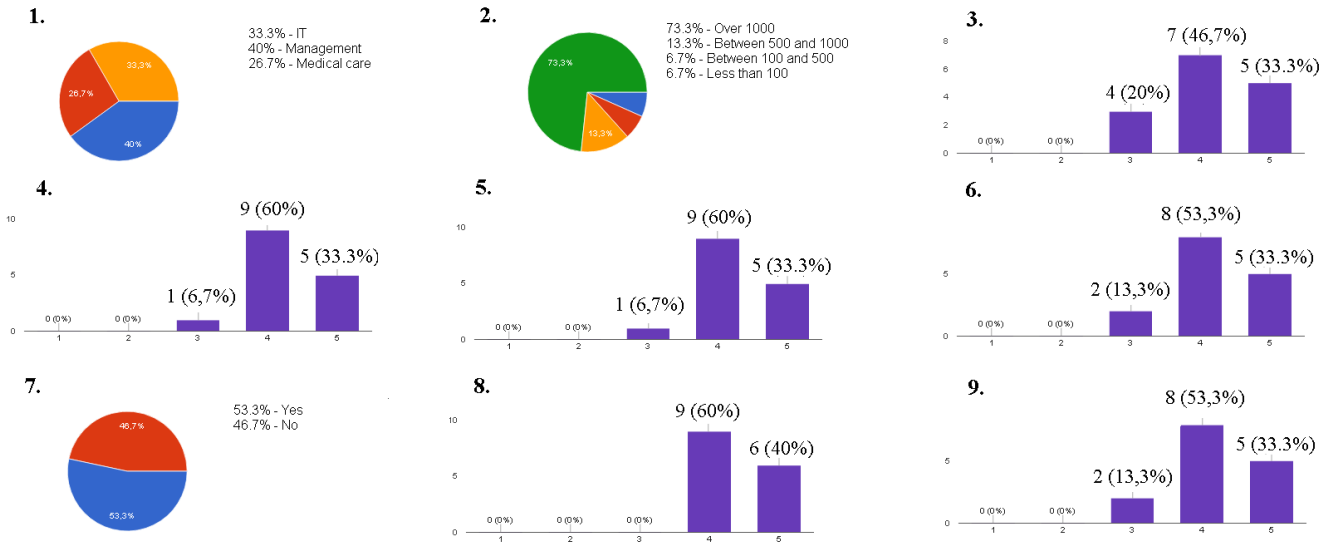

Fig. 1: Evaluation questionnaire results

We used data from a one year period, from October 2015 to October 2016. In this time there were over 14,5 million affected users and 291 incidents.

The portal uses two properties to classify the breaches, type of breach and location of breach. For type of breach there are seven options: hacking/IT incident, improper disposal, loss, theft, unauthorized access/disclosure, other, and unknown. For the property location of breach there are eight options: desktop computer, electronic medical record, e-mail, laptop, network server, other portable electronic device, paper/films, and other. Associated with each incident there is also number of affected users, data, covered entity, state in which it occurred, and a description. However, the description is optional.

Table VI presents the results from the time period we used:

The categories provided are not very good to pinpoint the vulnerability behind it. Descriptions are very vague, and in many cases nonexistent. Although we made an effort to categorize these breaches according to the risks in our top, the result are in the Table VII.

In our categorization, some software vulnerabilities incidents can be network vulnerability related. However, we have no way of knowing which. The same happens with unauthorized systems access, some can be related to physical server access.

Comparing the data to our top 10 of cyber risks, excluding the cyber risks not related to privacy, we see that software vulnerabilities are clearly the biggest risk. Followed by unauthorized system access. Both lack of active protection measures, and lack of adequate security personnel are not directly exploitable and for that reason not validated in this method.

Compromising medical devices does not target confidentiality, but patient safety. Denial of service and business continuity targets availability. Both are excluded from this evaluation.

Network vulnerabilities are included in our software vulnerabilities data, due to the lack of descriptions. Their impact is inferior to software vulnerabilities, and that is the main reason they are ranked lower.

Social engineering has many attacks but few affected users.

Physical server access is within unauthorized systems access, as previously mentioned, due to the lack of information. The low position of this risk is due to the access required for a successful attack.

Mobile devices have a very big number of affected users, and number of incidents. The position in the top is justified by the low impact an attack of this nature has.

C. Attack Demonstrations Evaluation

To evaluate our two video demonstrations we conducted a questionnaire. This questionnaire had five questions. The first two about the user profile, and the following three about the videos. We tried to evaluate the contents, appearance, and difficulty of understanding of the presented topics.

The target audience was general. Although, we tried to mainly distribute it to either IT or health sciences professionals. The reason for this distribution is the focus of our work to create awareness in these areas.

36 people answered our questionnaire. Overall, the results were positive. Raising awareness to the cybersecurity problem in the healthcare sector is our main goal, and these video demonstrations were a visual aid complementary to our top 10 document. The difficulty of understanding, and content had great feedback. The worse feedback we received was related to appearance, but we believe we still pass our desired message with the demonstrations, and succeed in complementing the top.

Type of breach	Location of breach	# users	# incidents
Unauthorized Access/Disclosure	Email	157360	30
Unauthorized Access/Disclosure	Network Server	743394	12
Unauthorized Access/Disclosure	Paper/Films	137634	48
Unauthorized Access/Disclosure	Other Portable Electronic Device	1540	2
Unauthorized Access/Disclosure	Electronic Medical Record	259989	14
Unauthorized Access/Disclosure	Other	165865	11
Unauthorized Access/Disclosure	Desktop Computer	16707	4
Unauthorized Access/Disclosure	Laptop	3118	1
Hacking/IT Incident	Network Server	11183370	49
Hacking/IT Incident	Email	76890	13
Hacking/IT Incident	Desktop Computer	137578	13
Hacking/IT Incident	Electronic Medical Record	110717	11
Hacking/IT Incident	Other	9436	4
Loss	Paper/Films	494894	6
Loss	Other Portable Electronic Device	7283	4
Loss	Other	10558	6
Theft	Desktop Computer	44900	8
Theft	Laptop	768947	26
Theft	Other	20347	5
Theft	Paper/Films	30294	16
Theft	Email	553	1
Theft	Electronic Medical Record	44761	2
Improper Disposal	Other Portable Electronic Device	2000	1
Improper Disposal	Paper/Films	122789	4

TABLE VI: Breach data from one year period

Risk	# users	# incidents
Software vulnerabilities	11517991	90
Unauthorized system access	1189073	42
Mobile devices	822670	40
Social engineering	234250	43

TABLE VII: Categorized incidents table

V. Conclusion

The growth of information technology has changed the face of many sectors, including healthcare. IT is associated with many security problems and lately there has been numerous successful attacks. This document studied some of the changes IT brought to healthcare along with their possible complications. The research tries to argue the idea that risk analysis is an important way to minimize risk effectively, by going in depth into some methodologies and their potential advantages. Tops were also analyzed for their syntheses capabilities.

We developed a top 10 of cyber risks for the Portuguese healthcare sector, which we believe represents well the current risks faced by this sector. This format allowed us to present the data in an organized manner but also improved ease of understanding to the people we presented it to.

The attack demonstrations clearly show cyber attacks can happen, and increase people's awareness to the ease of such attacks. They are available for viewing on YouTube.

We sent our document to over 100 people. By doing this we believe we are already contributing for our goal of raising awareness to the cybersecurity risks.

References

[1] C. C. Law and E. W. Ngai, "IT business value research: a critical review and research agenda," *International Journal of Enterprise Information Systems (IJEIS)*, vol. 1, no. 3, pp. 35–55, 2005.

[2] C. Humer and J. Finkle, "Your medical record is worth more to hackers than your credit card," *Reuters US*, 24 September 2014.

[3] OWASP, "OWASP Risk Rating Methodology," Available at https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology, 2016, [Online; accessed 24-May-2016].

[4] OWASP, "OWASP testing guide v4," 2014.

[5] P. A. F. de Sousa, "O sistema de saúde em Portugal: realizações e desafios," *Acta Paulista de Enfermagem*, vol. 22, pp. 884–94, 2009.

[6] U. D. of Health and H. Services, "U.S. department of health and human services office for civil rights breach portal," Available at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf, 2016, [Online; accessed 9-December-2016].

[7] R. M. M. Gomes and B. H. Soares, "Cybersecurity match supply and demand in Portuguese healthcare sector industry collaboration," 2016.

[8] Deloitte, "Networked medical device cybersecurity and patient safety: Perspectives of health care information cybersecurity executives," 2013.

[9] P. A. Williams and A. J. Woodward, "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem," *Medical devices (Auckland, NZ)*, vol. 8, p. 305, 2015.