Horizon 2020 Programme

H2020-SU-TDS-02-2018
Trusted digital solutions and Cybersecurity in Health and Care

ProTego

DATA-PROTECTION TOOLKIT REDUCING RISKS IN HOSPITALS AND CARE CENTERS

Project Nº 826284

ProTego

D3.1 Results of surveys and questionnaires to health staff and patients

Responsible:	Marina Salud
Contributors:	Marina Salud, OSR
Document Reference:	D3.1
Dissemination Level:	Public
Version:	1.01
Date:	02/04/2020

Executive summary

This document "D3.1 - Results of surveys and questionnaires to health staff and patients", describes the mechanism used to elicit the status of cybersecurity in the Protego test bed environments (Ospedale San Raffaele and Marina Salud) before the Protego tools will be developed and deployed. It describes the results obtained as well, offering a representative vision of the Protego final users, and allowing measuring the effect of the project by comparing these results with those that will be gathered during the project final phases.

Contributors Table

DOCUMENT SECTION	AUTHOR(S)	REVIEWER(S)
I, II, III, V, VI, VIII	Salvador Garcia (MS)	Antonio Jesús Gamito (GFI) Philip Usher (ICE)
II, IV, VI , VII	Diana Trojaniello (OSR)	Antonio Jesús Gamito (GFI) Philip Usher (ICE)

Table of Contents

Table of Figures

List of tables

Table of Acronyms and Definitions

Acronym / Definition	Explanation
EC	European Commission
WP	Work Package
GDPR	General Data Protection Regulation
KPI	Key Project Indicator
MS	Marina Salud
OSR	Ospedale San Raffaele
GDPR	General Data Protection Regulation
ISA	Information Security Awareness
HBM	Health Belief Model
EMR	Electronic Medical Record
CSBEH	Cybersecurity Behaviour
SUS	Perceived Susceptibility
SEV	Perceived Severity
BEN	Perceived Benefits
BAR	Perceived Barriers
SEF	Self-Efficacy
CUES	Cues to Action
SAN	Storage Area Network
EGC	Electrocardiogram

I. Introduction

The ProTego project is aimed to achieve objectives that improve cyber security in healthcare organisations, that will be measured though KPIs.

One of these objectives is to "*Increase patient trust and safety*" and it's closely related with user's cyber security awareness.

It is needed to analyse which type of users are going to use ProTego, in terms of IT maturity, how much they're aware about cyber risks, if they received education about the correct use of the tools and the risks, whether or not they know existing protocols showing how to behave under a security breach, etc.

To measure the impact of the ProTego tools, it is needed to gather this information before any of the products will be released and once all the solutions will be deployed.

But that information, as will be obtained from Ospedale San Raffaele (OSR) and Marina Salud (MS), two healthcare organizations acting as test bed in ProTego project, will also give a real perspective of the environments where project tools would be deployed and used.

The method selected to gather the referred information has been by running an online survey, covering different scopes (domains) and identifying the type of user (sample segmentation), as different types of users have different roles in cyber security and should be analysed separately.

The document is intended for use by participating researchers. In the early phases of the project it provides an overview of the users that will use the tools, and in later phases it will show the effect that the project has had from user's perspective.

Its conclusions will be used to design the educational framework that will be released as part of ProTego.

II. Process summary

As previously stated the study has been addressed by means of an online survey. The process has had four main phases as illustrated in Figure1:

1. Objectives: Definition of the objectives. These objectives guided the design of the tool (survey)
2. Design: Compose the appropriate domains, questions and samples to achieve the objectives
3. Collect: Execute the designed survey and process the data gathered, transforming that data into information.
4. Exploitation: Analysis of the information to extract knowledge. This phase started with the conclusions incorporated to the report but will go further, as this knowledge will help to design the educational program.

All the processes are completely GDPR compliant because any personal data has been collected and the identity of the users that completed the survey are completely anonymous

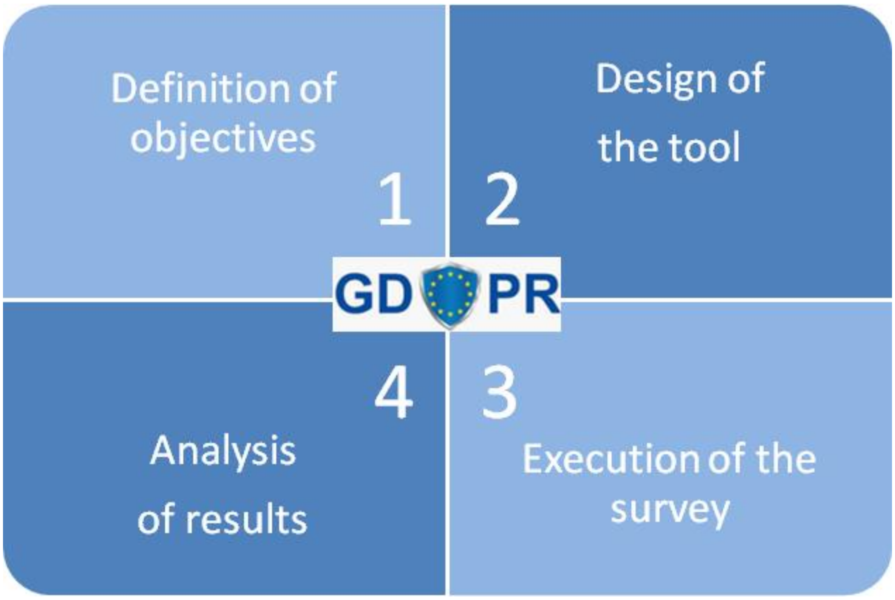


Figure 1: Process summary

II.1. Objectives

ProTego will develop and deploy both at hospitals premises and cloud infrastructures a set of technical tools that increase cybersecurity, as well an educational framework that will also improve cyber security by providing users protocols for interact with the systems and information that will increase user awareness.

In fact, hospitals represent a potential target for cyberattacks since their infrastructure could be exploited to extract valuable patient data. In particular, the next ProTego educational framework will try to make employees more aware of cybersecurity threats in order to prevent cyberattacks, thus increasing an overall protection of health care IT systems and data.

In this context, measuring the actual cybersecurity behaviours of employees in order to evaluate the target at risk represents the starting point of this plan.

Therefore, an ad hoc online survey was developed to assess the cybersecurity awareness (or **Information Security Awareness**[1]) of the future educational training target (i.e. OSR' and MS's employees) before designing new cybersecurity materials. Indeed, it was necessary to discover which employees are the most exposed to a cybersecurity risk, due to a low level of cybersecurity awareness, also considering other aspects such as the devices they use during their working activities (personal, business, electromedical devices) as well as their access to personal and special categories of data. In the study, the beliefs towards cybersecurity practices has been measured using the constructs of a behavioural model that has been widely used in health communication campaigns, namely the *Health Belief Model*.

The developed survey, executed before the ProTego tools have been deployed and after that, will serve as a baseline to assess the impact of the Project in terms of user education, and can also be used for benchmarking purposes.

II.2. Design

II.2.1. Background

Information Security Awareness (ISA) has been defined as the degree to which employees understand and adopt the recommended cybersecurity behaviours suggested in the organization's policy. However, ISA is a complex concept that includes different aspects ranging from knowledge related to information technology, to personal attitudes and beliefs towards the cyber risks. Thus, despite the importance of assessing cybersecurity awareness is widely recognized, there is no agreement on its measurement.

The common approaches are based either on *survey-based methods* or on *behavioural models*' applications. However, survey-methods often investigate only single areas of interest, while behavioural models tend to consider only the variables in the theory under investigation, excluding other important aspects that may have an impact on ISA. Promising research , which has tried to overcome these limitations, have been conducted in the last few years, however it is at an early stage of development, with few assessments of validity and reliability (e.g. Egelman and Peer, 2015; Öğütçü, Testik, & Chouseinoglou, 2016).

With the same objective, an ad hoc survey has been developed for the present research. The survey aimed to provide an overarching understanding of employee's cybersecurity awareness considering both the beliefs which may predict their cybersecurity behaviours, both some moderating variables that seemed to be relevant for the hospital context.

The choice of using a behavioural model to explore the factors underlying the cybersecurity behaviours came from the evidence that human improper behaviours result to be the weakest link of cybersecurity systems (Wiederhold, 2014): understanding the attitudes and beliefs behind the cybersecurity practices could give some insights in order to intervene on a deeper level on these behaviours.

II.2.2. The Health Belief Model

The Health Belief Model (Rosenstock, 1966) is a behavioural model that argues that individuals' likelihood of engaging in health preventive actions is determined by their perceived susceptibility to a health condition, by the perceived severity of it and by fewer perceived costs than benefits of the actions made to prevent it (Michie, West, Campbell, Brown, & Gainforth, 2014).

Skinner et al. (2015) summarised the definitions of the six primary components of the model which are able to predict the likelihood of performing the recommended behaviour as outcome variable,

[1] Information Security Awareness (ISA) has been defined as the degree to which employees understand and adopt the recommended cybersecurity behaviours suggested in the organization's policy.

also giving practical advice about the possible intervention strategies that can be used to influence these factors.

- **Perceived Susceptibility**. It is the degree to which the subject perceives himself or herself as vulnerable or at risk for a disease or a specific condition. An efficient strategy aimed at enhancing this component might describe the population at risk and the different levels of risk and tailor the risk perception in accordance with the subject's characteristics, making individual's perceptions more consistent with his or her risk.
- **Perceived Severity**. It includes the beliefs about the seriousness of a certain condition or disease, including the possible negative consequences and impact of that illness on life. A good strategy might specify the effects of a condition and trigger negative emotions such as distress or regret.
- **Perceived Benefits**. They refer to the potential positive effects of adopting a healthy behaviour, thus to the efficacy of a certain action to reduce the risk or the negative consequences of a condition. In order to increase the perceived benefits, it could be useful to provide information in favour of the recommended behaviour or trying to move the subject towards the desired action.
- **Perceived Barriers**. They are the negative aspects or obstacles the subject has to face in trying to adopt the healthy behaviour. They can be both tangible and psychological costs. It may be worthwhile to reassure the subject, to offer assistance or to correct eventual misinformation in order to reduce these barriers.
- **Self-Efficacy**. It is the confidence in one's ability to perform the recommended healthy behaviour. It is possible to increase the sense of self-efficacy providing training or guidance and using progressive goal setting, so that the subject will be more prone to engage in the recommended action and will reduce anxiety related to it.
- **Cues to action**. They refer to the internal or external factors which prompt the person to the healthy behaviour. It is appropriate to use reminders or recall system as well as increase awareness in order to offer these cues to the subject.

The model also considers other factors such as demographic information as well as structural and socio-psychological aspects as potential moderators of the beliefs related to the recommended behaviour, thus influencing healthy behaviours in an indirect way (Skinner et al., 2015). Sociodemographic factors may include age, gender, ethnicity, personality, socioeconomic status or knowledge.

The Health Belief Model has already been applied to assess cybersecurity awareness of home adopters and different organizations' employees, however no studies specifically related to the hospital context have been found. For example, Ng et al. (2009) collected the answers of 134 employees, but the respondents coming from the health or medical industry represented only the 2,2% of the sample. Furthermore, a main limitation reported from previous similar studies (e.g. Claar & Johnson, 2011) was considering large and undefined populations of interest.

Hence, the present study represents the first attempt to measure cybersecurity awareness with the Health Belief Model in the hospital context. Other than providing further evidence to the applicability of the model in cybersecurity field, using the HBM as a tool to assess cybersecurity behaviour will add to ProTego project a theoretical background which might offer a deeper understanding of hospital users in order to design a more appropriate educational framework, as it plans.

II.2.3. Research Model Development

In this study we explored the aspects behind cybersecurity behaviours performed by OSR’s and MS’s employees, using the HBM as a reference. This results in a total of six main hypothesized relationships that have been examined in the research.

Even if most studies which used Health Belief Model considered the likelihood of performing a behaviour (i.e. behavioural intention) as dependent variable, in the present research, the actual self-reported behaviours related to cybersecurity will be considered as target. This method has already been applied in a preventive healthcare study which asked subjects to report what health behaviours they really engage in (Jayanti & Burns, 1998) and also in a previous study that used the HBM to study cybersecurity behaviours of employees (Ng at al., 2009). Indeed, even if measuring self-reported behaviours might lead to self-report bias, considering the actual behaviours instead of intentions to perform them might reduce the possibility of employees to answer basing on what they evaluate as socially desirable. Moreover, according to Ng et al. (2009) it could be easier and more objective to self-assess own behaviour instead of own intention, as also highlighted by the “intention-behaviour” gap issue raised by Sheeran and Webb (2016).

Additionally, to overcome the limitations related to the debated relationships among the HBM’s constructs that led to many variations in how it has been applied (e.g. the debate for which barriers and benefits should be subtracted one to another or not; the possibility to combine additively or multiplicatively perceived susceptibility and perceived severity to create the overarching construct of “perceived threat”), in the present study, they will be considered in their direct paths relatively to the dependent variable; also, the variable “perceived threat” will not be included.

The figure below (Figure 2) shows the conceptual model of the research which is based on the Health Belief Model.

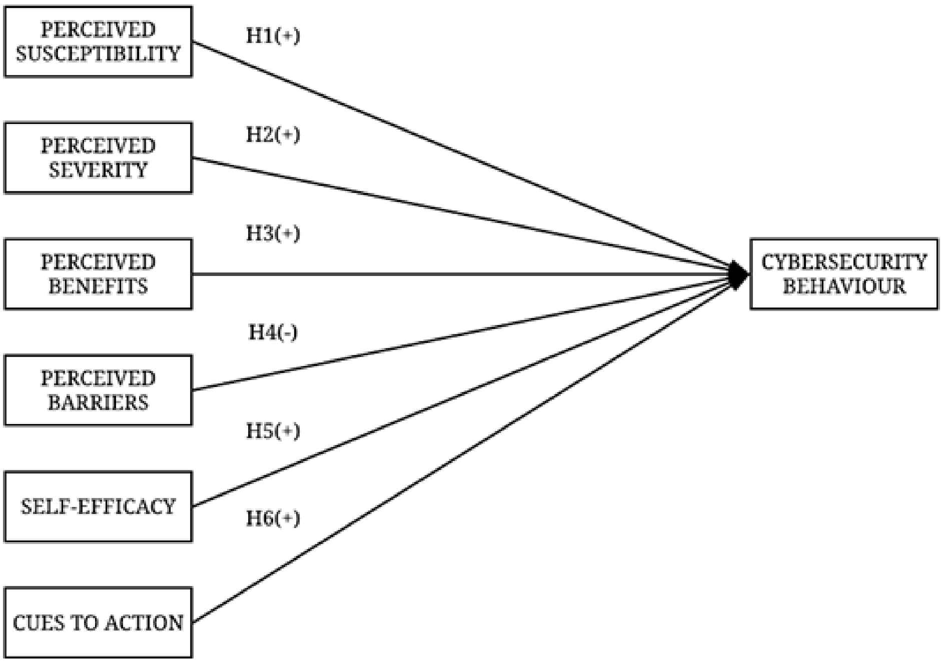


Figure 2: Research Model

II.3. Execution

Users did get notified via both an internal email communication and work meetings, notifying that the survey was published and accessible.

The survey was accessible through the Hospitals intranet for a 3 weeks period.

After that period the survey was closed and we started to process the information gathered.

II.4. Analysis

The objective of this phase is to transform the data into knowledge, that is, to extract conclusions that help us to define strategies in the design of the educational framework, especially in those actions addressed to increase user awareness.

As the reader will see in following sections, MS and OSR have followed two different approaches to perform the analysis of results and extract conclusions. In spite of that, the same survey has been used as its content allows both ways of interpretation.

- In **MS** the focus has been set at the segmentation of the target universe by a stratified sampling method. The population (hospital employees) has been divided into five user groups with clearly defined differences that are relevant to the research objectives, and the results have been embodied and construed attending to that stratification.
- In **OSR** the research methodology has been based on the investigation of two research questions and subsequent hypotheses: the first studied if independent variables based on the six main HBM’s constructs were related with the final Cybersecurity Behaviour results, and the second studied if other factors as sociodemographic, job-related and technology-related variables have an impact on the relationship between the five HBM’s constructs and the dependent variable “Cybersecurity Behaviour”.

III. Survey execution in MS

III.1. Sampling method

In MS the strategy has been to apply a stratified sampling, by dividing the MS' employees into five categories, attending to the professional group they belong to.

The reason is that these five categories have substantial differences in their work protocols (applications they use, permissions, differences in security policies, etc.) that make that the exposure to threads would be different and so part of the educational framework might be adapted for each user type.

We considered that in MS this variable is more significant than other like sociodemographic or any other behavioural variables.

It's worth to say that in Marina Salud does not exist the role of "Researcher" because it's a medium to small hospital and in Spain healthcare structure this activity tends to be done in larger Hospitals.

The resulting stratification in MS has produced these five user types:

1. IT (Information Technology department staff): they make the most exhaustive use of the systems, have higher privileges, and decide the security policies that the rest of users will follow. In Protego, they will deploy the produced tools and use them, configuring the connections between Protego and the rest of the systems. They will design the logics behind the Risk Assessment tools.

2. Support staff; within this group we consider the not clinical users working in support areas different than IT, this is, Human Resources, Financials, Logistics, Maintenance, and Appointments scheduling. They neither use the EMR nor access directly to the patient's record but use other applications that are hosted in the Hospital data center and thus need to be considered.

3. Physicians: they work almost exclusively with the Hospital EMR Cerner Millennium. They make intensive use of the patient's data and have special privileges that allow them to order actions that may have higher impact over the patient's health and safety. They order the actions (treatments, cares, drugs, tests) that the rest of the clinical users will follow.

4. Nurses: as the physicians they work almost exclusively with the EMR, but we made a distinction because they use to follow the indications ordered by physicians, although they also add information into the patient's record. From this point of view we would say that their impact over the patients' health is lower than physicians.

5. Nurse assistants: They assist nurses in less complex tasks. They only have privileges to read instructions and can't modify information into the EMR.

III.2. Validation of the instrument

This task started with the survey designed by OSR over HBM's constructs. It was reviewed with MS' IT managers and Quality department and the conclusions were that it would be desirable to shorten the survey by removing some questions out of the "Awareness Health Belief Model" key domain.

The reason was that it takes more than 15 minutes to complete the survey and the risk of drop off was considered high, and some descriptive questions were found with no effect over the conclusions. Those questions are located in the following domains:

- Attitude toward new technologies
- Cyber attacks' experience
- Some of the Devices used during working activities

- Processing of personal data
- Some of the Awareness exercises

The final decision was to maintain the complete survey, but it will be considered to shorter it in further uses.

The same reviewers designed the procedure to analyse the data gathered, introducing the concept of “Risk awareness profile” of an organization, comprising ten questions chosen as survey KPIs. This will be presented further in this document.

III.3. Execution

The survey was distributed in Spanish using a corporate WordPress plugin. Users were notified via an internal email, notifying the link to the survey.

Additionally each responsible of department explained the topic of the project and the convenience of fulfilling the survey.

The period for data collection started on 2019 October 1st to October 25th.

All the answers were made compulsory so that all the gathered responses would be complete.

III.4. Number of responses obtained

After 25 days from the notification to staff that the survey is available, we gathered 136 responses and the following graph shows the distribution in terms of type of user, which has been the variable to perform the stratification.

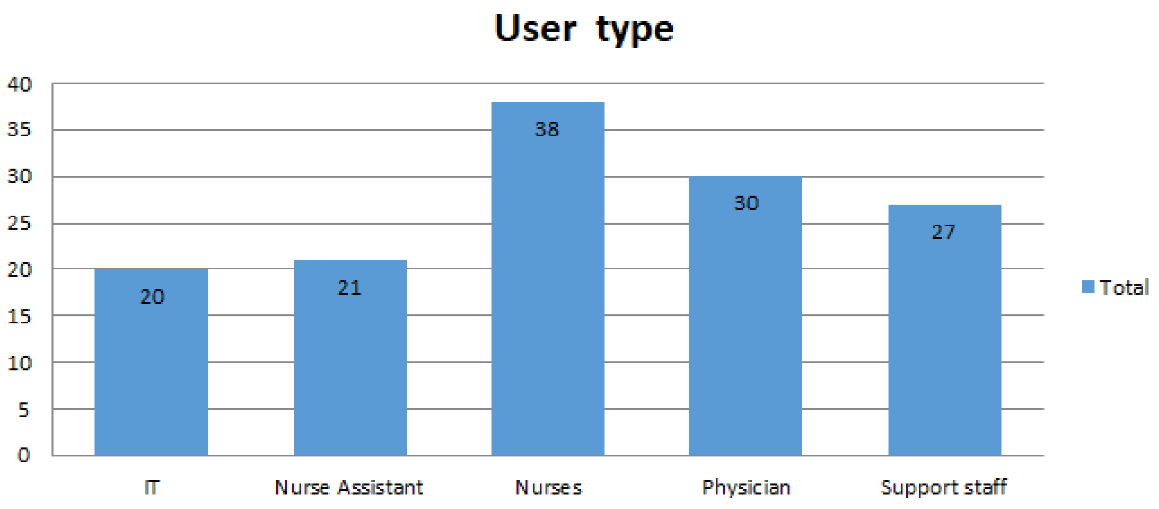


Figure 3: MS strata responses

The following table shows the participation achieved in MS, which will be the first result to analyze:

User type	Total staff	Responses obtained	Percentage (%)

IT	20	20	100
Support	276	27	9,78
Physician	360	30	8,33
Nurses	436	38	8,72
Nurse assistants	219	21	9,59
TOTAL	1311	136	10,37

Table 1: MS responses obtained

From the previous table it is worth to remark three important points:

1. The IT user type contains the main stakeholders for ProTego project, and the 100% of users responded to the survey.
2. The total sample size results in a 95% confidence level and 7% margin of error, what are acceptable results to make the survey reliable.
3. It’s needed to increase user awareness about cybersecurity for users outside IT department, what would increase the number of participants in such kind of studies. The number of users that did not respond the survey is itself an important indicator.

III.5. Analysis of results

III.5.1. Risk awareness profile

As stated at the beginning of this document, one of the main objectives of the survey are, first, to assess the cybersecurity awareness of the future educational training target and, second, to serve as a benchmark that allows to perform future trend analysis and even compare different organizations following the same pattern.

To achieve this, ten high representative questions have been selected, and the results to each one have been bunched to dichotomy, showing the percentage of negative answers. These negative answers can also be understood as the risks revealed by the survey and, so, the survey KPIs.

This strategy, represented by a spider diagram, shows the ”*risk awareness profile*” of the organization.

The following table shows the design of the Risk Awareness Profile tool:

ID	ID DOMAIN	DOMAIN	DOMAIN QUESTION	QUESTION	ANSWERS CONSIDERED
Q1	1	Demographics	N/A	Number of users that did not answer the survey	% users that did not answer the survey
Q2	2	Technological Expertise	1	How would you define your current technological expertise?	% of users that declare themselves as beginners
Q3	4	Cybersecurity Background	2	Which tools does the Hospital provide to inform its employees on cybersecurity?	% of users that can’t identify training tools provided by the hospital
Q4	6	Devices used during working activities	1	To carry out your working activities you use	% of users that don’t use mainly business devices on work activities
Q5	7	Awareness Health Belief Model (1)	1 & 2	Which of the following behaviours do you adopt in the working environment? Which of the following measures do you apply to protect your devices (both personal and/or business) from cyber attacks	% of users that apply less than 8 positive behaviours (0 to 17 scale)
Q6	7	Awareness Health Belief Model (1)	1 & 2	Which of the following behaviours do you adopt in the working environment? Which of the following measures do you apply to protect your devices (both	% of users that apply less than 5 positive behaviours (0 to 17 scale)

				personal and/or business) from cyber attacks	
Q7	8	Processing of personal data	3	Which tool do you use for sharing personal data and/or sensitive data of other people?	% of users that share sensitive data through untrusted tools (Personal e-mail, External Cloud, External USB/HD key, Skype, WhatsApp)
Q8	9	Awareness Exercises	4	Which of the two screens do you think is potentially risky in terms of cybersecurity?	% of users that could not identify a phishing email
Q9	10	Awareness Health Belief Model (2)	2	I feel that I could fall victim to a malicious attack if I failed to comply the regulation for the usage of computing resources	% of users that don't feel so much they can fall victim of a malicious attack
Q10	10	Awareness Health Belief Model (2)	12	It is inconvenient to spend time on cybersecurity training courses	% of users that don't see as positive to spend time on cyber security training

Table 2: Risk Awareness Profile design

Questions Q5 and Q6 reveals the measure of the CSBEH in two different ranges, but the aim of the educational framework is not only improve this factor but also others regarding the abilities to identify potential risks (Q4, Q8, Q7), risk and cybersecurity awareness (Q1, Q9, Q10), adherence to corporate protocols (Q3) and self-perceived IT maturity (Q2). Selected questions are also convenient for benchmarking purposes.

Results will be considered aggregate per user type, as they make different use of the system, face different risks and thus might need some differences in the educational material that will be released.

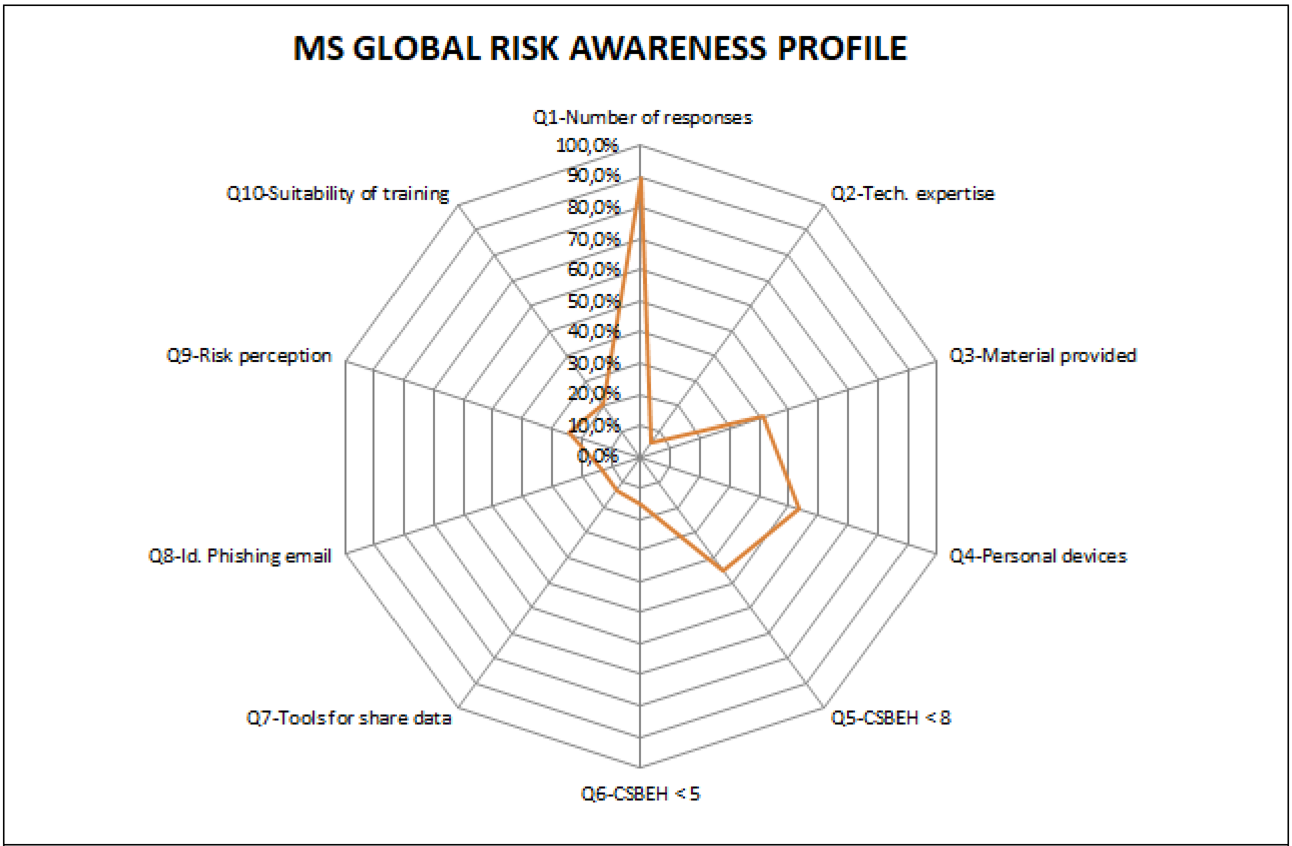
Table 3 shows the results obtained, in percentages, this is, the percentage of responses that will be understood as risk or items to improve.

QUESTION	IT (%)	Support (%)	Physician (%)	Nurse (%)	Nurse ass. (%)	GLOBAL (%)
Q1-Number of responses	0,0	90,4	91,3	91,7	90,2	89,6
Q2-Tech. Expertise	0,0	0,0	10,0	7,9	9,5	5,9
Q3-Informative material provided by the Hospital	40,0	48,1	50,0	36,8	28,6	41,2
Q4-Devices used during work activity	60,0	25,9	50,0	68,4	61,9	53,7
Q5-Awareness Health Belief Model (Less than 8)	35,0	59,3	26,7	34,2	47,6	45,4
Q6-Awareness Health Belief Model (Less than 5)	10,0	25,9	20,0	5,3	19,0	15,4
Q7-Tools used to share sensitive data	5,0	7,4	23,3	7,9	23,8	13,2
Q8-Identify phishing email	0,0	33,3	13,3	10,5	4,8	13,2
Q9-Perception of risk	0,0	22,2	53,3	5,3	42,9	24,3
Q10-Suitability to spend time in training	20,0	22,2	20,0	15,8	28,6	20,6

Table 3: Risk Awareness Profile results in MS

The results of the previous table have been translated into spider diagrams, allowing easier visualization and analysis. Table 4 includes two figures:

- the first figure illustrates the mean results for that study, which can be interpreted as the organization benchmark, not attending to user type
- the second figure shows the combined results for all user types (strata).



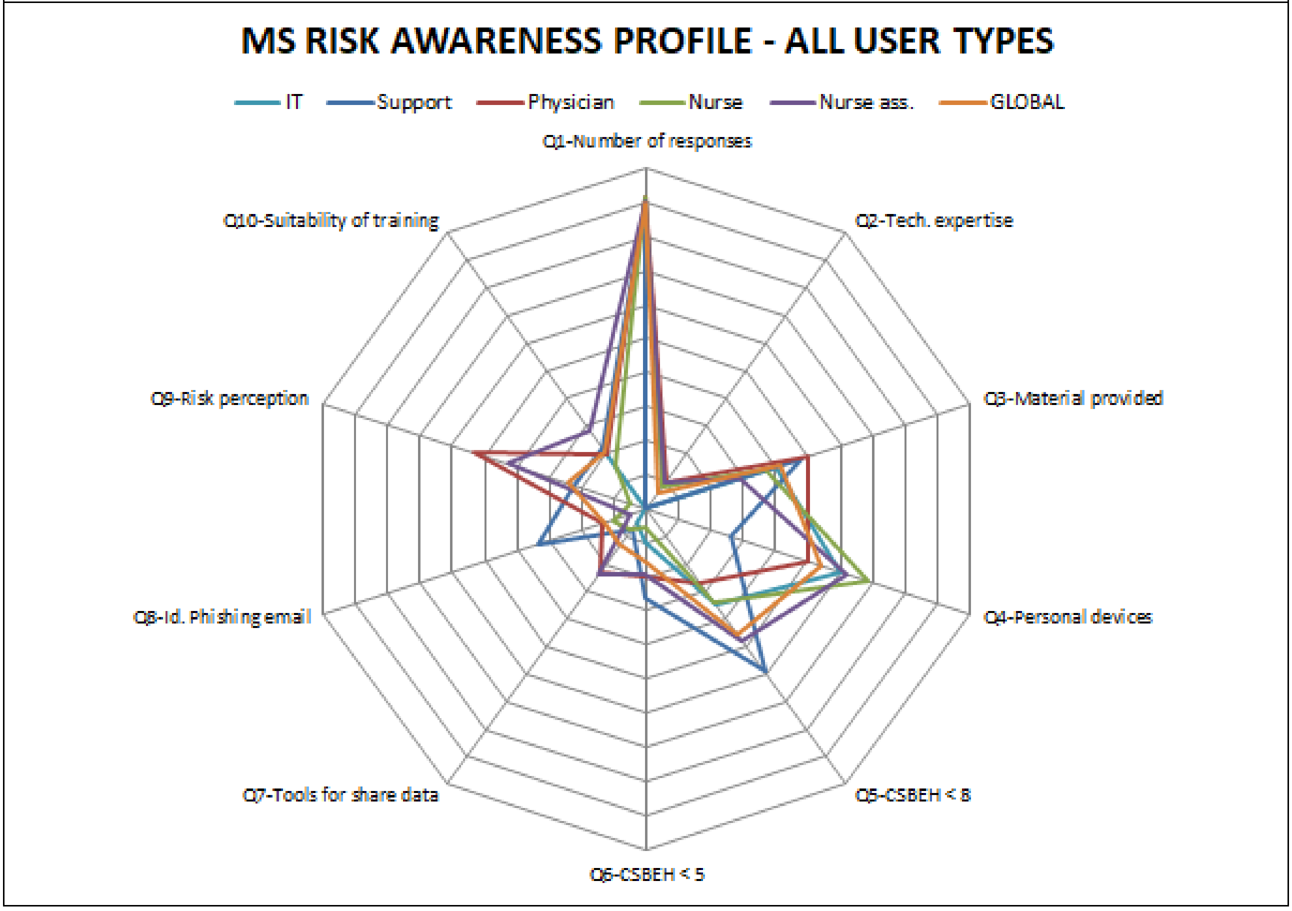
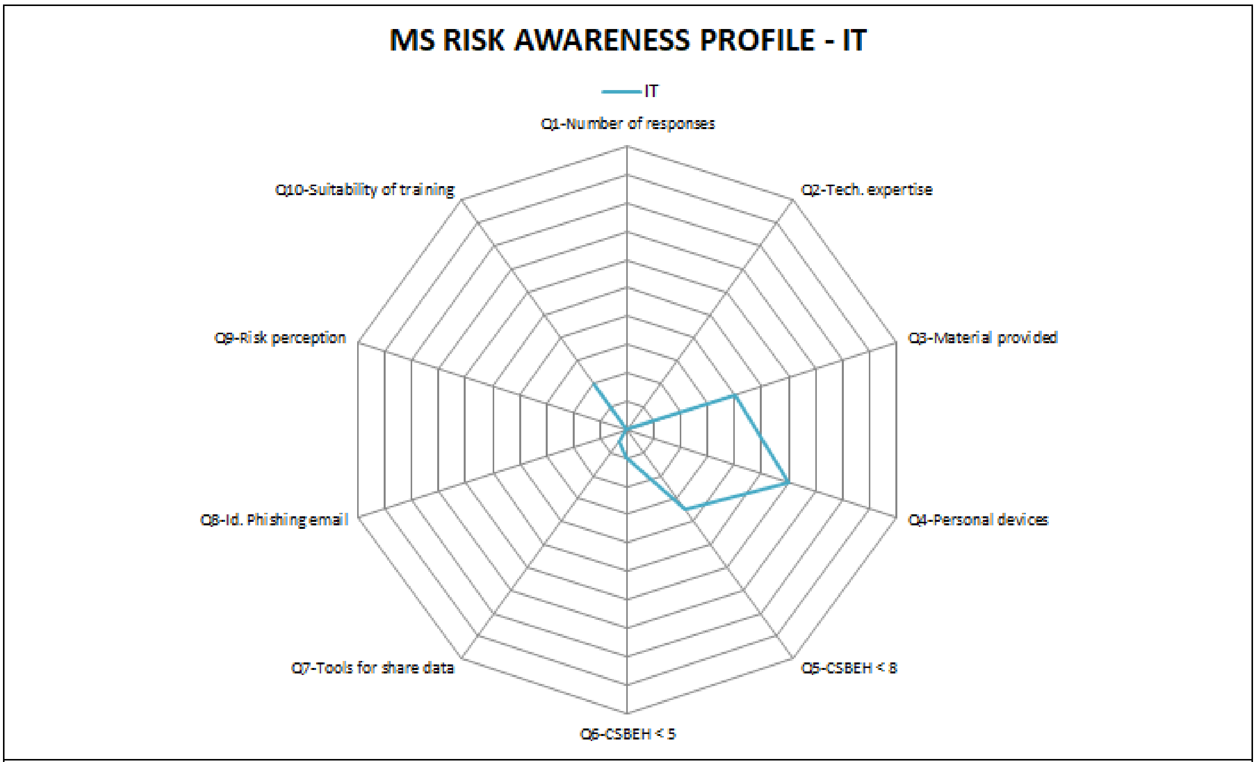
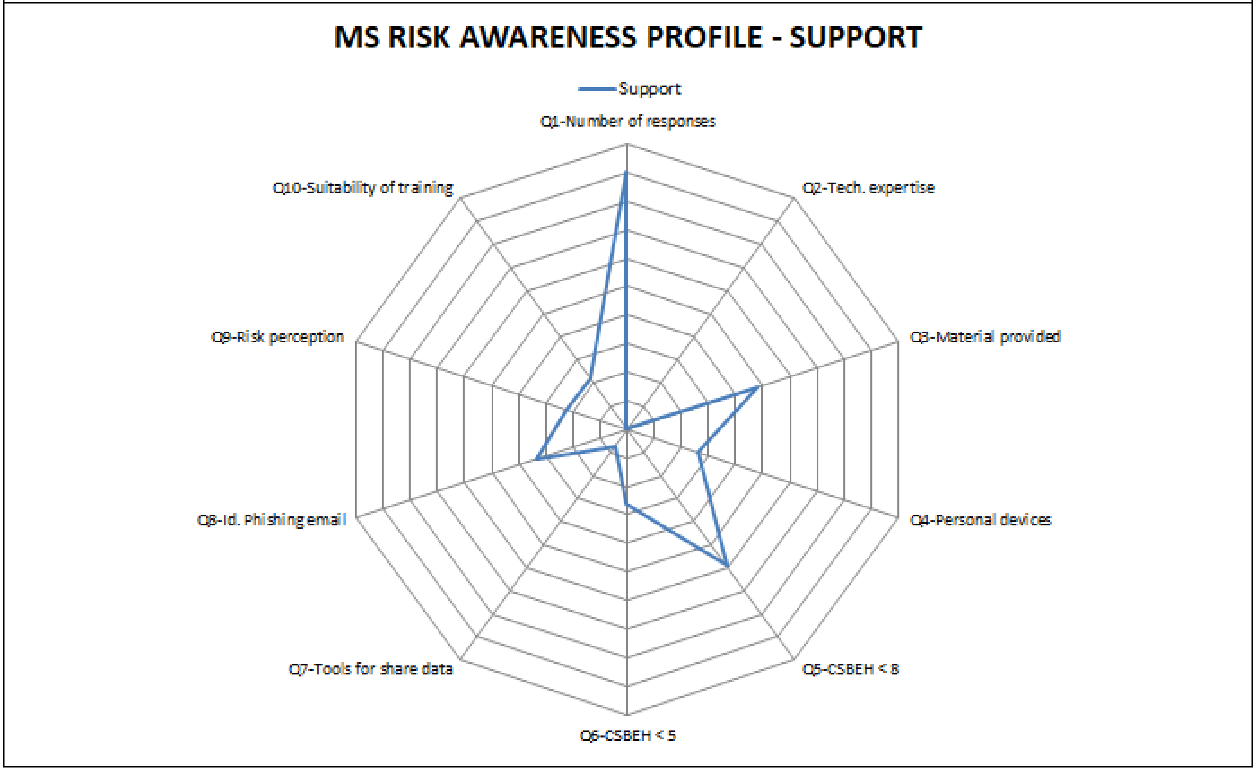
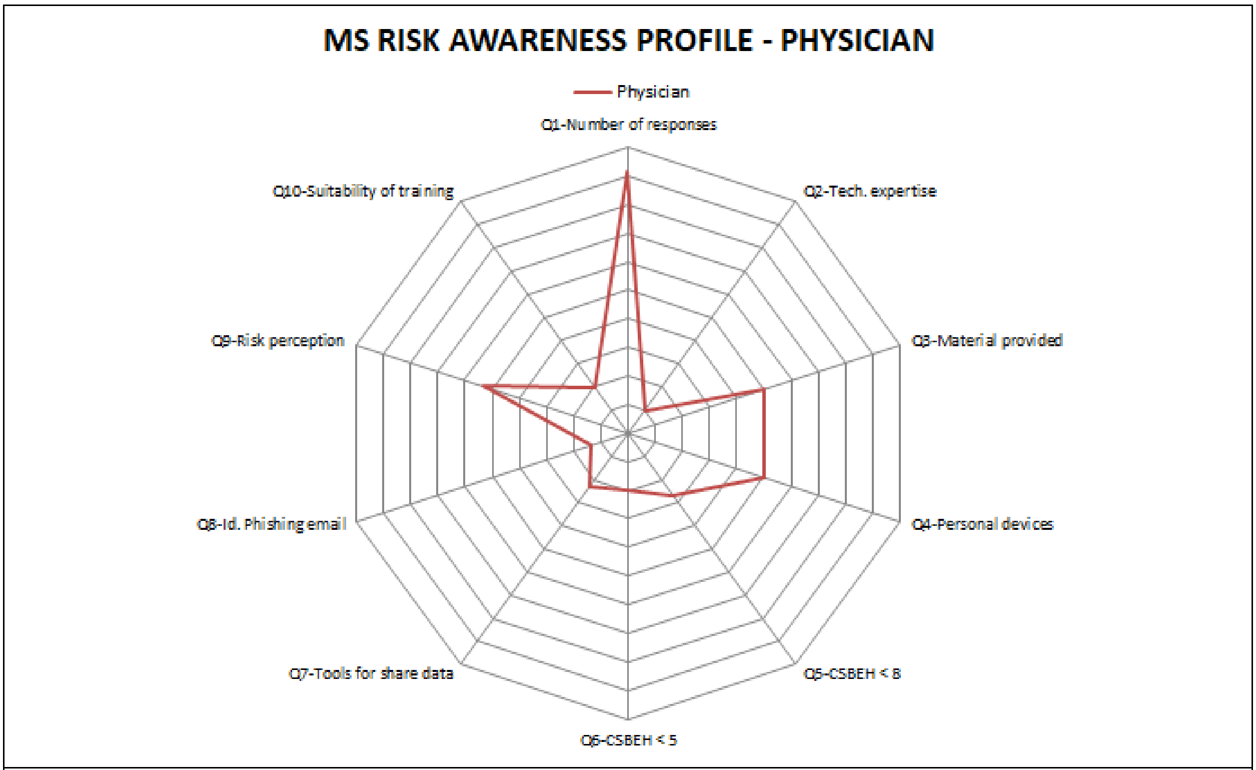


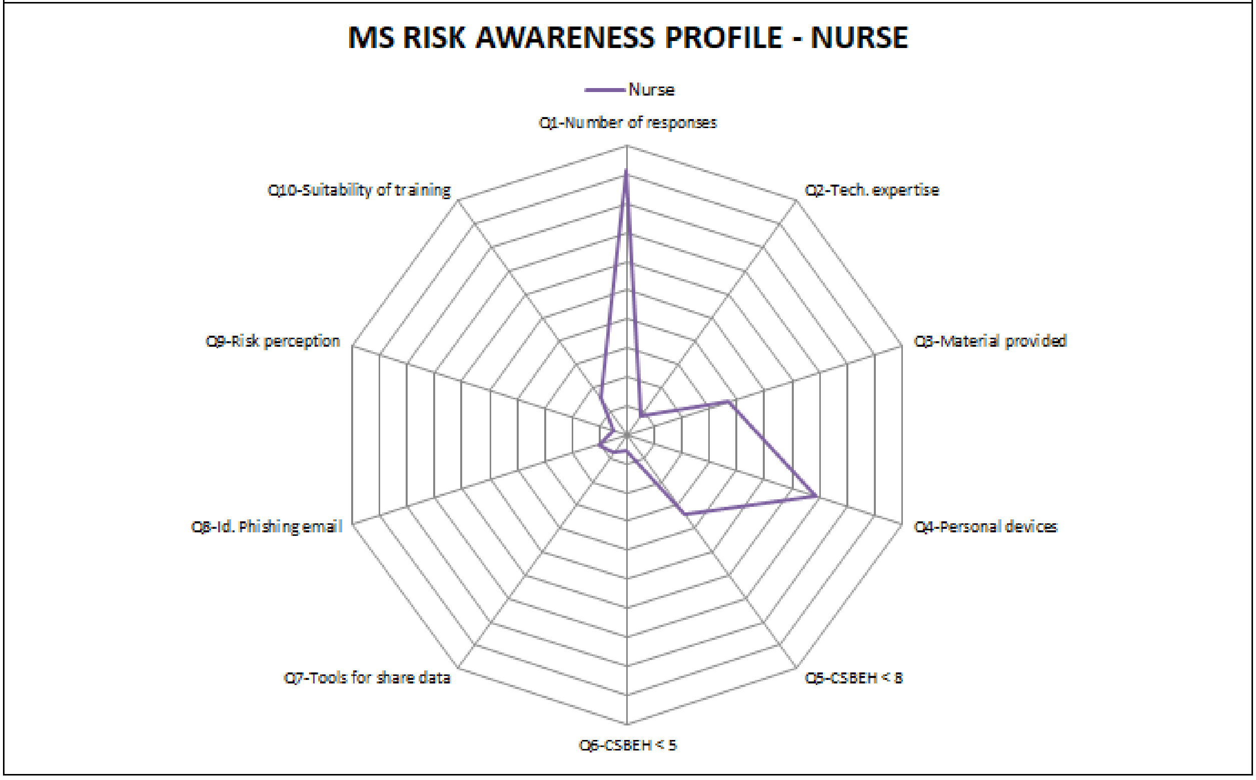
Table 4: MS global Risk Awareness Profile results

The Table 5 shows the MS risk awareness profile for each user type:


MS RISK AWARENESS PROFILE - IT
IT
Q1-Number of responses
Q2-Tech. expertise
Q3-Material provided
Q4-Personal devices
Q5-CSBEH < 8
Q6-CSBEH < 5
Q7-Tools for share data
Q8-Id. Phishing email
Q9-Risk perception
Q10-Suitability of training


MS RISK AWARENESS PROFILE - SUPPORT
Support
Q1-Number of responses
Q2-Tech. expertise
Q3-Material provided
Q4-Personal devices
Q5-CSBEH < 8
Q6-CSBEH < 5
Q7-Tools for share data
Q8-Id. Phishing email
Q9-Risk perception
Q10-Suitability of training


MS RISK AWARENESS PROFILE - PHYSICIAN
Physician
Q1-Number of responses
Q2-Tech. expertise
Q3-Material provided
Q4-Personal devices
Q5-CSBEH < 8
Q6-CSBEH < 5
Q7-Tools for share data
Q8-Id. Phishing email
Q9-Risk perception
Q10-Suitability of training


MS RISK AWARENESS PROFILE - NURSE
Nurse
Q1-Number of responses
Q2-Tech. expertise
Q3-Material provided
Q4-Personal devices
Q5-CSBEH < 8
Q6-CSBEH < 5
Q7-Tools for share data
Q8-Id. Phishing email
Q9-Risk perception
Q10-Suitability of training

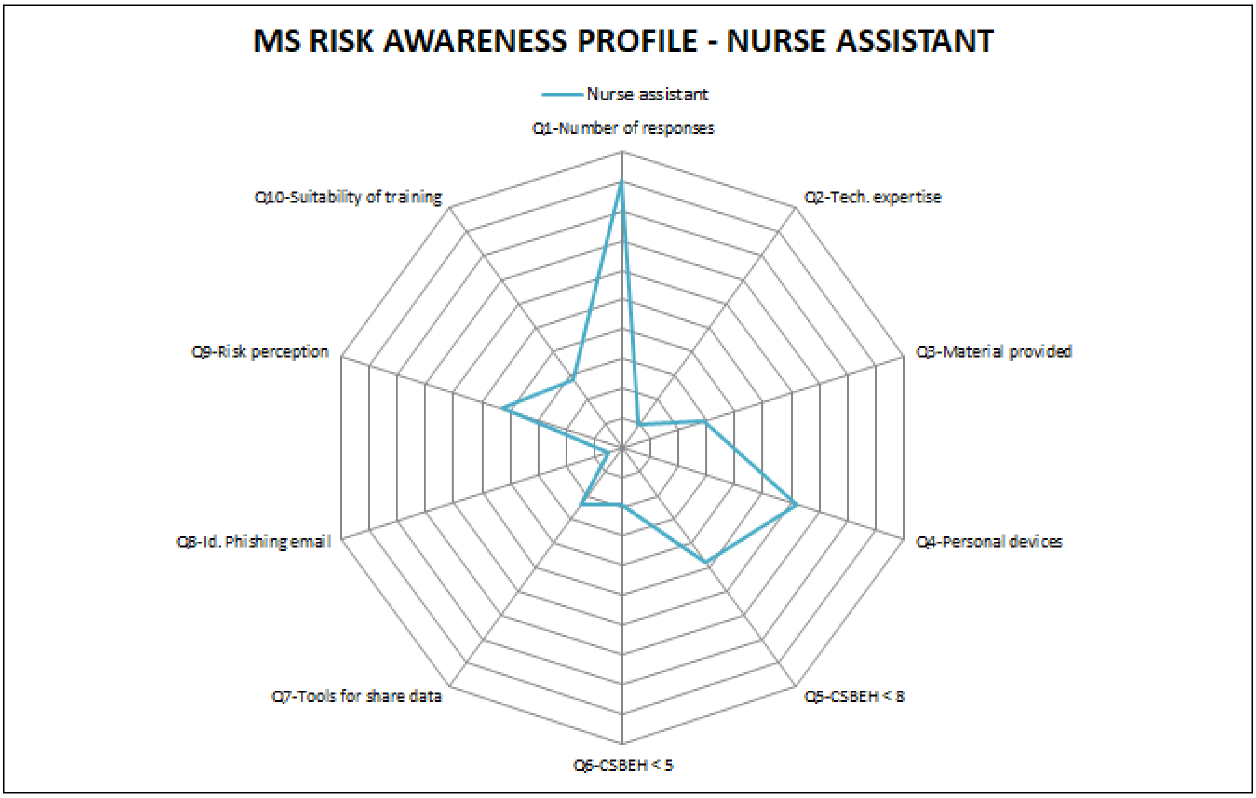


Table 5: MS stratified Risk Awareness Profile results

III.5.2. Conclusions

The detailed responses to the survey in MS have been included in the Appendix II. These details can be useful to explore some concrete detail, as the type of personal devices that users use, the less known type of cyber-attacks, etc.

In this section it has been included a brief conclusion for each domain in the survey, to offer an overview of the main concepts and help to take further decisions about awareness, training and education.

1. **Demographics:**

In Marina Salud the medium and representative user is a Spanish woman between 30 to 50 years old, with university education.

2. **Technological expertise:**

As expected, members of IT department are more experienced in the use of new technologies and about 75% declare themselves as expert users. Approximately 90% of the rest of users declare themselves as intermediate and less than 5% as beginners.

3. **Attitude toward new technologies:**

Again, there is a behavioural difference between IT members and the rest. IT staff is an early adopter while the rest of user types are mostly standard adopters.

4. **Cybersecurity background**

This section shows a clear lack of cybersecurity background, because the organization did not provide specific training and more than 40% of users can't identify any tool provided by the hospital to inform its employees on cybersecurity.

This is an important point to improve.

5. **Cyber attacks' experience**

Less than 10% of the users have not ever been aware to be under a cyber-attack and for those who had, the consequences faced were low grade (80%), if any.

It is needed to focus on the consequences a cyber-attack may have, especially in healthcare sector.

6. Devices used during working activities

The devices used to carry out working activities are mainly corporate devices, but 85% of the users also bring their personal devices to the Hospital and connect them to the Wi-Fi. That is, staff makes wide use of their personal devices in the hospital infrastructures.

7. Awareness Health Belief Model (1)

Users cope with the term cybersecurity and try to perform some actions to avoid risks, but these actions are limited to very basic actions (update antivirus or block pop-ups). They don't know what else to do, nor understand the risks they face.

8. Processing of personal data

The management of personal data (health, economics, identity data) is made from all user segments, mainly through business devices and almost exclusively through business applications.

To that extent, the treatment of sensitive data seems to be correct, but more than 20% of users also share sensitive data through untrusted channels as plain email, whatsapp or external usb devices. This is an important subject to focus on.

9. Awareness Exercises

The passwords strength is not a problem. MS users are able to create quality passwords because they are bounded by the internal password policy to create safe passwords and change them quite often.

10. Awareness Health Belief Model (2)

Most users feel that there is a real risk of receiving emails with virus or to be victim of a cyber-attack. But that is not aligned with the low perception they have than the Hospital can suffer a cyber-attack with serious consequences.

11. Attitude toward possible training course

More than 80% of users agree with the benefits of receiving cyber security training, and to do so both online or classroom training courses would be appreciated.

III.6. Implications and future perspectives

By the intervention made and described in this document, Protego has developed a standard tool that will allow to assess the current level of cyber security awareness of a healthcare organization, based on a few key indicators that are common enough and suitable for use in any Hospital

The results obtained in MS offer some guides that will be followed in the design of the future educational framework:

- It is needed to change the perception users have about of cyber-security: it really matters, it could have serious consequences and is part of the work duties of every Hospital employee.
- The organization has to provide material, adequate and enough, that allow employees to perform the correct cybersecurity behaviours.
- It is needed to emphasize the risks of sharing sensitive data through untrusted tools.
- It is needed to make users understand that some attack vectors could come through their personal devices, or simple actions like clicking a link in an email.

Deeper analysis will be made during the design of the educational framework.

IV. Survey execution in OSR

IV.1. Research Methodology

IV.1.1. Research Questions and Hypothesis

In the attempt to assess employees' cybersecurity awareness and its potential predictors through HBM's constructs, the current study investigated the following research questions and tried to test the subsequent hypotheses. The main hypotheses are related to the plausibility of the model to predict cybersecurity behaviours in the hospital context. The dependent variable and each of the six HBM's constructs with the related hypothesis are consequently defined below.

(a) Research Question 1 (**RQ1**): *Do Health Belief Model's main constructs predict cybersecurity behaviours of HSR' employees?*

- ***Cybersecurity Behaviour*** **(CSBEH)**. It refers to the user's actual response to a recommended computer security behaviour. The higher the number of self-reported cybersecurity behaviours, the higher the level of Information Security Awareness demonstrated by HSR's employees.
- ***Perceived Susceptibility*** **(SUS)**. In this study it refers to the user's belief that a cyber incident will occur. We hypothesize:

  H1**:** *Perceived susceptibility to cybersecurity incidents is positively related to cybersecurity behaviours.*

- ***Perceived Severity*** **(SEV)**. In this study it refers to the seriousness that the user will perceive once a cybersecurity incident has occurred. We hypothesize:

  H2*: Perceived severity of cybersecurity incidents is positively related to cybersecurity behaviours.*

- ***Perceived Benefits*** **(BEN)**. In this study it refers to the advantages or effectiveness that the user perceives in performing cybersecurity behaviours. We hypothesize:

  H3: *Perceived benefits of practicing cybersecurity behaviours are positively related to cybersecurity behaviours.*

- ***Perceived Barriers*** **(BAR)**. In this study it refers to the costs or inconveniences that the user perceives in performing cybersecurity behaviours. We hypothesize:

  H4: *Perceived barriers of practicing cybersecurity behaviours are negatively related to cybersecurity behaviours.*

- ***Self-efficacy*** **(SEF)**. In this study it refers to user's self-confidence in his or her abilities in performing the recommended cybersecurity behaviour. We hypothesize:

  H5: *Self-efficacy related to recommended practices is positively related to cybersecurity behaviours.*

- ***Cues to Action*** **(CUES**). They are the triggers that can motivate or activate the user to perform the recommended behaviour. They might include information security awareness programs as well as media news related to cyberattacks. In this study we will consider the likeliness to act based on HSR's informative material and communications as cues to action. We hypothesise:

  H6*: Cues to action are positively related to cybersecurity behaviour.*

Since the Health Belief Model suggests a moderated relationship between the independent variables and the dependent variable by demographic and socio-psychological factors, we also hypothesise moderated relationships between the six constructs and the target variable “Cybersecurity Behaviour”. In particular, this research will test different moderators to determine the level of impact that each may have on the relationship between the variables SUS, SEV, BEN BAR, SEF and the dependent variable CSBEH. No interaction effects have been hypothesized relatively to CUES; indeed, the original Health Belief Model does not suggest any relationship between other modifying variables (e.g. sociodemographic variables) and Cues to Action (Claar & Johnson, 2011).

In particular, interaction effects for sociodemographic variables (gender, age, educational level, nationality), job-related variables (job functional area, type of data processed, type of devices used during working activities) and technological-related variables (technological expertise, technological attitude, prior experience with cyberattacks) have been examined.

The second research question also aims to overcome the reductionism of theory-verification approach which usually does not consider other relevant factors in assessing Information Security Awareness.

(b) Research Question 2 (**RQ2**): *Do sociodemographic, job-related and technology-related variables have an impact on the relationship between the five HBM’s constructs and the dependent variable “Cybersecurity Behaviour”?*

We hypothesise that sociodemographic variables as well as job-related variables and technological-related variables may moderate the relationship between the independent variables (i.e. HBM’s constructs) and the dependent variable Cybersecurity Behaviour.

The complete research model with the hypothesized interaction effects is thus represented in the following diagram (Figure 4).

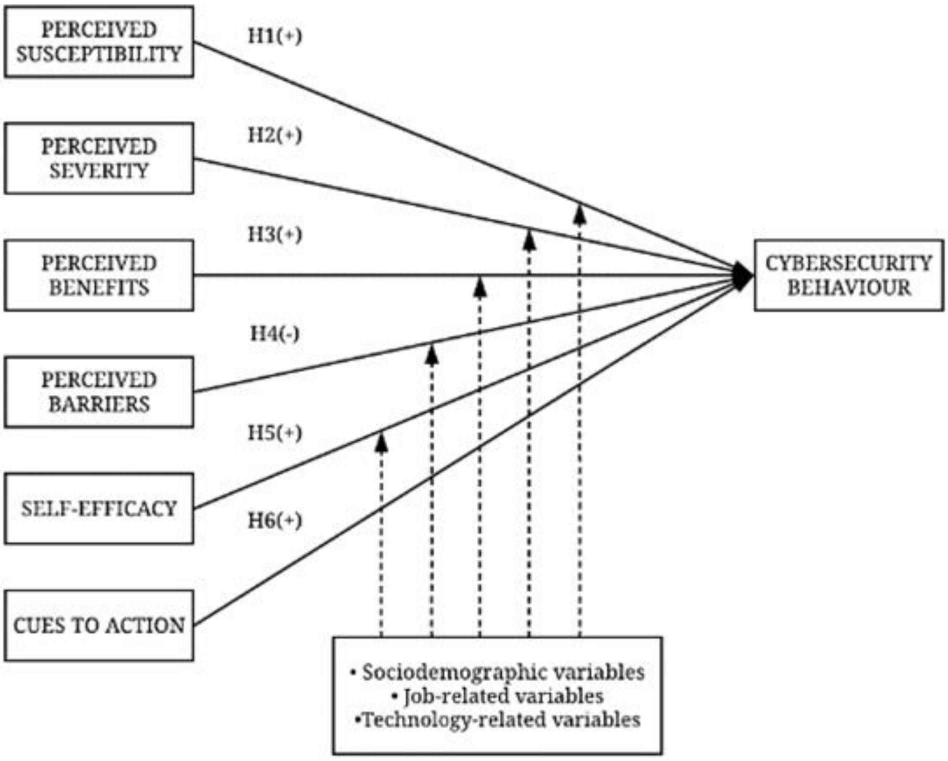


Figure 4: Research Model with hypothesized interaction effects

IV.1.2. Instrument Design

An *ad hoc* online survey was developed. The main objective of the survey was to assess the cybersecurity awareness of HSR's employees in order to better understand the target of the planned future educational training. Indeed, it was necessary to discover which employees are the most exposed to a cybersecurity risk, due to a low level of cybersecurity awareness, also considering other aspects such as the devices they use during their working activities (personal, business, electromedical devices) as well as their access to personal and special categories of data. As previously mentioned, Information Security Awareness has been operationalized in this study in terms of self-reported cybersecurity behaviours[2].

Additionally, the instrument was also designed with the intent of testing the plausibility of the Health Belief Model in predicting hospital employees' cybersecurity behaviours: ISA represents the dependent variable of the research model.

The survey used self-developed questions as well as items from previous research.

In particular, to measure HBM's constructs related to cybersecurity practices a questionnaire used in a study by Anwar et al. (2017) was adapted to the context of the hospital. Since Anwar et al. studied the cybersecurity behaviours of employees coming from different organization, the term "organization" was substituted with the term "hospital" whenever it appeared. In particular, the items related to the core constructs of the model were in their turn taken from Ng et al. (2009), Ifinedo (2012) and Rhee, Kim & Ryu (2009) by Anwar et al. (2017). These references have previously demonstrated good content, construct and content validity of their instruments. However, since the final survey was different from the original instrument, reliability of the items related to the six main independent variables will be checked. Sociodemographic variables as well as job-related and technology-related variables were added in order to gather more information about the subjects and to answer to the second research question. The measures used to assess the primary and secondary outcomes of the research are described in the following sub-sections.

IV.1.3. Primary Measures

The primary measures of the study were constituted by the six main constructs of the Health Belief Model (Perceived Susceptibility, Perceived Severity, Perceived Benefits, Perceived Barriers, Self-Efficacy, Cues to Action) and by the dependent variable Cybersecurity Behaviour (i.e. RQ1).

- The independent variables related to the six main HBM's constructs (**SUS**, **SEV**, **BEN**, **BAR**, **SEF**, **CUES**) were all measured using items on a 7 point-Likert scale ranging from "strongly disagree to" (1) to strongly agree (7) as done in the previous studies from which they were taken (i.e. Ng et al., 2009; Ifinedo, 2012; Rhee et al., 2009). The subjects had to evaluate the items indicating their level of agreement on a numerical scale ranging from 1 to 7. Numerical labels were explained by verbal labels provided into the instruction at the beginning of the survey's section.

  Each construct's measure was given by the average of the items related to each construct, as previously done by Ng et al. (2009).

  Hence, all the main constructs of HBM were measured to be later tested in the data analysis as possible predictors of "Cybersecurity Behaviour" (CSBEH).

[2] Information Security Awareness was also measured through practical exercises that have been proposed in the survey. However, that results will not be taken into consideration in the data analysis

- The dependent variable **CSBEH** intended to give a measure of the level of cybersecurity awareness of HSR's employees. A total of 17 behaviours have been selected from information technology literature (Teymourlouei, 2015; Coventry et al., 2014). In particular, they included both behavioural practices that a user can adopt (e.g. behaviours related to password or software use, etc.) and specific measures that one can apply to protect his/her devices (e.g. antiviruses, firewalls, etc.). A main limitation of previous studies in the field (e.g. Claar & Johnson, 2011; Ng et al., 2009) was the fact that they examined only one cybersecurity practice at a time, with a consequent low generalizability of the results to other cybersecurity behaviours. Considering together different security practices, that HSR's employees may apply, was also intended to overcome this limitation.

  The subjects were asked to select those sentences – among the provided options - that reflected their actual cybersecurity behaviours. Hence, the score of the dependent variable could range from a minimum of 0 (if no options were selected) to a maximum of 17 (if all options were selected).

The following table (Table 6) reports the items related to the primary measures.

Variable	Items (English)	Scale	Reference
SUS	**SUS1**: I feel that my chance of receiving an email attachment with a virus is high. **SUS2**: I feel that I could fall victim to a malicious attack If I failed to comply the regulation for the usage of computing resources. **SUS3**: I feel that an information security breach may occur in the Hospital I work for.	Totally disagree (1) Totally agree (7)	Ng et al., 2009; Ifinedo, 2012
SEV	**SEV1**: It would be a serious problem for me if someone got access to my confidential information without my consent. **SEV2**: It would be a serious problem for me if I lose data resulting from hacking. **SEV3**: It would be a serious problem for me if the health of others were in danger due to a cyberattack.	Totally disagree (1) Totally agree (7)	Ifinedo, 2012; Self-developed (SEV3)
BEN	**BEN1**: I believe that checking the filename of the emails' attachments is useful. **BEN2**: I believe that changing the default privacy and security settings of the website I visit is useful. **BEN3**: I believe that backing up business data on business network drives is useful.	Totally disagree (1) Totally agree (7)	Ng et al., 2009
BAR	**BAR1**: It is inconvenient to check the security of an e-mail with attachments. **BAR2**: It is inconvenient to back up a computer regularly. **BAR3**: It is inconvenient to spend time on cybersecurity training courses.	Totally disagree (1) Totally agree (7)	Ng et al., 2009
SEF	**SEF1**: I have the skills to implement security measures to stop people from getting my confidential information. **SEF2**: I have the skills to handle virus-infected files. **SEF3**: I have the skills to implement security measures to stop people from damaging my computer.	Totally disagree (1) Totally agree (7)	Ifinedo, 2012; Rhee et al., 2009
CUES	**CUES1**: If the Hospital provided me with informative materials about cybersecurity, I would be more conscious of cyber risks.	Totally disagree (1) Totally agree	Ng et al., 2009

	CUES2: If the Hospital's Service Desk sent me warnings or communications on cybersecurity, I would be more conscious of cyber risks.	(7)	
CSBEH	**Cybersecurity Behaviours** I use different passwords for my different accounts I don't install freeware I don't write my passwords on paper supports I don't share my passwords with my colleagues I don't save my passwords on the browser I am using I don't install pirated software I check the security setting of a web site before entering any private information I don't open e-mail attachments from people I do not know I don't use USB keys whose provenance is unknown **Cybersecurity Measures** I manage the privacy settings of web sites I keep the antivirus updated I block the pop-up I backup business data on business network drives I set the web browser to stricter security levels I use a firewall I use filters for e-mail I keep the operating system updated	Minimum Score: 0 Maximum Score: 17	Teymourlouei, 2015; Coventry et al., 2014

Table 6: OSR primary measures

IV.1.4. Secondary Measures

The secondary measures of the study were the hypothesized moderating relationships of relevant variables between the independent variables that will be find significant predictors and the dependent variable (i.e. RQ2). The potential moderators have been chosen both considering those factors that literature has previously shown as implicated in the relationship between HBM’s constructs and cybersecurity behaviours (i.e. theorical approach) and reasoning about the potentially relevant factors that should be considered in the hospital context, after having examined the topic of cybersecurity in healthcare sector.

In particular, the secondary measures have been divided in sociodemographic variables, job-related variables and technological-related variables in the rationale of the questionnaire.

Sociodemographic variables

Sociodemographic variables included gender, age, and educational level. These aspects have been taken into account according to the considerations of Rosenstock (1974) – the HBM’s author - for which the sociodemographic factors can moderate the effects of the model’s constructs on the individual’s behaviour.

In addition, demographic variables have already been found to be predictors of risk perception by Bronfman, Cifuentes, and Gutiérrez (2008), thus resulting relevant to be assessed also when dealing with cyber risks.

- _Gender_. Gender is one of the most fundamental group distinctions and being part of that group can have a large impact on an individual’s attitudes and beliefs (Nosek, Banaji, &

Greenwald, 2002). Thus, considering the role of gender, relatively to cybersecurity beliefs and behaviour, can be relevant. For example, Anwar et al., 2014 found a significant interaction effect of gender and self-efficacy on cybersecurity behaviour. Significant interactions of Gender with SUS, SEV, BEN, BAR and SEF on Cybersecurity Behaviour have been tested.

- *Age*. As gender, age is another fundamental group to which human beings belong to (Nosek et al., 2002). As such, being young or old might have an impact on attitudes and behaviours. In particular, previous research (e.g. Czaja et al., 2006) related to technology has demonstrated that older adults (60-91 years) are generally less likely to use technologies than younger. Hence, we hypothesize significant moderating effects between age and beliefs on cybersecurity behaviour. The subjects will be divided into appropriate age-groups for the analysis.
- *Educational Level*. As a relevant sociodemographic variable, also educational level will be examined as a potential moderator. Claar and Johnson (2011) have already considered the interaction effect of educational level with HBM's constructs in determining cybersecurity behaviour without finding significant effects in a sample of home adopters; however, since the sample characteristics are quite different from this previous study, the relationship will be re-tested. Participants will have to report their educational level at the beginning of the survey choosing among seven educational levels: Primary School, Middle School, High School, Bachelor's Degree, Master Degree, Ph.D/Doctorate, Other.

Job-related variables

The peculiarity of the healthcare sector and, specifically, of the hospital context in dealing with the topic of cybersecurity has clearly emerged from literature. Thus, examining the impact of job-related variables which belongs to this context could be important in the attempt to better understand the characteristics of the sample in order to design more appropriate interventions.

- *Job Functional Area*. Hospitals' employees are commonly divided in four job functional areas: Clinical Area, Research Area, Staff Area and Technical Area. We hypothesize that being part of one or another area might moderate the relationships between the cybersecurity beliefs (i.e. SUS, SEV, BAR, BEN, SEF) and the Cybersecurity Behaviour. The way in which "being a clinician" interacts, for instance, with self-efficacy in determining the cybersecurity behaviour the subject reports to adopt, could be different from the way in which "being a technician" does it.
- *Type of data processed*. Hospitals' employees might process different types of data. According to GDPR (Regulation, 2016) data can be divided into personal data and non-personal data. Among personal data, a particular type of data is represented by special categories of personal data (i.e. ex "sensitive-data"). Specifically, respondents will need to specify if and which kind of data they process during their working activities (only personal data, both personal and sensitive data, neither of the two types of data). Hypothesizing that those who process personal data and special categories of personal data would have different perceptions related to cybersecurity in comparison to those who do not, interaction effects between HBM's constructs and types of data processed on Cybersecurity Behaviour will be tested. For instance, those who process both personal and sensitive data might perceive different levels of perceived severity with consequent different levels of CSBEH.
- *Type of devices used during working*. Hospitals' employees can use different types of devices during their working activities. A main distinction can be drawn between those devices which are provided by the organization (i.e. "business devices") and those which are not (i.e. "personal devices"). Hypothesizing that those employees who use only

business devices could have different perceptions related to cybersecurity behaviour, potential interaction effects between the HBM's beliefs and types of devices used have been considered. For example, the type of devices used during working activities might moderate the relationship with perceived severity in determining cybersecurity behaviour.

- *Electromedical devices that collect patients 'data*. Similarly to what has been hypothesized for the type of data processed and type of devices used during working activities, a distinction between those employees who use electromedical devices that collect patients 'data (i.e. Electronical Health Record systems) and who do not, has been considered. Again, potential interaction effects of this variable with cybersecurity beliefs might lead employees to adopt different cybersecurity behaviours. The decision to monitor this measure in the survey has been suggested from literature review from which it clearly emerged that a main cyber risk in the healthcare sector is represented by the properties of this kind of devices. Respondents will be asked to report whether they use or not these electronical devices which collect patients' data, specifying which particular devices they use.

Technological related-variables

- *Technological expertise.* The hospital's employees might show different levels of technological expertise that could be relevant to be assessed in this kind of study. Indeed, according to Lane & Lyle (2012, p.1) "*the first requirement in order to make informed technology-related decisions (…) is to understand the current levels of technological expertise*". The decision to add a technological expertise measure was given by the idea that different levels of technological expertise might have a different impact on the users' beliefs (i.e. HBM's constructs). Indeed, as supported by literature evidences knowledge by technological experts may reduce the perceived risks, thus influencing computer security behaviours (e.g. in social media use: Garg & Camp, 2015). This can be explained by the fact that, usually, when people believe they are in control of something, their perception of risk is reduced (Adams, 2012). In order to assess technological expertise, a scale which evaluates computer and web-based skills has been selected from literature. In particular, a scale originally developed to assess the technological expertise of a university community (Lane & Lyle, 2011) was used to assess the technological expertise of the HSR's employees. This measure requires the respondents to rate their technological expertise on a scale from 1 to 5. Three points of the scale have been defined by the authors to assist the subjects in their responses, thus employees will be asked to choose the level that better reflect their actual level of technological expertise:
    - *Beginner* - characterised as 1 and 2 on scale - = "f*or example, able to use a mouse and keyboard, create a simple document, send and receive email, and/or access web pages*";
    - *Intermediate* - characterized as 3 on scale - = "*for example, able to format documents using styles or templates, use spreadsheets for custom calculations and charts, and/or use graphics/ web publishing software*";
    - *Expert* - characterized as 4 and 5 on scale - = "*for example, able to use macros in programs to speed tasks, configure operating system features, create a program using a programming language, and/or develop a database*".
    - *Attitude toward new technology*. The choice of considering attitude toward new technology as a potential moderating variable came from the considerations related to the affect heuristic, for which, the more technologies (or activities) are associated with positive feelings, the less they are judged to be risky and the more they are judged to be beneficial (Finucane, Alhakami, Slovic, & Johnson, 2000).

Hypothesizing that attitude towards new technologies can thus show a moderating effect on hospitals' cybersecurity beliefs (e.g. perceived benefits, perceived barriers, etc.) a measure was selected from previous literature. In particular, a scale adapting the Technology Adoption Life Cycle (Rogers, 1995) has been chosen. This sociological model has been used to describe the acceptance of a new product or innovation since '50s. In particular, according to this model an individual can recognize him or herself as a "Innovator", as a "*Early Adopter*", as part of "*Early Majority*", as part of "*Late Majority*" or as a "*Laggard*" relatively to a technology. These labels have initially been provided by Beal and Bohlen (1956) in the agricultural context to describe the different attitudes of farmers in accepting innovative instruments for their work. In the survey, HSR's employees will be asked to choose among five definitions of an ordinal scale that have already been applied to operationalise the above-mentioned different profiles (e.g. In: Lane & Lyle, 2012):

- "I am the kind of person that is always looking for new products/ technology even before it becomes available on the market" (i.e. Innovator)
- "I am the kind of person that tend to adopt the latest technologies as soon as they become available on the market" (i.e. Early Adopter)
- "I am the kind of person that tend to buy new products/technology when it is widespread" (i.e. Early Majority)
- "I am the kind of person that tend to buy new products/technology when it becomes mainstream" (i.e. Late Majority)
- "I am the kind of person that tend not to adopt new products/technologies" (i.e. Laggard)
- Cyberattacks' experience. The last technology-related secondary measure regards the prior experience with cyberattacks. In particular, hospital's employees will be asked to report if they have ever noticed to be under a cyber-attack.

We decided to consider this measure because hypothesizing that a prior experience with cyberattacks might change users' beliefs about cybersecurity; for instance, users who had this experience might perceive more susceptibility to a new attack with consequent different cybersecurity behaviours. This idea was also supported by literature evidence. Indeed, Claar and Johnson (2011) – who considered this parameter in a previous similar study in which they applied the HBM to examine the cybersecurity behaviour of home users – found significant moderating effects of this measure on self-efficacy and perceived severity.

IV.1.5. Validation of the instrument

Instrument validation consisted in assessing content validity of the survey. In particular, the content validity related to the HBM's constructs was guaranteed, as previously specified, by drawing representative questions from a previous study (i.e. Anwar et al., 2017) that used the Health Belief Model to study cybersecurity behaviours of different organizations' employees. Additionally, pre-tests of the complete instrument were conducted by administering the survey to the employees of the Center for Advanced Technology in Health and Wellbeing of I.R.C.S.S. San Raffaele and interviewing experts in this field (i.e. Information Systems Directorate -DSI - and computer engineers).

Hence, the items of the survey were redefined based on the feedbacks gathered from these pre-tests. In particular, the number of items for each construct was reduced. Indeed, given the presence of many additional information that the survey needed to take into account due to project ProTego's objectives, the original questionnaire by Anwar et al. (2017) resulted too long with a consistent risk of survey drop outs. A total of 17 items – anchored on 7-point Likert scales - have been consequently chosen to reflect the six main constructs of the Health Belief Model. Also, the technological expertise measure (Lane & Lyle, 2011) was reduced from 5 to 3 levels; in particular, the three main definitions provided by the authors to help the users in their responses will be considered as the three levels of an ordinal scale on which the employees will rate their technological expertise level. Indeed, the fact that only three descriptions were provided by the authors to define five levels of the scale was judged confusing by a large part of the subjects in the pre-test.

The final version of the questionnaire (in English) has been reported in Appendix1.

IV.2. Inclusion/Exclusion criteria

The population of interest was composed by HSR's employees, which have been divided by considering their four main Job Functional Areas (i.e. Clinical Area, Research Area, Staff Area, Technical Area). Only HSR's employees with the institutional e-mail account with a "@hsr.it" e-mail's domain were taken into consideration for the survey's administration. Only one inclusion criterion has been considered, that is being an employee of San Raffaele Hospital who uses the organization's Wi-Fi or the LAN connection provided by HSR during working activities (i.e. "OSR Personal"). This criterion, after the privacy policy acceptance, was checked with the first question of the survey.

IV.3. Procedure

The study took place at IRCSS San Raffaele Hospital (Milan, Italy), using a convenience sample. The survey was created and distributed in Italian using Qualtrics, a subscription software which allows to collect and analyse data for different objectives (Qualtrics, 2019).

The data collection started on 10th of June 2019 and was closed on 25th of June 2019. An e-mail containing the study's presentation with the anonymous link to access the survey was sent to all HSR's employees via the official e-mail of HSR's moderated lists ("Liste Moderate OSR"). The e-mail explained the topic of the project and underlined that the gathered data were anonymous and used only for research aims. All the answers were made compulsory so that all the gathered responses would be complete.

IV.4. Data analysis

All the data were analysed using IBM SPSS Statistics (Version 25).

First of all, we will provide the Mean and Standard deviation for the variable *Age* and will run the frequency's analyses of all the categorical variables of the sample – divided for the Job Functional Area reported by the employees (i.e. Clinical Area, Research Area, Staff Area, Technical Area) - that were *Gender* (Male, Female, Not-Specified), *Nationality* (Italian, Other), *Educational level* (Primary school, Middle school, High school, Bachelor's degree, Master's degree, Ph.D./doctorate, Other), *Technological expertise* (Beginner, Intermediate, Expert), *Attitude toward new technology* (Innovator, Early adopter, Early majority, Late majority, Laggard) *Cyberattacks' experience* (Yes/No), *Processing of data* (Yes, only personal data, Yes, both personal and special categories of data, No, neither of the two), *Devices used during working activities* (Mainly personal devices, Mainly business devices, Both, None of them), *Use of* *electromedical devices that collect patients' data* (Yes, No), *Attitudes toward a possible training* (Yes, No, I don't know, It depends).

Then, to test the hypothesis that the mean scores of the different groups of the categorical variables *Gender*, *Age* (24 – 38 years, 39-52 years, 53 – 66 years), *Educational level*, *Job Functional Area*, *Technological expertise*, *Attitude toward new technology*, *Cyberattacks' experience*, *Processing of data*, *Devices used during working activities*, *Use of electromedical devices that collect patients' data* were statistically different relatively to the variable Cybersecurity Behaviour, several Kruskall-Wallis Tests and Mann-Whitney Tests were run. The decision to adopt these parametric tests was due to the fact that a prior Kolmogorov-Smirnov Normality Test (K-S Test) – that will be reported - showed that the variable CSBEH was not normally distributed.

Finally, the main hypotheses related to the first and second research question will be tested using firstly multiple regression (RQ1) and secondly using an interaction effect analysis (RQ2).

IV.5. Global sample description

IV.5.1. Descriptive statistics

A total of **217 answers have been collected**, however, 56 subjects have been excluded because they did not satisfy the inclusion criteria. Consequently, a total of **161 responses** have been considered valid for the data analysis.

The sample consisted in 72 employees from Clinical Area, 58 employees from Research Area, 21 employees from Staff Area and 10 employees from Technical Area.

The following table (Table 7) shows the demographics and the main characteristics of the respondents subdivided for the Job Functional Area (i.e. Clinical Area, Research Area, Staff Area, Technical Area) that they reported belonging to. As it can be observed the sample consisted largely of Italian females with master's degree, form the above-mentioned Clinical Area. Most of respondents reported no prior experience to cyberattacks and medium level of technological expertise and attitude towards technology. The 82,6% showed an interest in a possible cybersecurity training.

	Clinical Area (N=72)	**Research Area** (N=58)	**Staff Area** (N=21)	**Technical Area** (N=10)
Age (Min = 24; Max = 66) M = 43.58 (Sd = 11.743)	46.68 (11.82)	38.88 (10.75)	42.33 (11.58)	51.10 (5.76)
Gender				
Male	25 (34.7%)	14 (24.1%)	11 (52.4%)	7 (70.0%)
Female	46 (63.9%)	42 (72.4%)	9 (42.9.%)	3 (30.0%)
Not-Specified	1 (1.4%)	2 (3.4%)	1 (4.8%)	
Nationality				
Italian	71 (98.6%)	55 (94.8%)	20 (95.2%)	10 (100.0%)

Other	1 (1.4%)	3 (5.2 %)	1 (4.8%)	-
Educational level				
Primary school	-	-	-	-
Middle school	3 (4.2%)	-	1 (4.8%)	-
High school	15 (20.8%	4 (6.9%)	2 (9.5%)	4 (40.0%)
Bachelor’s degree	14 (19.4%)	6 (10.3%)	3 (14.3%)	2 (20.0%)
Master’s degree	25 (34.7%)	20 (34.5%)	11 (52.4%)	4 (40.0%)
Ph.D./doctorate	3 (4.2%)	25 (43.1%)	2 (9.5%)	-
Other	12 (16.7%)	3 (5.2%)	2 (9.5%)	-
Technological expertise				
Beginner	22 (30.6%)	3 (5.2%)	-	1 (10.0%)
Intermediate	48 (66.7%)	39 (67.2%)	14 (66.7%)	5 (50.0%)
Expert	2 (2.8%)	16 (27.6%)	7 (33.3%)	4 (40.0%)
Attitude toward new technology				
Innovator	1 (1.4%)	2 (3.4%)	2 (9.5%)	1 (10.0%)
Early adopter	11 (15.3%)	8 (13.8%)	4 (19.0%)	1 (10.0%)
Early majority	30 (41.7%)	29 (50.0%)	9 (42.9%)	7 (70.0%)
Late majority	21 (29.2%)	17 (29.3%)	5 (23.8%)	1 (10.0%)
Laggard	9 (12.5%)	2 (3.4%)	1 (4.8%)	-
Cyberattacks’ experience				
Yes	30 (41.7%)	24 (41.4%)	11 (52.4%)	6 (60.0%)
No	42 (58.3%)	34 (58.6%)	10 (47.6%)	4 (40.0%)
Devices used during working activities				
Mainly personal devices	3 (4.2%)	10 (17.2%)	1 (4.8%)	-
Mainly business devices	36 (50.0%)	23 (39.7%)	15(71.4.%)	6 (60.0%)
Both	33 (45.8%)	25 (43.1%)	5 (23.8%)	4 (40.0%)
None of them	-	-	-	-
Use of electromedical devices that collect patients’ data				
Yes	25 (34.7.%)	3 (5.2%)	1 (4.8%)	1 (10.0%)
No	47 (65.3%)	55 (94.8%)	20 (95.2%)	9 (90.0%)
Processing of data				
Yes, only personal data	7 (9.7%)	13 (22.4%)	8 (38.1%)	3 (30.0%)
Yes, both personal and special categories of data	62 (86.1%)	16 (27.6%)	12 (57.1%)	5 (50.0%)
No, neither of the two	3 (4.2%)	29 (50.0%)	1 (4.8%)	2 (20.0%)
Attitudes toward				

a possible training				
Yes	62 (86.1%)	48 (82.8%)	15 (71.4%)	8 (80.0%)
No	.	1 (1.7%)	1 (4.8%)	-
I don't know	4 (5.6%)	4 (6.9%)	2 (9.5%)	1 (10.0%)
It depends	6 (8.3%)	5 (8.6%)	3 (14.3%)	1 (10.0%)

Table 7: Main characteristics of the participants by Job Functional Area

Cybersecurity Behaviour (CSBEH)	**N**	**Mean**	**Standard Deviation**
Gender			
Male	57	9,45	3,49
Female	100	9,01	3,23
Age			
24 – 38 years	60	8,84	3,10
39 – 52 years	55	9,34	3,73
53 – 66 years	46	9,43	3,07
Educational level			
Primary school	-	-	-
Middle school	4	8,25	3,59
High school	25	8,68	3,97
Bachelor's degree	25	9,00	2,72
Master's degree	60	8,76	3,32
Ph.D./doctorate	30	10,71	2,84
Technological expertise			
Beginner	26	7,95	2,70
Intermediate	106	9,01	3,19
Expert	29	10,73	3,76
Attitude toward new technology			
Innovator			
Early adopter	6	11,40	2,07
Early majority	24	10,16	3,27
Late majority	75	9,68	3,23
Laggard	44	7,78	3,35
	12	7,73	2,57
Cyberattacks' experience			

Yes	71	9,38	3,34
No	90	9,00	3,31
Devices used during working activities			
Both personal and business	81	9,37	3,49
Mainly business	80	8,96	3,15
Processing of data			
Yes, only personal data	31	9,36	2,72
Yes, both personal and special categories of data	95	8,64	3,42
No, neither of the two	35	10,31	3,31
Use of electromedical devices that collect patients' data			
Yes			
No	30	8,37	3,13
	131	9,35	3,35

Table 8: Mean Scores and St. Deviations of CSBEH

IV.5.2. Non parametric tests

Preliminary analyses were run to check whether there were any significant differences between the dependent variable ("Cybersecurity Behaviour") and the characteristics of the sample (Gender, Educational Level, Job Functional Area, Technological Expertise, Attitude towards new technology, Cyberattacks' Experience, Processing of data, Type of devices used during working activities, Use of electronical medical devices that collect patients' data) that will be later tested as potential moderating variables.

Because Kolmogorov-Smirnov (p value = .006 < .05) showed that the main variable Cybersecurity Behaviour (i.e. "CSBEH") was not normally distributed, non-parametric tests were performed.

Gender and CSBEH

A Mann-Whitney Test has been conducted to test whether there was a significant difference in cybersecurity behaviour levels across gender. Those subjects who did not want to specify the gender were considered as missing values (N = 4) for this analysis. The U test was 2.486 with a p value = .182 (< .05). Thus, a not significant difference in cybersecurity behaviour scores of males and females has been found.

Age and CSBEH

A Kruskall-Wallis Test has been conducted to test whether there was a significant difference in cybersecurity behaviour levels across three different age subgroups (24 – 38 years, 39-52 years, 53 – 66 years). Subgroups cut-points were decided using the Visual Binning module of SPSS. The H test value was 3,159 with a p value = .206 (> .05). Thus, a not significant difference in cybersecurity behaviour scores across the three age groups has been found.

Educational level and CSBEH

A Kruskall-Wallis Test has been conducted to test whether there was a significant difference in the cybersecurity behaviour scores across different educational levels. Since the H test value was 10.152 with a p value = .071 (> .05) , again, no significant differences have been found.

Job Functional Area and CSBEH

A Kruskall-Wallis Test has been conducted to test whether there was a significant difference in cybersecurity behavior levels across the four job functional areas in which employees have been divided. It revealed a significant difference: H value was 11.169 with a p value = .011 (< .05). In particular, Pairwise Comparisons showed that the difference between Clinical Area employees and Research Area employees was not significant (Adj.p value = .645 > .05) as well as the difference between Clinical Area and Staff Area (Adj.p value = 1.000 >.05), the difference between Research Area and Staff Area (Adj.p value = 1.000 > .05), the difference between Research Area and Technical Area (Adj.p value = .121 > .05) and the difference between Staff Area and Technical Area (Adj.p value = .231> 0.5).

The *only significant difference was the one between Clinical and Technical Area* (Adj.p value = 0.008 < .05).

Technological Expertise and CSBEH

A Kruskall-Wallis Test has been conducted to test whether there was a significant difference in the cybersecurity behaviour scores across different levels of technological expertise. A significant difference was observed: H test = 8.550 with a p value: = .014 (< 0.05). In particular, the difference between Beginners and Intermediates was found not significant (Adj. p value = .522 > .05) as well as the difference between Intermediates and Experts (Adj p.value = .073 > .05).

The *only significant difference was the one between Beginners and Experts* (Adj.p value = 0.013 < .05).

Attitude toward new technology and CSBEH

A Kruskall-Wallis Test has been conducted to test whether there was a significant difference in the cybersecurity behaviour scores across different levels of attitude toward new technology. In general, a significant difference was observed: H test = 12.459, with a p value = .014 (< 0.05).

However, at first glance, Pairwise Comparisons did not seem to show significant differences between each level of the two variables. This effect was explained taking into account that the Bonferroni correction used by the software for the *post-hoc* analysis, is a very conservative method, especially with variables with more than three levels as in this case (Bonferroni, 1936). Applying a less stringent criterion (Adj significance < .150) *the most evident subgroup difference was the one between Early Adopters and Late Majority subjects* (Adj. p value = .115).

Cyberattacks' experience and CSBEH

A Mann-Whitney Test has been conducted to test whether there was a significant difference in cybersecurity behaviour levels relatively the to the previous experience with cyberattacks. However, no significant difference has been found (H test = 3.011; p value = .529 > .05).

Processing of data and CSBEH

A Kruskall-Wallis Test has been conducted to test whether there was a significant difference in the cybersecurity behaviour levels relatively to the type of data (personal/sensitive/none) that employees process. In general, a significant difference was observed: H test = 6.730 with a p value = .035 (< 0.05). In particular, the difference between those who process both personal and sensitive data and those who process only personal data was not significant (Adj.p value = .965 > .05) as well as the difference between those who process only personal data or do not process neither of the two kinds of data (Adj. p value = .655 >.05).

The *only significant difference was the one between those employees who process both personal and sensitive data and those who not process neither or the two kinds of data* (Adj. p value: .030 < .05).

Types of devices used during working activities and CSBEH

A Mann-Whitney Test has been conducted to test whether there was a significant difference in the cybersecurity behaviour levels relatively to the type of devices that employees use during their working activities. Considering a new recoded variable for which employees were divided in those who use only organizational devices versus who use mostly personal devices or both types of devices. However, no significant difference has been found: U test = 2.954, with a p value = .331 > .05).

Electromedical devices that collect patients' data and CSBEH

A Mann-Whitney Test has been conducted to test whether there was a significant difference in the cybersecurity behaviour levels between those employees who use electronical medical devices that collect patients' data versus those who do not. However, no significant difference has been found (U test = 2.206 with a p value = .292 > .05).

To sum up, significant differences in *the cybersecurity behaviour levels have been found across different job functional areas, across different levels of technological expertise and attitude towards new technology and relatively to the type of data processed during working activities* by HSR's employees.

IV.5.3. Hypotheses Testing

(RQ1) Can HBM's constructs predict jointly Information Security Awareness operationalized in terms of Cybersecurity Behaviour?

(RQ2) Do these dimensions contribute significantly to prediction of CSBEH? Do sociodemographic, as well as job-related and technology-related variable have an impact on the relationship between the individual's beliefs and the cybersecurity behaviour?

Firstly, to test this set of hypotheses, a multiple regression and a moderation analysis were run to test whether the six main HBM's construct and the potential interaction effects of moderating variables could successfully predict ratings of Cybersecurity Behaviour (CSBEH). Successively, a Hierarchical Regression Analysis was carried out to synthetize the total variance explained by the final research model.

IV.5.3.a. Multiple regression: HBM's predicting Cybersecurity behaviour

A multiple linear regression was run to predict Cybersecurity Behaviour (CSBEH) based on Perceived Susceptibility (SUS), Perceived Severity (SEV), Perceived Benefits (BEN), Perceived Barriers (BAR), Self-Efficacy (SEF) and Cues to Action (CUES). Thus, the regression was conducted using the six constructs (SUS, SEV, BEN, BAR, SEF, CUES) as independent variables and the variable "Cybersecurity Behaviour" as dependent variable (i.e. CSBEH).

In particular, since no *a priori* hypotheses had been made to determine the order of entry of the predictor variables, a direct method (i.e. Enter Method) was used; thus, all of the predictor variables have been entered together.

A significant regression equation was found [F change (6, 154) = 7,655, p < .000, R = .479, R^2 = .230, Adj R^2 = .200].

In the model, the six hypotheses related to the first research question were examined:

- H1, which predicted that Perceived Susceptibility (SUS) would be positively related to Cybersecurity Behaviour was not supported (β = 0,021, p > .700 n.s.);
- H2, which predicted that Perceived Severity (SEV) would be positively related to Cybersecurity Behaviour was supported (β = 0,250, p <.020);
- H3, which predicted that Perceived Benefits (BEN) would be positively related to Cybersecurity Behaviour was not supported (β = - 0,004, p > .900 n.s.);
- H4 which predicted that Perceived Barriers (BAR) would be negatively related to Cybersecurity Behaviour was supported (β = - 0,215, p <.005);
- H5 which predicted that Self-Efficacy (SEF) would be positively related to Cybersecurity Behaviour was supported (β = 0,307, p < .001);
- H6 which predicted that Cues to Action (CUES) would be positively related to Cybersecurity Behaviour was partially supported. Indeed, CUES demonstrated an to be negatively related to the dependent variable (β = - 0,239, p < .004).

Thus, we can state that the independent variables SEV, BAR, SEF and CUES were significant predictors, while the independent variables SUS and BEN were not.

The following table shows the results of the multiple regression analysis (see Table 9).

Model	Coefficient	St. Error	Standardized Coefficient (β)	Sig.
(Constant)	5,58	1,87		,003
SUS	,057	0,21	,021	,787
SEV	,784	0,31	,250	,013
BEN	-,010	0,30	-,004	,972
BAR	-,449	0,15	-,215	,004
SEF	,691	0,16	,307	,000
CUES	-,565	0,19	-,239	,003

Table 9: Multiple Regression Analysis Coefficients

Hence, considering only significant predictors, HSR employees' predicted CSBEH is equal to 5,580 + 0,784 (SEV) – 0,449 (BAR) + 0,691 (SEF) – 0,565 (CUES), where all the independent variables were measured on a scale ranging from 1 to 7 Likert-points.

IV.5.3.b. Moderation Analysis: interaction effects of sociodemographic, job-related and technology related factors

A moderation analysis was conducted to test the hypotheses that sociodemographic variables as well as job-related and technology-related variables might moderate the relationships between the independent variables (i.e. HBM's constructs) and the dependent variable Cybersecurity Behaviour.

The hypothesized interaction effects were studied only among those predictors resulted significant in the multiple regression analysis (i.e. SEV, BAR, SEV) in order to check whether it was possible to better explain the cybersecurity behaviour.

Hence, the interactions of these three main constructs by sociodemographic variables (i.e. gender, educational level, age groups) job-related variables (job functional area, types of devices used during working activities, use of electromedical devices that collect patients' data, processing of data) and technological-related variables (technological expertise, attitude toward new technology, cyberattacks' experience) on CSBEH have been studied through a moderation analysis with GZLM module of SPSS and further explored applying PROCESS v3.3 by Hayes (Hayes, 2017).

In particular, the variables "Technological Expertise", "Devices used during working activities" and "Processing of data" were treated as dichotomic for this analysis, thus considering three new recoded variables for which employees were divided in experts *versus* non-expert (which merged together both "Beginners" and "Intermediates") – for the first variable, in those who use only organizational devices *versus* who use mostly personal devices - for the second variable – and in those who process personal data (which merged together those who process personal data and those who also process special categories of data) *versus* those do not process any kind of personal data – for the third variable.

The main effects of two independent variables (a construct and a potential moderator) and the interaction between the two has been tested in each regression. In particular, CSBEH always inserted as dependent variable, while the independent variables were one significant construct of the HBM and one of the above-mentioned categorical variables.

Using GZLM module allows to simply use categorical variables (dichotomic and multilevel) in the analysis, which end up being dummy coded in the program when it runs. Also PROCESS v3.3 allows to specify if the variable inserted as potential moderator (W) is multi-categorical or not. This condition has been introduced for all non-dichotomic potential moderating variables (i.e Age-group, Educational Level, Job Functional Area and Attitude Toward New Technology). Thus, no dummy variables have been created.

All the interaction terms for BAR were not significant, as well as most of the interactions for SEV and SEF. Only two significant interactions were found; those between SEV and Technological Expertise and SEF and Use of electromedical devices that collect patients' data on the dependent variable CSBEH.

IV.6. Discussion

Relatively to the main constructs of the Health Belief Model, results showed that Perceived Severity, Perceived Barriers, Self-Efficacy and Cues to Action are determinants of a user's Cybersecurity Behaviour, which in this study operationalized the complex concept of Information Security Awareness.

In particular, *Self-Efficacy resulted the strongest predictor*, thus suggesting that being confident in own abilities to apply the necessary cybersecurity measures becomes extremely relevant to comply with cybersecurity advice. This study's finding is in line with a meta-analysis which examined the prediction of health behaviour which showed that self-efficacy is most strongly related to intention and behaviour (Milne, Sheeran, & Orbell, 2000) However, since the mean scores related to self-efficacy were the lowest compared to the other constructs (with the exception of Perceived Barriers that were already supposed to be low), **it is recommendable for the hospital to focus on this component in order to increase cybersecurity behaviour of HSR's employees**.

Also the construct of *Perceived Barriers resulted a significant predictor of CSBEH*; in particular Perceived Barriers showed a negative relationship with Cybersecurity Behaviour. Thus, we can argue that employees who do not encounter many barriers in applying cybersecurity measures are more likely to engage in correct cybersecurity practices. Even though the respondents also reported many Perceived Benefits (as observable looking at the mean scores) this construct did not result as a significant predictor thus letting us to assume that having low perceived barriers outweigh in importance the fact of having high benefits in determining cybersecurity behaviour. Hence, **a possible implication from which San Raffaele Hospital's DSI could take advantage from could be seeking to maintain barriers low, also instead of seeking to make perceived benefits higher**.

The results also inverted the direction of the hypothesis related to the variable *Cues to Action*, which *showed a negative instead of a positive relationship with cybersecurity behaviour*. In particular, Cues to Action were operationalized in this study as **the potential efforts of San Raffaele Hospital and Hospital's Service Desk to inform the employees about the cyber risks via warnings and communications** (i.e. Items: CUES1: "*If the Hospital provided me with informative materials about cybersecurity, I would be more conscious of cyber risks*"; CUES2: "*If the Hospital's Service Desk sent me warnings or communications on cybersecurity, I would be more conscious of cyber risks*"). Lower scores of Cues to Action corresponded to higher level of Cybersecurity Behaviour, and *vice versa*. This result shows that the employees whose risk perception would not be influenced by HSR's warnings are the ones who already adopt the correct cybersecurity measures, while those who do not engage in these behaviours are those that declare that would be influenced by this type of communication. Hence, providing this type of messages could positively influence those who reported the lowest number of cybersecurity behaviours. In particular, observing the mean scores of CSBEH divided by Job Functional Area, we might hypothesize that the most receptive target of these advice would correspond Clinical Area's employees. Additionally, because the β scores of SEF were higher than the β scores of CUES we could also conclude that the internal component (i.e. Self-Efficacy) plays a more important role compared to the external stimuli from environment (i.e. Cues to Action) when dealing with cybersecurity behaviour. Of course, since the CUES were measured considering only two items that were mostly related to informative or warning material, this conclusion does not regard other possible forms of cues to action (e.g. news of cyberattacks occurred in other hospitals, etc.) that have not been considered in the present study. Indeed, respondents might also have been focused more on the possibility to receive material than on the likeliness of being alarmed by the risks that this communication could vehiculate.

Multiple regression analysis also showed that *Perceived Susceptibility was not a significant predictor of CSBEH*; this could be explained if we consider that HSR's employees might not be fully aware of the likelihood of cyberattacks in the hospital context, thus SUS is not a decisive factor in their cybersecurity behaviour. If that is the case, this result would emphasize **the necessity to develop security awareness programs aimed at warning HSR's employees against the actual risks of cyberattacks related to their work-place**. This result was consistent with Carpenter's metanalysis (2010), which estimated the effect of each construct of the HBM on health behaviour outcomes, finding that the susceptibility beliefs estimates were predicted to be near to zero for both prevention and treatment behaviours. However, the already-mentioned studies which applied the Health Belief Model in the context of cybersecurity (Claar & Johnson, 2011; Ng et al., 2009) showed an opposite pattern that we tried to understand. In particular, both the analysis of Claar and Johnson (2011) - which examined the behaviour of home-adopters - and the analysis of Ng et al. (2009) - which explored the cybersecurity behaviour of employees from different types of organizations - found that Perceived Susceptibility was one of the strongest predictors in determining cybersecurity behaviour. Since the main difference between these and our study was related to the different context of application, we imagine that this dissimilar result might be determined right from the peculiarity of the hospital context. This would also be in line with the previous explanation for which HSR's employees do not imagine that cyberattacks might occur at their work place, thus not considering themselves as a possible target of this kind of incidents.

Differently, *Perceived Severity resulted to be a significant predictor of CSBEH*, which means that HSR's employees judgment related to the severity of an eventual cyberattack is determinant in their behaviour. In particular, the higher the scores in perceived severity, the higher the level of cybersecurity behaviour that they exhibit. From this perspective, it becomes important not only to inform about the likelihood of cyberattacks to occur, but especially to highlight the consequences that a cyberattack might bring into this context. Thus, **a communication more oriented to the effects of the cyberattacks might be more effective in influencing employees' security behaviours**.

Finally, of the ten hypothesized moderating variables (Gender, Age, Educational Level, Job functional area, Technological expertise, Attitude toward new technology, Cyberattacks' experience, Processing of data, Devices used during working activities, Use of Electromedical devices which collect patients' data) only two showed significant moderating effects with the HBM's constructs on the dependent variable.

In particular, *the first significant interaction effect was the one of Perceived Severity and Technological Expertise on CSBEH*. This result suggested that being expert could strengthen the direct relationship between SEV and CSBEH (even if the same trend is observable also in non-experts); we could explain this outcome assuming that for the experts, perceiving more severity has a more important role in determining their cybersecurity behaviour. However, we also noticed that who reported to be "Expert" but showed lower levels of Perceived Severity exhibited the lowest level of Cybersecurity Behaviour. Thus, **we can affirm that even when individuals consider themselves as expert in technology, they are not always free from the risk of not applying the correct cybersecurity behaviours; in particular, a low severity perception related to cyberattacks seems to lead to non-adoption of security measures**. The fact that at lower scores of Perceived Severity non-experts reached higher levels of CSBEH compared to experts (who report the same low scores of SEV) could be motivated by the fact that non-expert tend to follow default cybersecurity measures – maybe suggested by others – while experts consciously choose to not apply some measures due to an underestimation of the risks of cyberattacks (i.e. low perceived severity).

Lastly, *the interaction effect of Self-Efficacy and Use of Electromedical Devices which collect patients' data was significant on CSBEH*, showing that not using Electromedical Devices seem to strengthen the relationship between SEF and CSBEH. The most curious aspect regards the part of the sample which reported to use this type of devices; indeed, the higher levels of Self-Efficacy have been expressed by those who reached the lower scores in CSBEH. In the attempt to explain this result, one may suppose an overconfidence or control bias associated with the use of these devices. Further research is needed to explore this hypothesis in order to understand whether and why the Self-Efficacy perceptions related to cybersecurity behaviour are distorted when using these instruments. Of course, this evidence arises a central risk; it indicates that those who use these devices – which collect sensitive information – might not be able to accurately evaluate their actual cybersecurity skills. Thus, **HSR interventions could be oriented, on one hand, to increase the self-efficacy of employees who do not use electromedical devices which collect patients' data, on the other hand to monitor and – if necessary – to settle the levels of self-efficacy of those who manage these devices.**

Because the survey was also designed to better understand the target of the future educational framework aimed at increasing cybersecurity awareness -- considering the objectives of the project ProTego – few words will be also spent about the impressions related to the Information Security Awareness level of the sample that have been analysed through the non-parametric tests.

The sample generally showed a medium level of CSBEH; in particular, *the significant differences in the mean scores of cybersecurity behaviours were noticed across the different Job Functional Areas in which employees reported to work*, across different *levels of Technological Expertise and of Attitude towards new technology, and finally relatively to the Type of data processed during working activities* (personal data, special categories of data, no neither of the two). In particular, the lowest mean scores were observed in those from Clinical Area, those who reported to be "Beginners" relatively to their technological expertise and to be "Laggards" relatively to their attitude toward new technology, and those who process both personal and special categories of data. Especially the latter result suggests that **San Raffaele Hospital should put more attention to train employees who process this information in order to prevent the risks of potential cyberattacks** (See Table 8 for the mean scores and st. deviations of cybersecurity behaviour divided by the characteristics of the sample).

IV.7. Conclusions

The findings of the research provide empirical evidence that the main constructs of the Health Belief Model can effectively be used to study cybersecurity behaviours; from this perspective, a Health Communication model reveals to be a valuable instrument in the context of public security.

Even if this conclusion has already been demonstrated by previous studies, our research tried to control and to overcome two main limitations of the latter. Firstly, the use of large and undefined samples (e.g. Claar & Johnson, 2011) that limited the practical applications of previous research due to validity issues. Secondly, the fact of measuring only one cybersecurity practice at a time (as done for instance by Claar & Johnson, 2011 and Ng et al., 2007), instead of observing different cybersecurity behaviours as we did. Indeed, even if one hand this choice could give raise to multidimensionality issues that should be checked, on the other hand it offers the possibility to generalize the results to other information security practices.

Furthermore, the present work allowed ProTego to use a theory-based survey, whose results provided some suggestions that could be followed as guidelines in designing the educational framework aimed at increasing the cybersecurity awareness of HSR's employees. In particular, since the results showed that the largest contributor of Cybersecurity Behaviour is Self-Efficacy in own's abilities to engage in the suggested behaviour, an educational intervention might should try to increase the sense of self-efficacy of HSR's users (with a special attention for employees who use electromedical devices which collect patients' data whose self-efficacy should be monitored). It remains a priority also to maintain Perceived Barriers low as well as to increase Perceived Severity. Finally, since the Cues to Action examined in the study resulted negatively associated to the Cybersecurity Behaviour, it could be worth thinking about other cues– different from those considered as items in the present survey - which may trigger employees to adopt the correct cybersecurity behaviours.

IV.8. Implications and future perspectives

ProTego project will have the possibility to design a more appropriate educational framework based on these results. The future intervention will have to focus on the modification of the factors which demonstrated to predict cybersecurity behaviour, with the aim to increase the cybersecurity awareness of hospital's employees. The efficacy of this intervention could also be evaluated by comparing the preliminary and final results related to the constructs of the study.

Inputs for designing the future educational framework are listed below:

- Increase the sense of self-efficacy of HSR's users
- Maintain perceived barriers low
- Design a communication which is more oriented to the negative effects of the cyberattacks (increase perceived severity)
- Exploit those cues to action that may trigger employees to adopt the correct cybersecurity behaviours

V. Overall conclusions

The work done at this stage of the ProTego project and described in this document gives the basis of what should be an organizational approach of cyber security in healthcare organizations

It has been released a tool that allows to assess the current cyber security awareness on a healthcare organization, and also makes possible benchmarking and trend analysis.

The job done has been based in standard models and tools, previously applied in different sectors and this job has applied them to healthcare industry.

The results obtained in both ProTego test bed users offer the guiding principles of what will be the educational framework, focusing the resources in those areas that will have a higher return.

VI. References and Internet Links

S. Egelman and E. Peer, (2015). “Scaling the security wall: developing a security behavior intentions scale"

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). "Analysis of personal information security behavior and awareness. Computers & Security"

Brenda K. Wiederhold (2014). "Cyberpsychology, Behavior, and Social Networking"

Rosenstock (1966). "The Health Belief Model"

SF Michie, R West, R Campbell, J Brown, H Gainforth (2014). "ABC of behaviour change theories"

CS Skinner, J Tiro, VL Champion (2015). "Health Behavior: Theory, Research, and Practice"

RK Jayanti, AC Burns (1998). "The Antecedents of Preventive Health Care Behavior: An Empirical Study"

P Sheeran, TL Webb (2016). "The intention–behavior gap"

M Anwar, W He, X Yuan (2017). "Cybersecurity Behavior Training for Employees"

Pr Ifinedo (2012). "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory"

HS Rhee, C Kim, YU Ryu (2009). "Self-efficacy in information security: Its influence on end users' information security practice behavior"

H Teymourlouei (2015). "Quick Reference: Cyber Attacks Awareness and Prevention Method for Home Users"

L Coventry, P Briggs, D JeskeAad, V Moorsel (2014). "A Structured Means for Creating and Evaluating Behavioral Nudges in a Cyber Security Environment"

NC Bronfman, LA Cifuentes, and VV Gutiérrez (2008). "Explanatory power of the classic psychometric paradigm in risk"

B.A. Nosek, M.R. Banaji, A.G.Greenwald (2002). "Harvesting implicit group attitudes and beliefs from a demonstration web site"

SJ Czaja, N Charness, AD Fisk, C Hertzog (2006). "Factors predicting the use of technology: Findings from the center for research and education on aging and technology enhancement"

E. Rogers (1995). "Diffusion of Innovations. New York: Free Press"

V. Garg ; L.J. Camp (2015). "Spare the rod, spoil the network security? Economic analysis of sanctions online"

C.A. Lane, H.F. Lyle (2011). "Obstacles and supports related to the use of educational technologies: The role of technological expertise, gender, and age"

M.L. Finucane, A.Alhakami, P. Slovic, S.M. Johnson (2000), "The affect heuristic in judgments of risks and benefits

VII. Appendix 1 - Cybersecurity Awareness Survey

English Survey

Cybersecurity Awareness Survey

The survey aims to collect information on **cybersecurity awareness** and it is part of **ProTego**, a project funded by the European Commission under the Horizon 2020 Research and Innovation program. The aim of this project is to develop a data-protection toolkit reducing risks in Hospitals and Care Centers.

The following questions have been developed by the Center for Advanced Technology in Health and Wellbeing and the San Raffaele Hospital's Information System.

The procedure involves filling in an online survey that will take approximately 10 minutes. Your responses will be confidential and we do not collect identifying information such as your name, email address or IP address.To help protect your privacy, the surveys do not contain information that can personally identify you. All data will be collected, managed and stored in electronic format by the Center for Advanced Technology in Health and Wellbeing. The data collected will be disseminated anonymously through scientific conferences or scientific publications. The results of this study will be used for research purposes only.

Please select your choice below.

Clicking on "Yes" button below indicates that:

you have read the above information

you voluntarily agree to participate

If you do not wish to participate in the research study, please decline your participation by clicking on "No" button.

Informativa sulla Privacy di Qualtrics

1. **Do you agree to participate in this survey?**

- Yes
- No*

*Thank you for considering the survey!

2. **Do you use the WiFi (wireless) or the LAN (wired) connection provided by the Hospital during your working activities?**

- Yes
- No*

*Thank you for taking part in the survey. We are now collecting answers

from people that use the WiFi or the LAN connection of the Hospital.

3. **Which job functional area do you work in?**

- Clinical → Please enter your profession: ………………………………………………
- Research → Please enter your profession: ………………………………………………
- Staff → Please enter your profession: ………………………………………………
- Technical → Please enter your profession: ………………………………………………

4. Gender:

- Male
- Female
- I'd rather not specify

5. Age: [Enter manually]

……………………………………………

6. Nationality: [Enter manually]

……………………………………………

7. What is your highest level of education?

- Primary School
- Middle School
- High School
- Bachelor's degree
- Master's degree
- Ph.d./doctorate
- Other: (Indicate) ………………………………………………

8. How would you define your current technological expertise?

- **Beginner**: for example I am able to use a mouse and keyboard, create a simple document, send and receive e-mail, and/or access web pages
- **Intermediate**: for example I am able to format documents using styles or templates, use spreadsheets for custom calculations and charts, and/or use graphics/web publishing
- **Expert**: for example I am able to use macros in programs to speed tasks, configure operating system features, create a program using a programming language, and/or develop a database.

9. How would you define your attitude toward new technologies?

- I am the kind of person that is always looking for new products/technology even before it becomes available on the market
- I am the kind of person that tend to adopt the latest technologies as soon as they become available on the market
- I am the kind of person that tend to buy new products/technology when it is widespread
- I am the kind of person that tend to buy new products/technology when it becomes mainstream
- I am the kind of person that tend not to adopt new products/technologies

10. Have you ever noticed to be under cyber attack?

- Yes, I have noticed it
- No, I haven't noticed it

In this section we will ask you some questions on the electronic devices that you use during your working activities.

11. To carry out your working activities you use::

- Mainly personal devices (smartphone, computer, tablet)
- Mainly business devices (smartphone, computer, tablet provided by the Hospital)
- Both
- None of them

12. Which of the following behaviours do you adopt in the working environment? (It is possible to select more than one options)

□ I use different passwords for my different accounts
□ I don't install freeware
□ I don’t write passwords on paper supports
□ I don’t share my passwords with my colleagues
□ I don’t save my passwords on the browser I am using
□ I don’t install pirated software
□ I check the security setting of a web site before entering any private information
□ I don't open e-mail attachments from people I do not know
□ I don't use USB keys whose provenance is unknown
□ (X) None of these

13. Which of the following measures do you apply to protect your devices (both personal and/or business) from cyberattacks? (It is possible to select more than one options

□ I manage the privacy settings of web sites
□ I keep the antivirus updated
□ I block the pop-ups
□ I backup business data on business network drives
□ I set the web browser to stricter security levels
□ I use a firewall
□ I use filters for e-mail
□ I keep the operating system updated
□ (X) None of these

14. Do you use electromedical devices that collect patients' data during your working activities (e.g. glucometer, infusion pump, pacemaker, etc.)?

- Yes
- No

14.1) In particular, which electromedical devices do you use? (Indicate)

……………………………………………………………………………………………

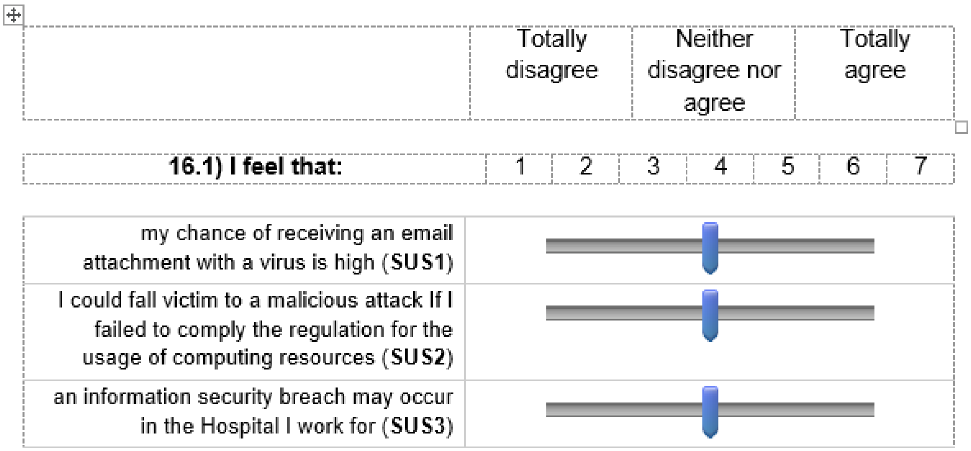
In this section we will ask you some questions on: personal data, and sensitive data

15. Do you process personal data and/or sensitive data of other people during your working activities?

- Yes, only personal data (e.g. name, surname, e-mail, etc.)
- Yes, both personal and sensitive data (e.g. data concerning health, sexual orientation, etc.)
- No, neither of the two

16. In this section we will ask you to indicate your level of agreement on some statements on a scale ranging from 1 to 7 (1= Totally disagree; 7= Totally agree).

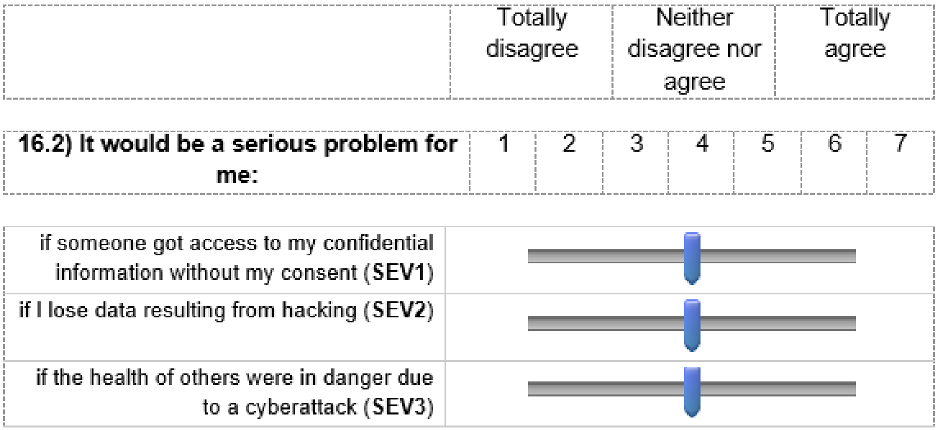
You must move the slider to register the answers.



	Totally disagree	Neither disagree nor agree	Totally agree

16.1) I feel that:	1	2	3	4	5	6	7

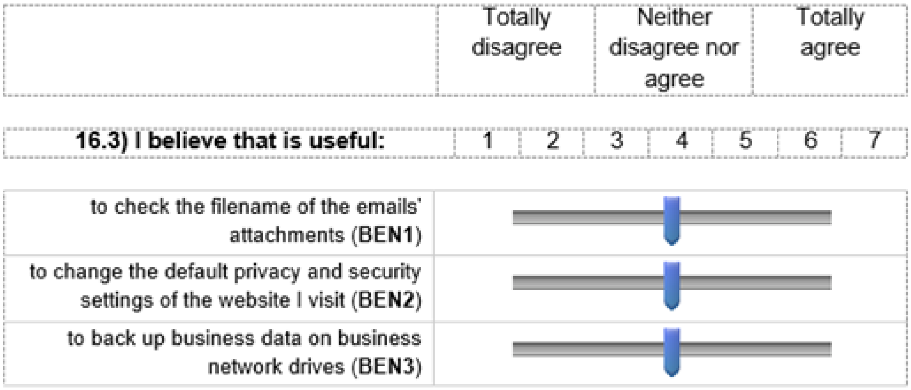
my chance of receiving an email attachment with a virus is high (**SUS1**)	
I could fall victim to a malicious attack If I failed to comply the regulation for the usage of computing resources (**SUS2**)	
an information security breach may occur in the Hospital I work for (**SUS3**)	



	Totally disagree	Neither disagree nor agree	Totally agree

16.2) It would be a serious problem for me:	1	2	3	4	5	6	7

if someone got access to my confidential information without my consent (**SEV1**)	
if I lose data resulting from hacking (**SEV2**)	
if the health of others were in danger due to a cyberattack (**SEV3**)	



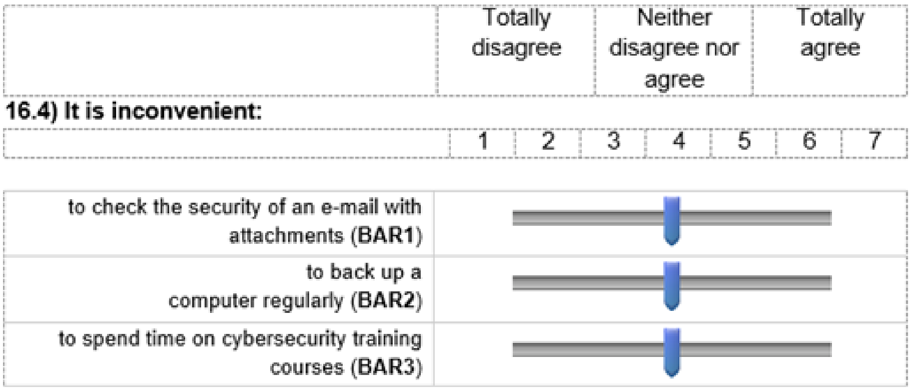
	Totally disagree	Neither disagree nor agree	Totally agree

16.3) I believe that is useful: 1 2 3 4 5 6 7

to check the filename of the emails' attachments (**BEN1**)

to change the default privacy and security settings of the website I visit (**BEN2**)

to back up business data on business network drives (**BEN3**)



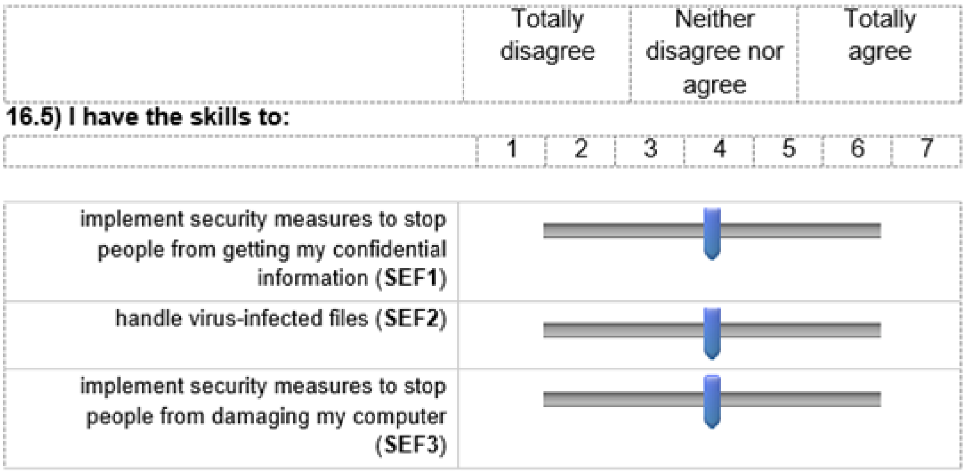
	Totally disagree	Neither disagree nor agree	Totally agree

16.4) It is inconvenient: 1 2 3 4 5 6 7

to check the security of an e-mail with attachments (**BAR1**)

to back up a computer regularly (**BAR2**)

to spend time on cybersecurity training courses (**BAR3**)



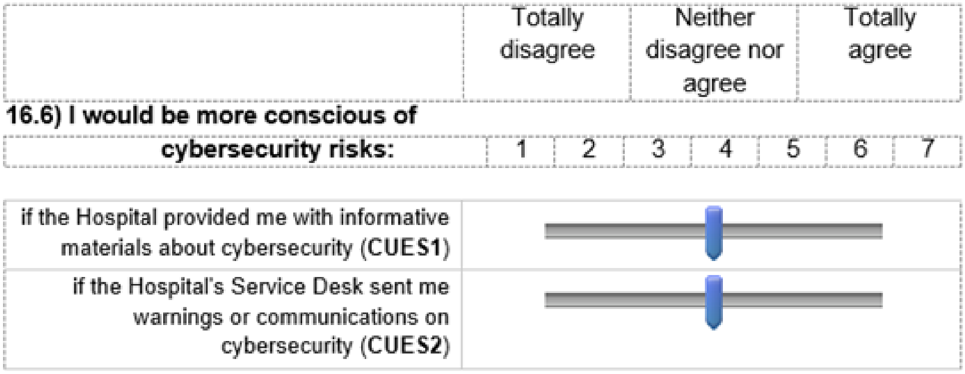
	Totally disagree	Neither disagree nor agree	Totally agree

16.5) I have the skills to: 1 2 3 4 5 6 7

implement security measures to stop people from getting my confidential information (**SEF1**)

handle virus-infected files (**SEF2**)

implement security measures to stop people from damaging my computer (**SEF3**)



	Totally disagree	Neither disagree nor agree	Totally agree

16.6) I would be more conscious of cybersecurity risks: 1 2 3 4 5 6 7

if the Hospital provided me with informative materials about cybersecurity (**CUES1**)

if the Hospital's Service Desk sent me warnings or communications on cybersecurity (**CUES2**)

In this last section we are interested to know your opinion on cybersecurity training.

17. Do you believe that a cybersecurity training course would help you to prevent and face cyberattacks?

- Yes
- No
- I don’t know
- It depends on: (Indicate)

……………………………………………

17.1) How would you like to be informed on cybersecurity? (It is possible to select more than one options)

□ Classroom training courses

□ Online training courses

□ Printed informative material (e.g. poster, flyer, brochure, etc.)

□ Online informative material (e.g. poster, flyer, brochure, informative e-mail, etc.)

□ Other: (Indicate)

……………………………………………

Thank you for taking the time to complete the survey.

All your answers have been correctly registered.

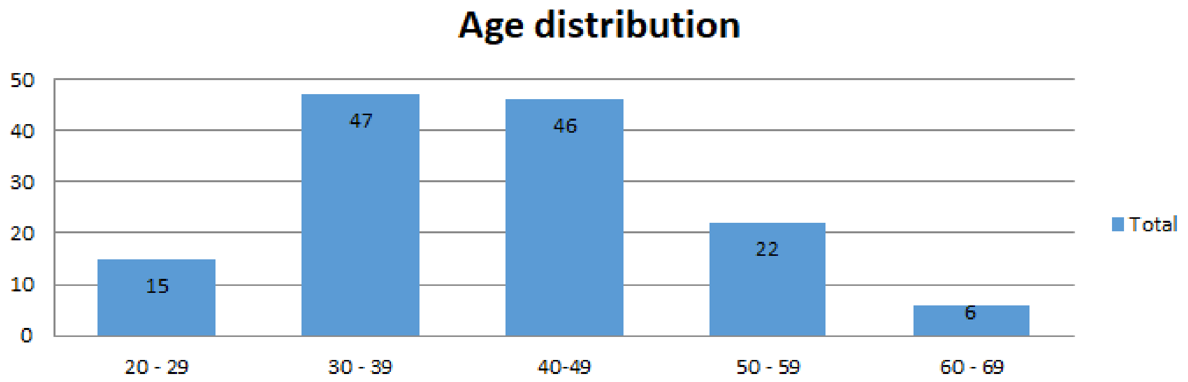
[1] Any information which are related to an identified or identifiable natural person”, such as name, identification number, location data, online identifier etc.

[2] Special categories of personal data include data “revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation

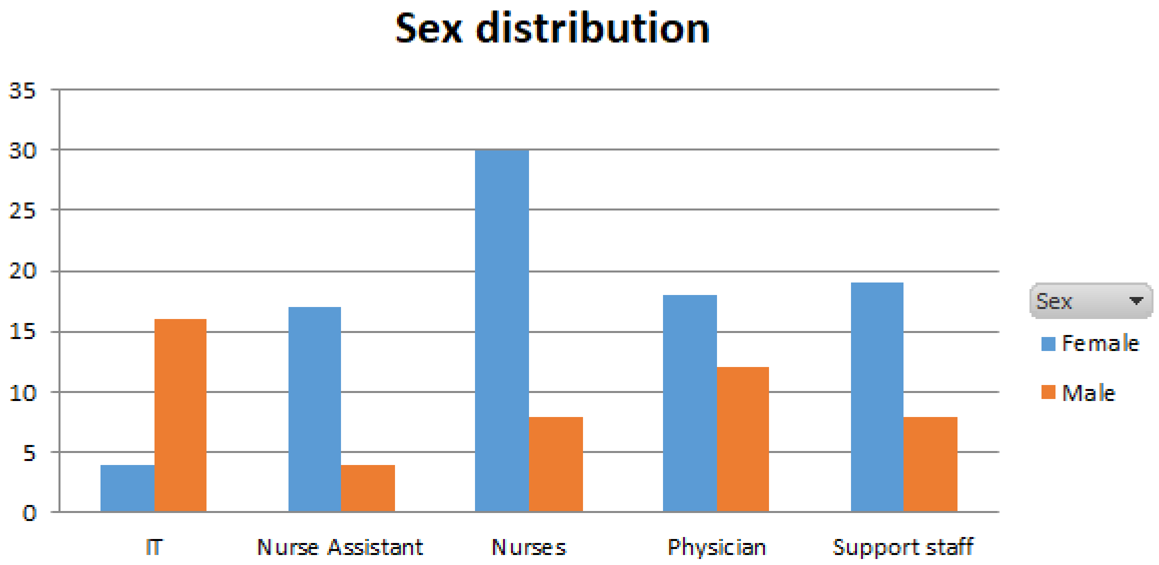
VIII. Appendix 2 – Detailed results in MS

Domain 1: Demographics

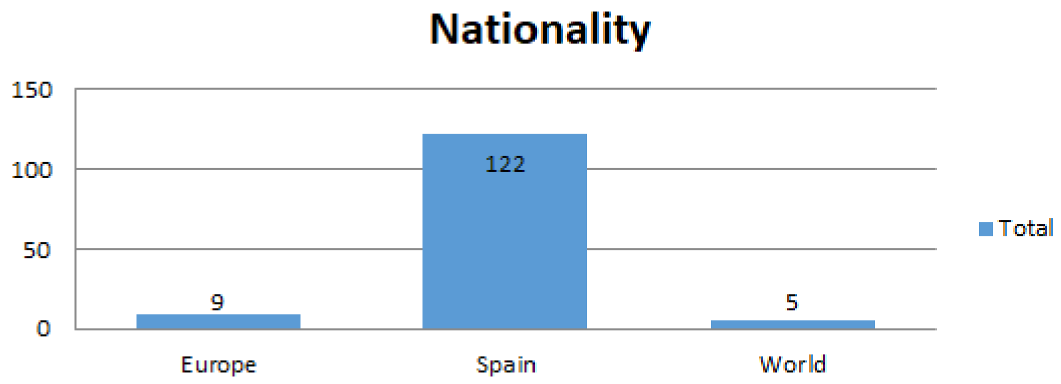
Age distribution: The majority of users are between 30 to 50 years old.



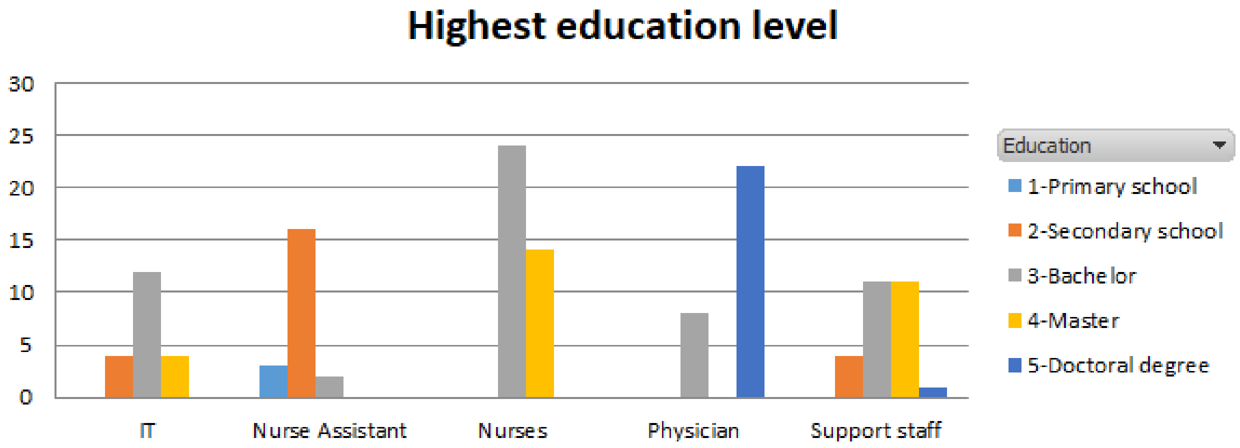
Sex distribution: Majority of women in all the segments except in IT, but that's not representative because IT only represents the 1,5% of the staff.



Nationality: Almost all the users that respond the survey are from Spain, what reflects the reality of the Human Resources in MS.



Highest education level: Almost all users have University education. We can see just a few users outside this in IT and support staff groups.

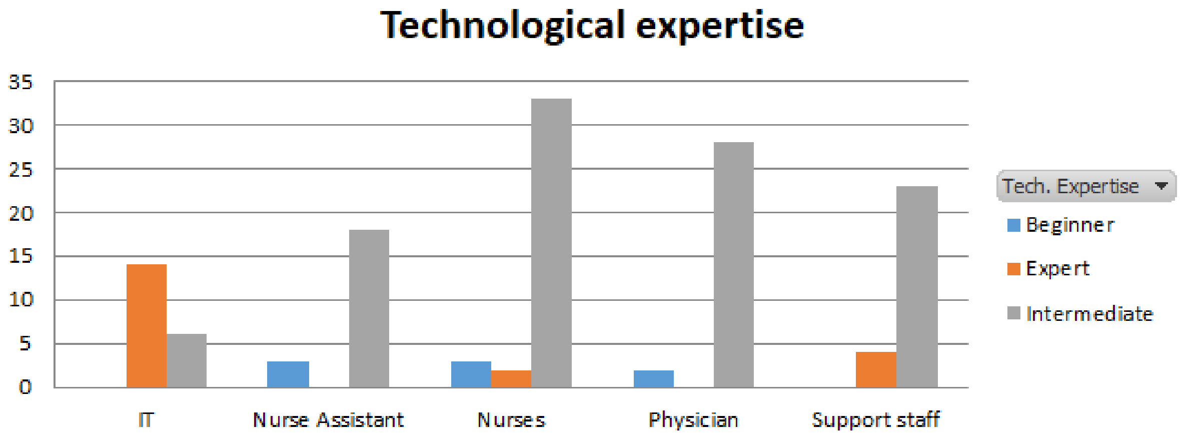


Domain 2: Technological Expertise

Question: How would you define your current technological expertise?

Responses:

1. Beginner: for example I am able to use a mouse and keyboard, create a simple document, send and receive e-mail, and/or access web pages
2. Intermediate: for example I am able to format documents using styles or templates, use spreadsheets for custom calculations and charts, and/or use graphics/web publishing
3. Expert: for example I am able to use macros in programs to speed tasks, configure operating system features, create a program using a programming language, and/or develop a database.



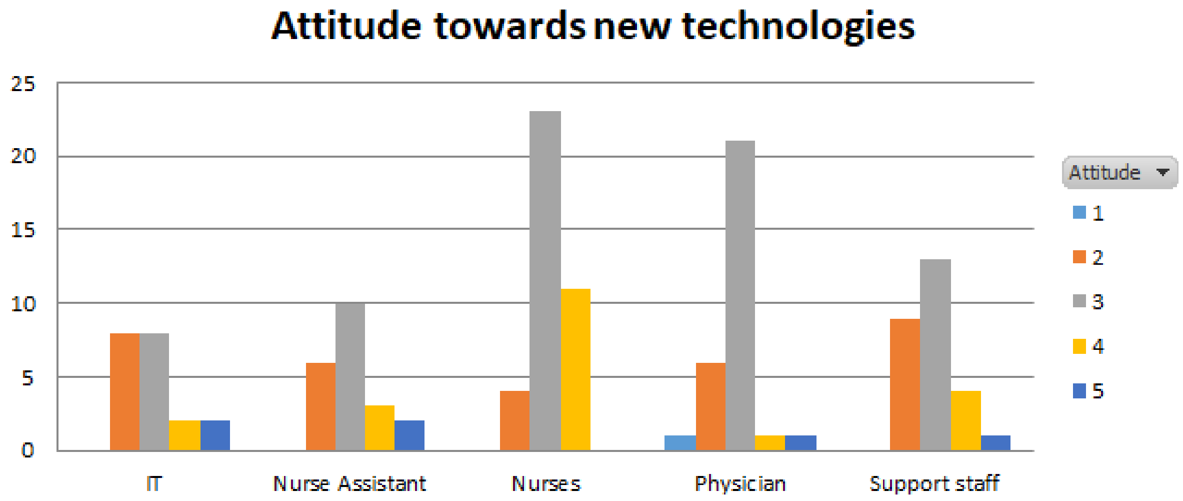
Comment: The vast majority of users consider themselves as intermediate users, that is, they use technology but only know what is needed to achieve their goals and don’t care about security, speed or productivity. In the IT department users are slightly different, as expected they consider they have advanced skills.

Domain 3: Attitude toward new technologies

Question 1: How would you define your attitude toward new technologies?

Responses:

1. I am the kind of person that is always looking for new products/technology even before it becomes available on the market
2. I am the kind of person that tend to adopt the latest technologies as soon as they become available on the market
3. I am the kind of person that tend to buy new products/technology when it is widespread
4. I am the kind of person that tend to buy new products/technology when it becomes mainstream
5. I am the kind of person that tend not to adopt new products/technologies



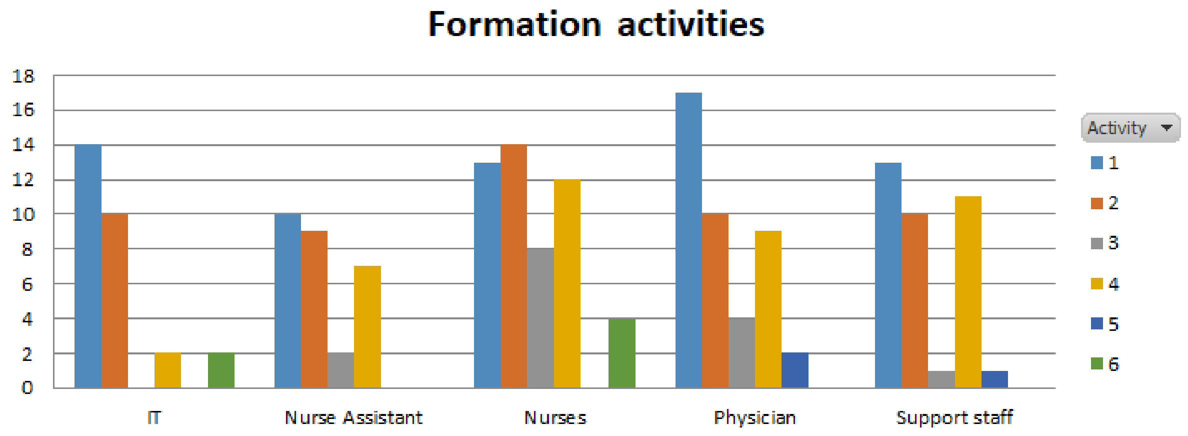
Comment: Most of users adopt new technologies from the moment they are released (known to the market) until they become mainstream. There are no ”experimental” users and only a residual number of users that don’t tend to adopt new technologies.

Domain 4: Cybersecurity Background

Question 1: Which of the following activities do you carry out to be informed on cybersecurity?

Responses:

1. I read articles
2. I consult online materials
3. I attend specific training courses
4. None
5. I don't know
6. Other: (indicate)

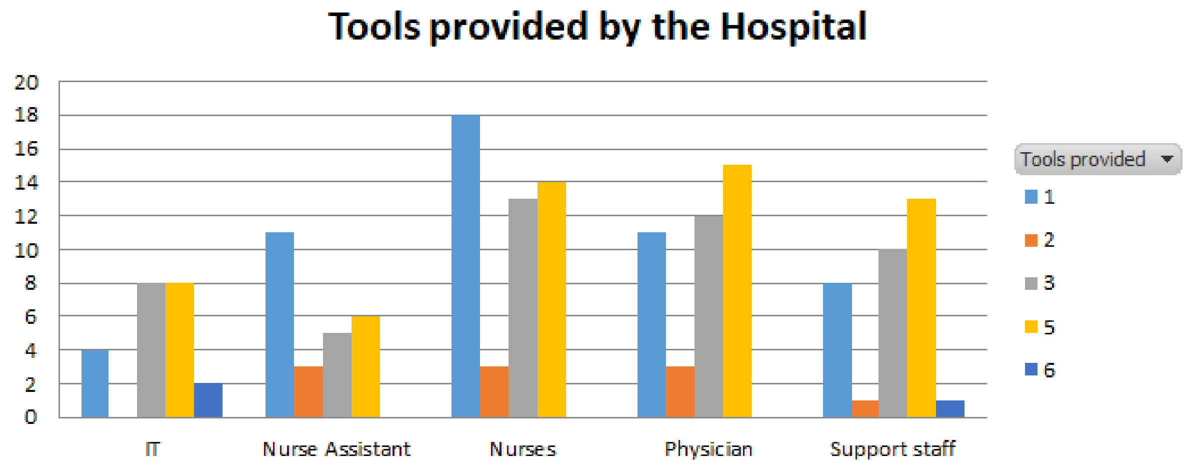


Comment: There are a significant number of users that don't carry any special activity to be informed about cybersecurity topics. Between those users who carry out any initiative to do that, the preferred way is to read online materials and articles. The only extra activity reported is to ask other close people with more knowledge about cyber security.

Question 2: Which tools does the Hospital provide to inform its employees on cybersecurity?

Responses:

1. A regulation for the usage of computing resources
2. Cybersecurity training courses
3. Informative materials on cybersecurity sent by e-mail
4. I don't know
5. None
6. Other: (Indicate)



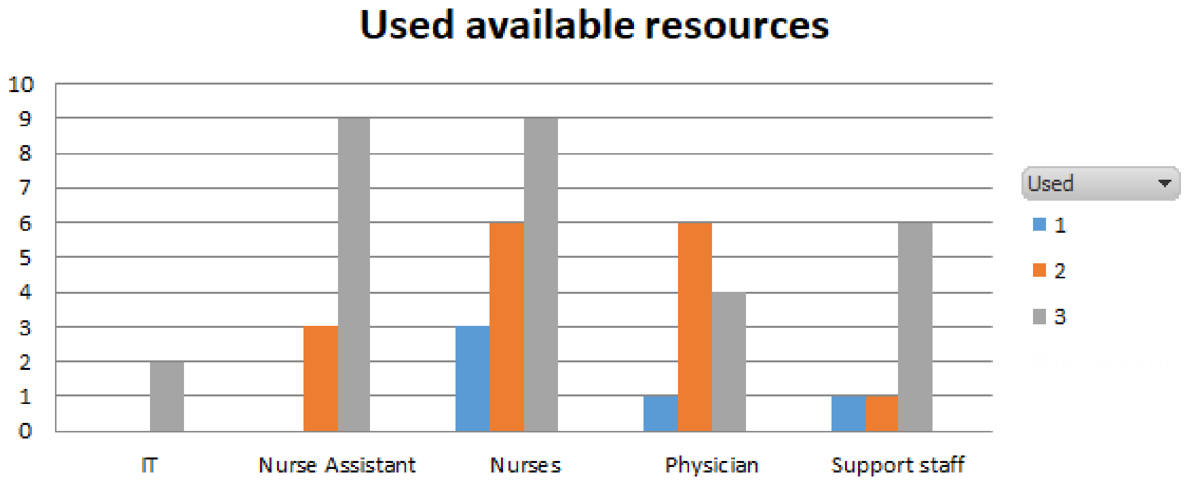
Comment: The results to this question make clear that there is a lack of specific training on cyber security. Despite all users identify that there are available some contents related with cyber security, they also say that the organization did not offer any training regarding cyber security.

Question 3: Have you ever consulted the Hospital's regulation for the usage of computing resources and/or attended a cybersecurity training course recommended by the Hospital?

Responses:

1. Yes, both

2. Yes, just one of them
3. No
4. I don't know



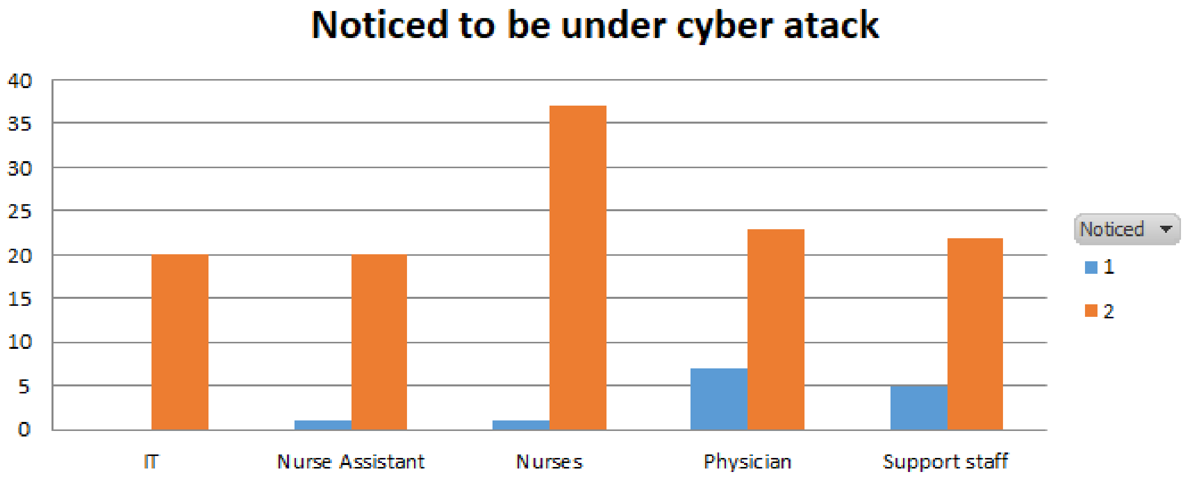
Comment: This question is complementary to the previous one, that is, only users that responded that know that the hospital has provided materials related to cyber security that users can use on their own, can respond to this question. Regardless of the materials used, what is revealing is the high number of users that don't use the material that is available, without a targeted and directed training.

Domain 5: Cyber attacks' experience

Question 1: Have you ever noticed to be under cyber attack?

Responses:

1. Yes, I have noticed it
2. No, I haven't noticed it

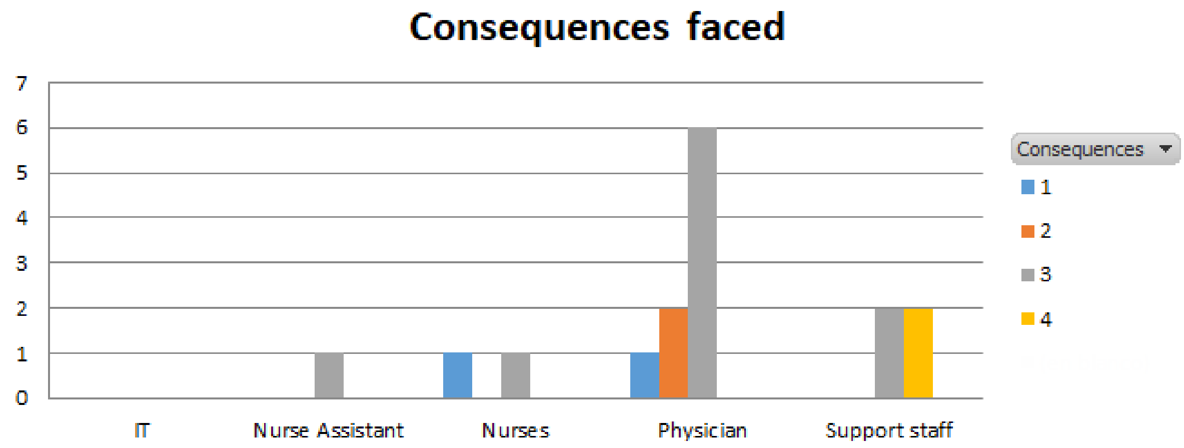


Comment: Most users of all categories have not ever noticed to be under a cyber attack.

Question 2: Which consequences did you face? (It's possible to select more than one option)

Responses:

1. Data Loss
2. Money Loss
3. Computer slowing down
4. I haven't noticed any consequences
5. I don't know
6. Other: (Indicate)

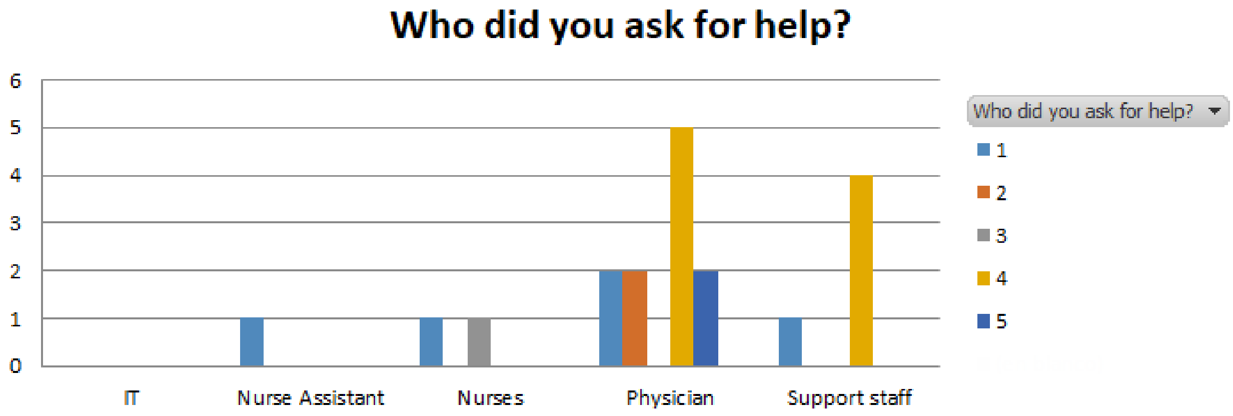


Comment: This question was only answered by users that responded that ever noticed to be under a cyber attack. Only few users noticed that the cyber attack may have real consequences as loos of money or data. The major part of users didn't perceive the risk they were exposed to.

Question 3: Who did you ask for help? (It's possible to select more than one option)

Responses:

1. To anyone, I was able to manage the situation by myself
2. To a tech expert friend/acquaintance
3. To the device's manufacturer
4. To the Hospital's Information System through the Service Desk or through other channels: (Indicate)
5. To the competent local authorities
6. I don't know
7. Other: (Indicate)



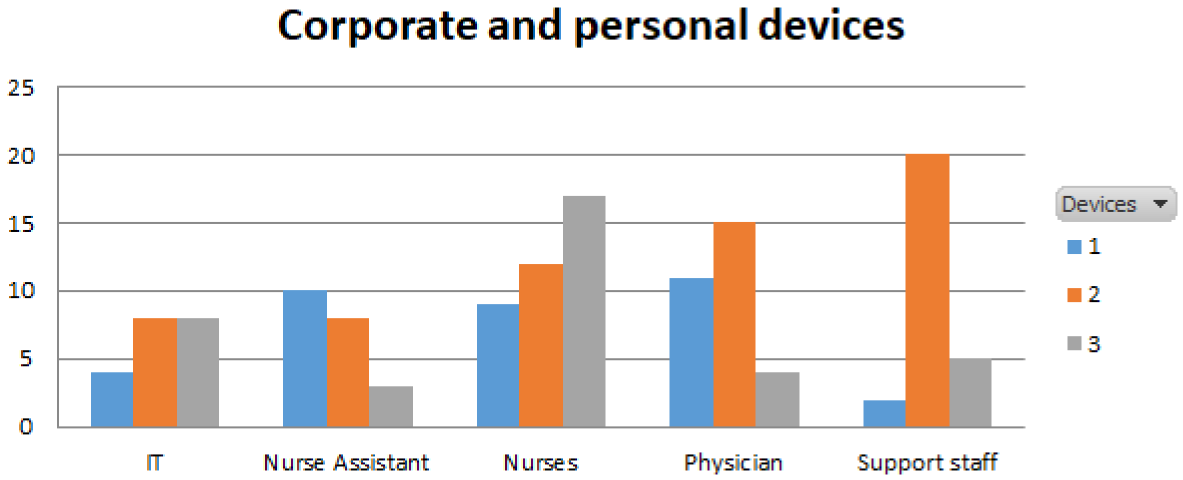
Comment: The fifty percent of users asked the Service Desk of the Hospital for help. As the rest of the users may or not suffer the cyber attack in their work place, the service desk seems an important point to reinforce with appropriate protocols.

Domain 6: Devices used during working activities

Question 1: To carry out your working activities you use:

Responses:

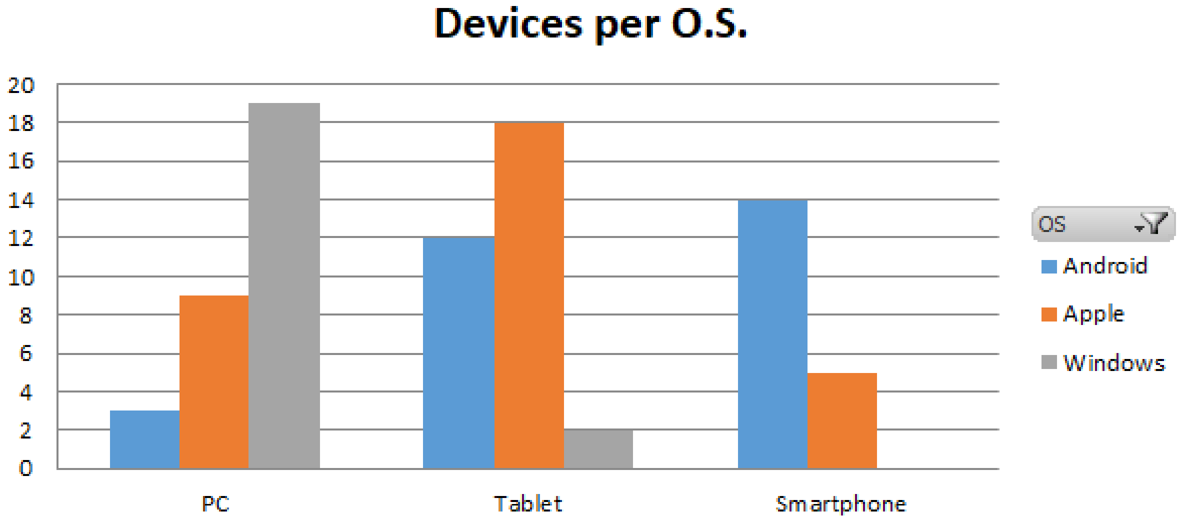
1. Mainly personal devices (smartphone, computer, tablet)
2. Mainly business devices (smartphone, computer, tablet provided by the Hospital)
3. Both corporate and personal



Comment: Except in the Support staff segment we see that there are many no corporate devices that are connected to the Hospital networks and used to carry out working activities.

Question 2: Which operating systems are installed in the personal devices you use to carry out your working activities?

Responses:

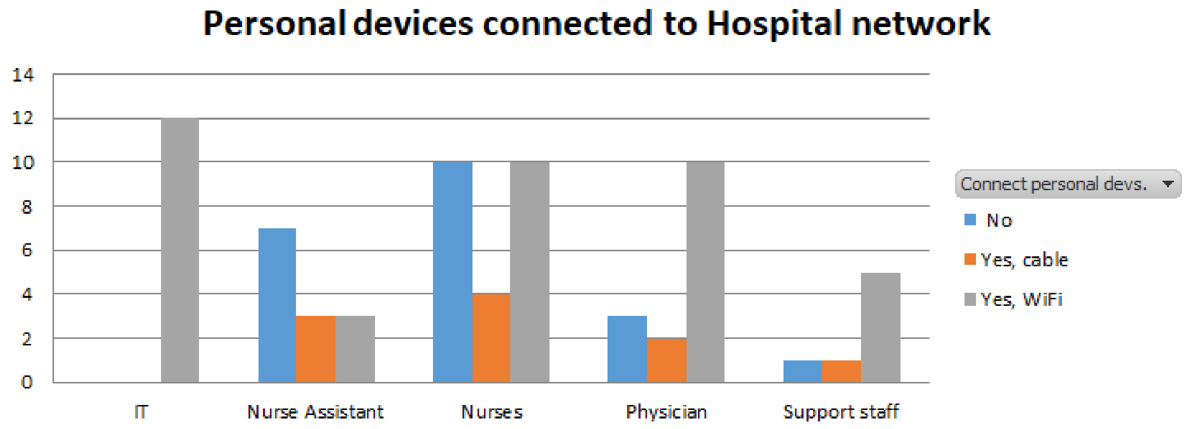


Comment: This question refers to personal devices. In this question the type of user is not relevant. The results show that Windows is the Operative System more used in PCs, while in tablets and Smartphones the systems used are Android and Apple without a significant difference between them.

Question 3: Have you ever connected your personal device/s to the Hospital network?

Responses:

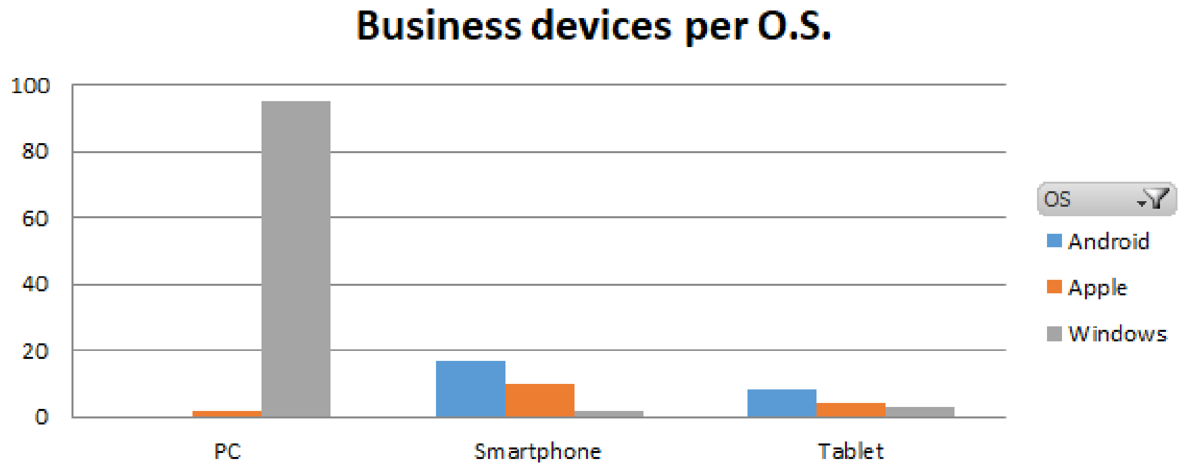
1. Yes, by cable
2. Yes, through Wi-Fi
3. Yes, through Bluetooth
4. No



Comment: Most of users connect their devices to the Hospital WIFI. Cable connection is not allowed by the Hospital policy except to a small group of VIP users.

Question 4: Which operating systems are installed in your business devices you use to carry out your working activities?

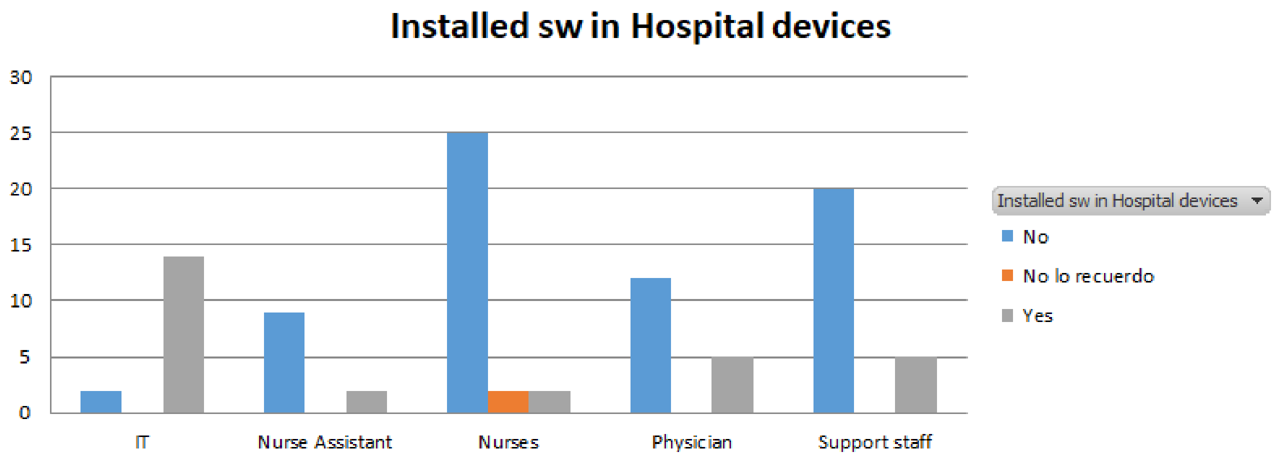
Responses:



Comment: This question refers to business devices. We see that the distribution is mostly the same as in personal devices. Personal computers mainly in Windows, and tablets and Smartphones mixed between Apple and Android.

Question 5: To carry out your working activities, have you ever installed software or applications in your business devices that are not provided by the Hospital?

Responses:

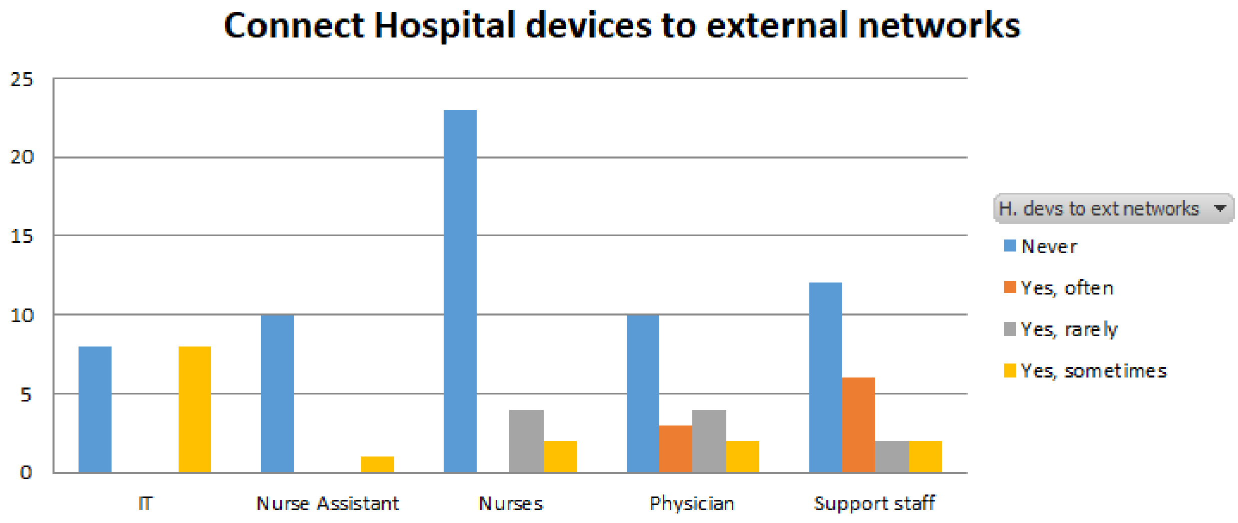


Comments: Installing sw in Hospital devices is not extended practice in Marina Salud, due to the security policies. Outside IT department, only some VIP users have been provided with smartphones and they can install apps in those smartphones. But IT department received requests for software installation in PCs, so we think users will try to install application in any device they use quite often.

Question 6: Have you ever connected the business devices to networks that are not managed by the Hospitals? (e.g. public WiFi, home WiFi)

Responses:

1. Yes, always
2. Yes, often
3. Yes, sometimes
4. Yes, rarely
5. Never

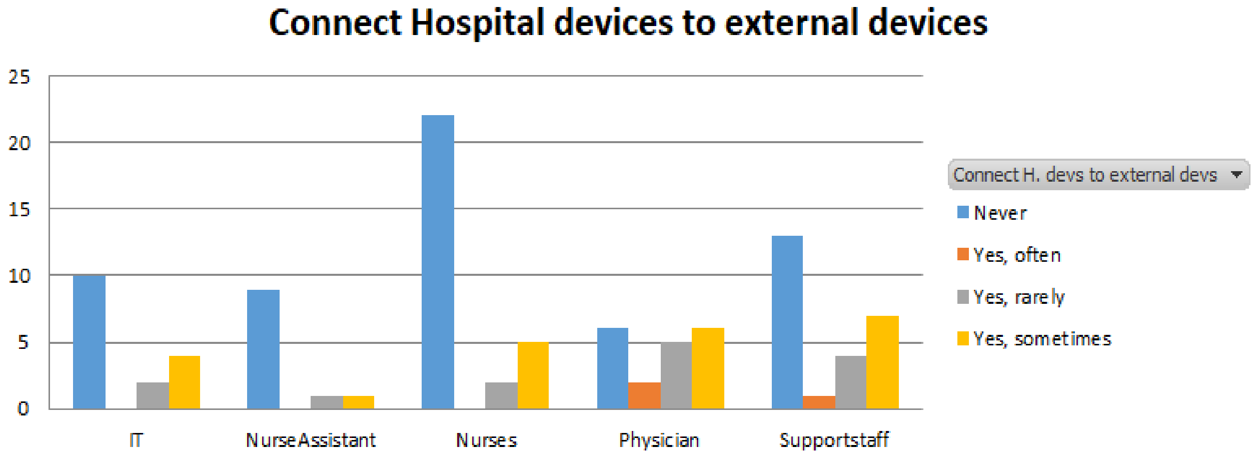


Comments: The major part of users in Marina Salud that are provided with devices are not allowed to take those devices from the Hospital to home or other places, where they can connect them to external networks. But despite it's not a common behavior it happens and so it's a source of risk that needs to be managed, and an item that needs to be treated in educational framework.

Question 7: Have you ever connected your business devices to devices that are not managed by the Hospital (e.g. personal smartphone, personal USB key, etc.)?

Responses:

1. Yes, always
2. Yes, often
3. Yes, sometimes
4. Yes, rarely
5. Never



Comments: Again this behavior is conditioned by the security policies. It's not allowed for many users to connect usb keys, etc. But those who are allowed to do it, perform this type of connections. So it's another potential subject for educational framework.

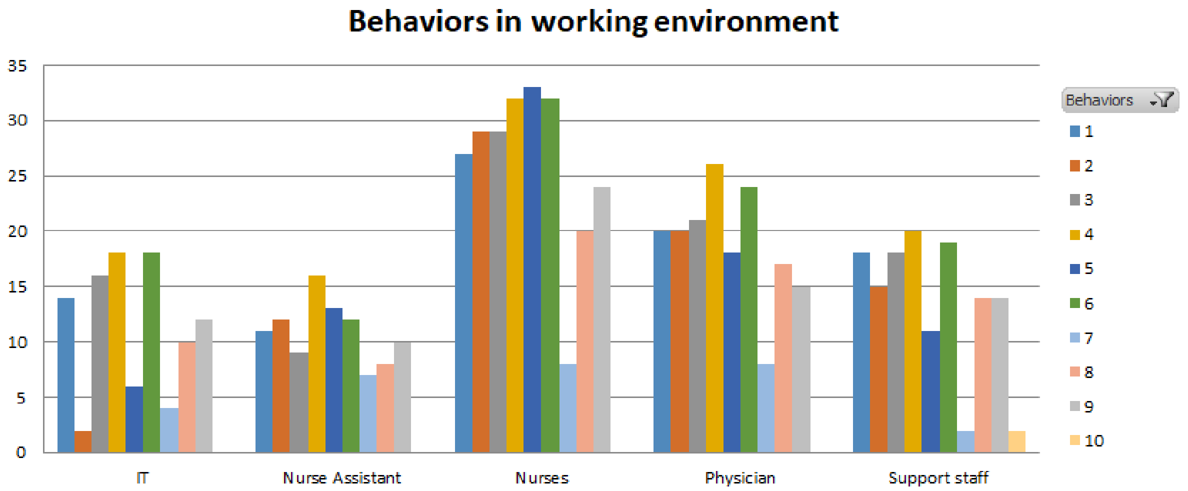
Domain 7: Awareness Health Belief Model (1)

Question 1: Which of the following behaviours do you adopt in the working environment?

Responses:

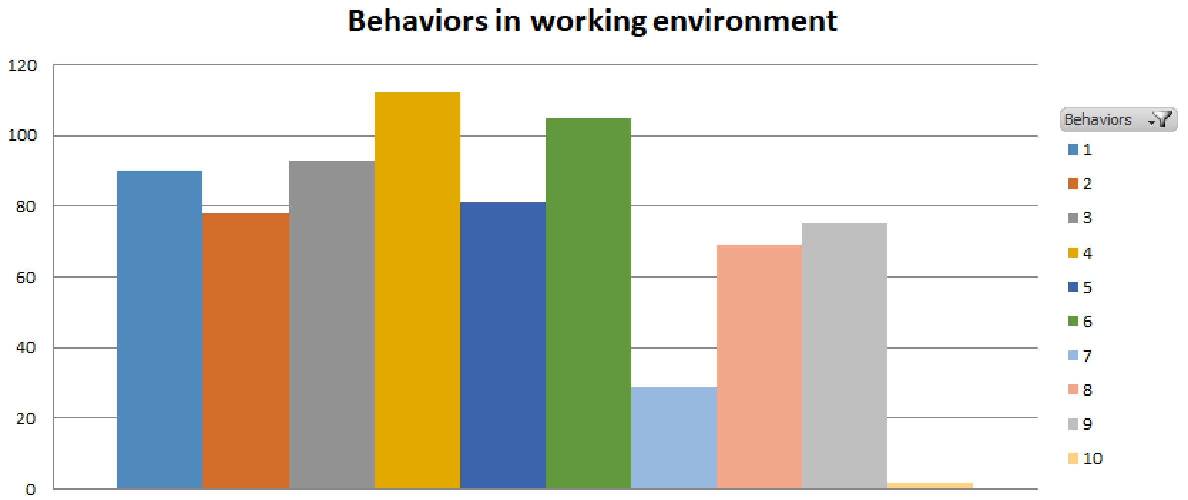
1. I use different passwords for my different accounts
2. I don't install freeware
3. I don't write my passwords on paper supports
4. I don't share my passwords with my colleagues
5. I don't save my passwords on the browser I am using
6. I don't install pirated software
7. I check the security setting of a web site before entering any private information
8. I don't open e-mail attachments from people I do not know
9. I don't use USB key that I don't
10. None of these

First, we show the responses by each user type:



But it doesn't show significant differences, except that IT members don't see as a high risk practice the installation of free software and the fact of storing passwords in browsers.

Next figure shows the same information combined, without the user type variable:



From this point of view we see that the items #7 (I check the security setting of a web site before entering any private information) and #8 (I don't open e-mail attachments from people I do not know) need to be reinforced with education.

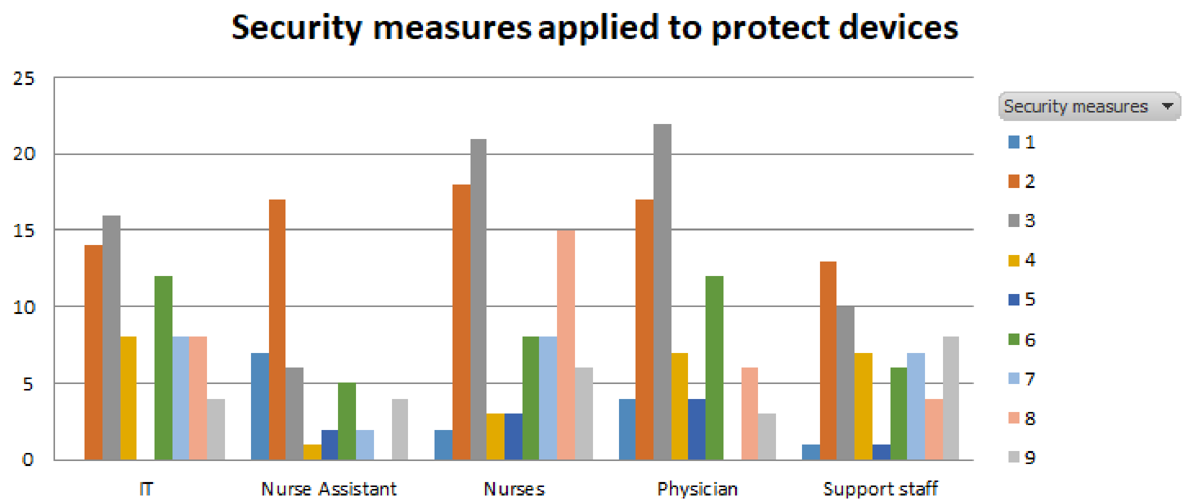
Comments: All users take into account to apply some good practices in their normal behavior. That indicates that cybersecurity is a concept that users already acquired, but it's needed to explain users the risks related with some of their actions where they seem not to be aware of the risks behind them.

Question 2: Which of the following measures do you apply to protect your devices?

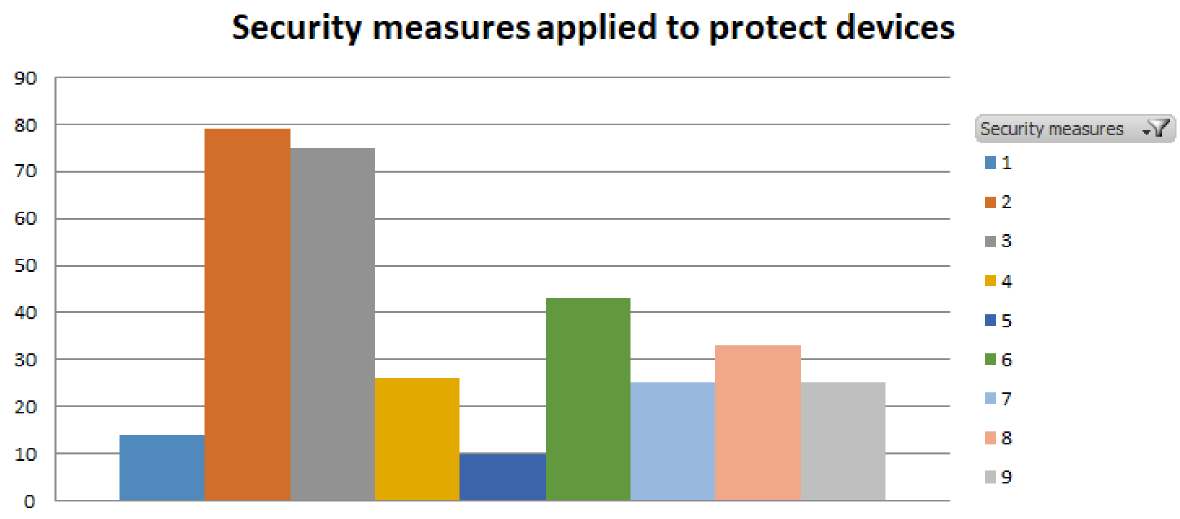
Responses:

1. I manage the privacy settings of web sites
2. I keep the antivirus updated
3. I block the pop-up
4. I backup business data on business network drives
5. I set the web browser to stricter security levels
6. I use a firewall

7. I use filters for e-mail
8. I keep the operating system updated
9. None of these



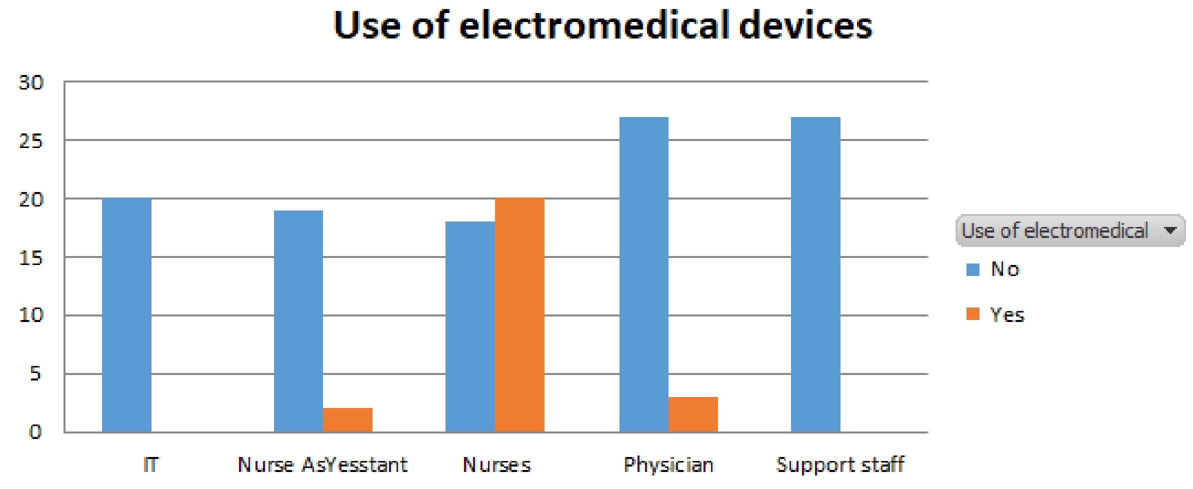
And the same view with aggregated data for all the user types:



Comments: The measures #2 (keep the antivirus updated) and #3 (block the pop-up) are the most used. It’s needed to reinforce the concepts regarding the rest of the measures.

Question 3: Do you use electromedical devices that collect patients' data during your working activities (e.g. glucometer, infusion pump, pacemaker, etc.)?

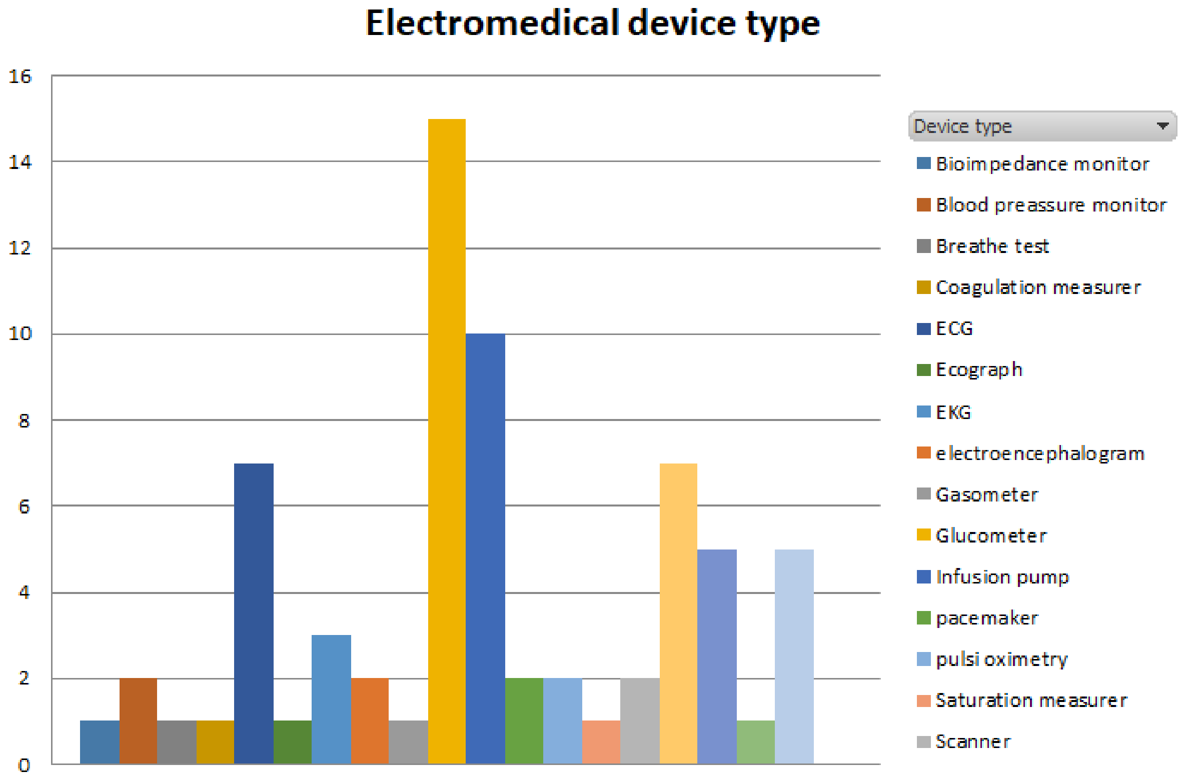
Responses:



Comments: Electromedical devices are mainly used by nurses. Physicians and nurse assistant personnel also make some use of them.

Question 4: Which electromedical devices do you use?

Responses:



Comments: Abstracting the concrete device reported in each response, among the more used devices there are items from the two main categories (in terms of cyber-security):

- "Big devices", such as ECG or infusion pumps, that are connected to the Hospital network and usually coordinated by a gateway device that gathers the data from all of them and send it to the centralized hospital EMR. These devices are exposed to bigger risks, and those risks are perceived by IT department and thus security measures are taken.
- "Small devices", such as glucometers or pulsi-oximetrys. These devices are not usually connected to the hospital network, but use to get connected via USB to corporate

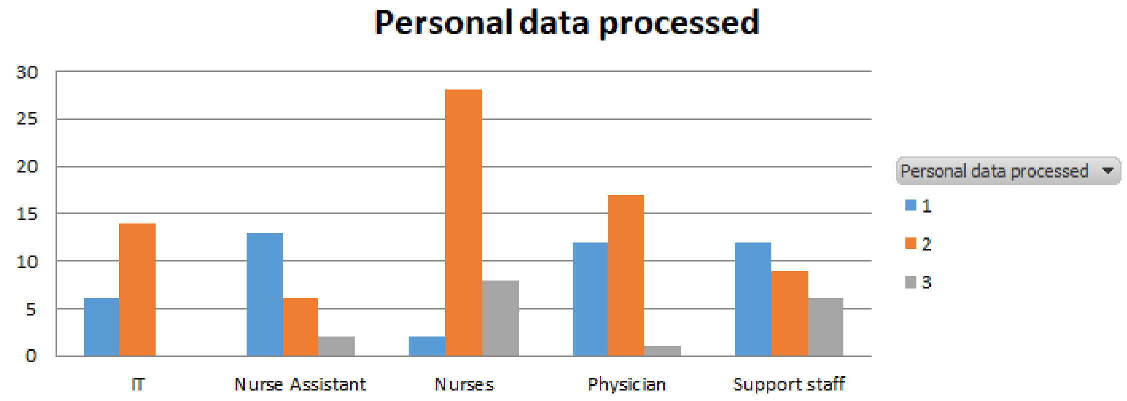
workstations to download data, etc. As the perceived risk is lower, the security measures are also less accurate.

Domain 8: Processing of personal data

Question 1: Do you process personal data and/or sensitive data of other people during your working activities?

Responses:

1. Yes, only personal data (e.g. name, surname, e-mail, etc.)
2. Yes, both personal and sensitive data (e.g. data concerning health, sexual orientation, etc.)
3. No, neither of the two

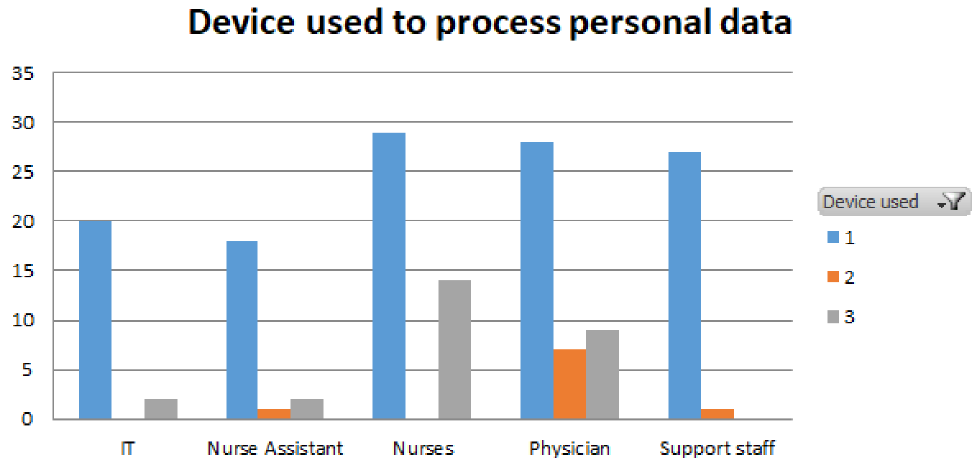


Comments: Members of all user type process personal and sensitive data.

Question 2: Which devices do you use to process personal data and/or sensitive data?

Responses:

1. Business devices
2. Personal devices
3. Medical devices
4. None of these

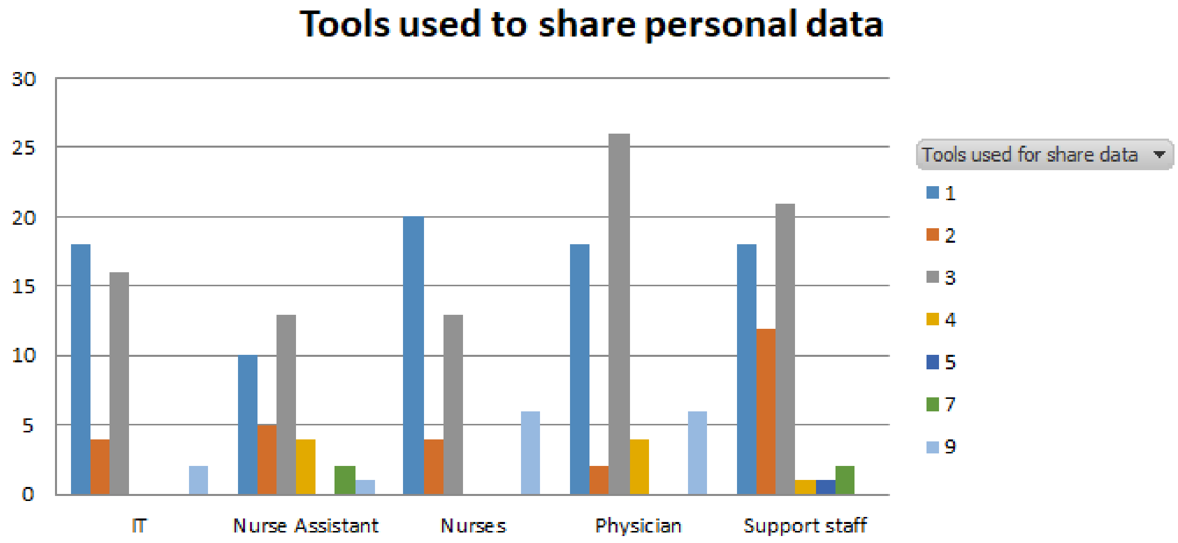


Comments: Only physicians treat personal data through devices that have not been provided by the hospital

Question 3: Which tool do you use for sharing personal data and/or sensitive data of other people?

Responses:

1. Business application
2. Business file sharing
3. Business e-mail
4. Personal e-mail
5. External Cloud
6. Business Cloud (Dropbox Enterprise)
7. External USB/HD key
8. Skype
9. Whatsapp
10. None of these
11. Other: (Indicate)



Comments: The most used tools used to share personal data are business applications and email. But there are other inappropriate uses like watsapp, external cloud or external USB/key. The Hospital does not provide a corporate cloud repository, in Marina Salud this concept has been implemented through a corporate Storage Area Network (SAN) that is physically in the Hospital Data Center.

Domain 9: Awareness Exercises

Question 1: You are now pretending to write a "hacker resistant" password.

Please make sure you'll remember it!

Responses:

The following table shows a representative extract of the password users have introduced as response to this question.

EBekatatva010609	20191977	1013%Al%Em_2	95sanmiPe
Tracatra898	AlDaA1986#	Alzira85	MS20190102VTS
P1zz@0p@3ll@	A44784478eb	Ajdef201710	Migen123*
Estre@restA	Oct2019mantra	JCJRNA1989?	Rahina!19
zeqtia21n1992	Lwt65qW.	Gata80+1	Sauxarera81
Cadiz2019	NEus2011	MOP6julio15	Prefieropaezza@1

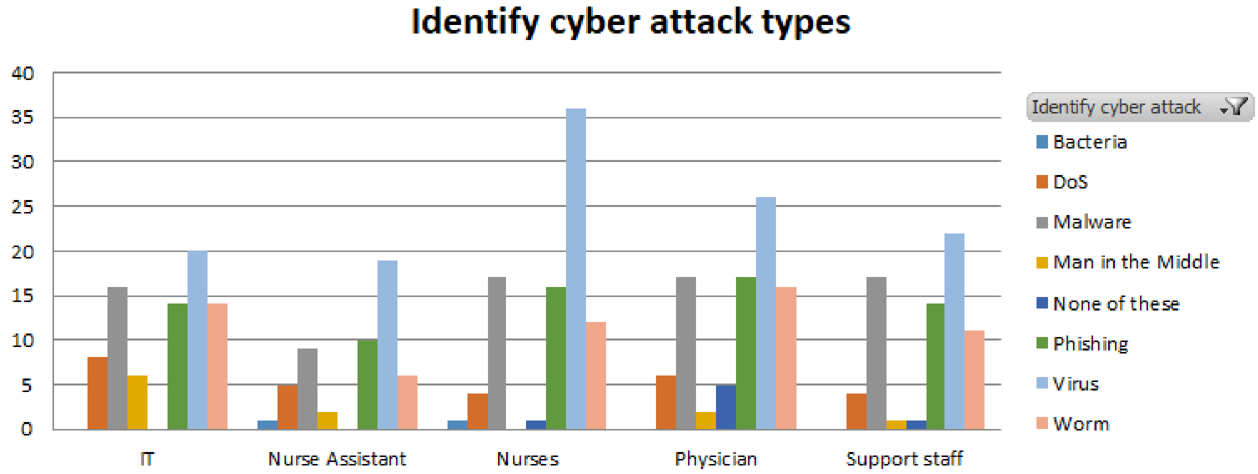
Bestia21n1992	1013%Al%Em_2	crmLyy.1	Patriwiki3580
Cadiz2019	Alzira85	Pr1sc1l@3891e	Satoyduck
wSdrt045Oa	AlDaA1986#	Panxito149	sazrQmento1019

Comments: Due to that the password policy in Marina Salud is quite restrictive and users need to change it every 45 days, users are able to find strong passwords. Originals passwords have been modified to not include possible real ones, but keeping its original strength.

Question 2: Indicate which of the following options you can identify as cyber attacks.

Responses:

1. Virus
2. Denial of Service
3. Bacteria
4. Malware
5. Worn
6. Jungle
7. Phishing
8. Man in the Middle
9. None of these



Comments: Users are familiar with the most common type of cyber-attacks. But there are some of them as “man in the middle”, “Denial of Service” that only IT staff is able to identify.

Question 3: Match the following definitions with the cyber attacks they refer to. If you don't know the cyber attack please select "I don't know".

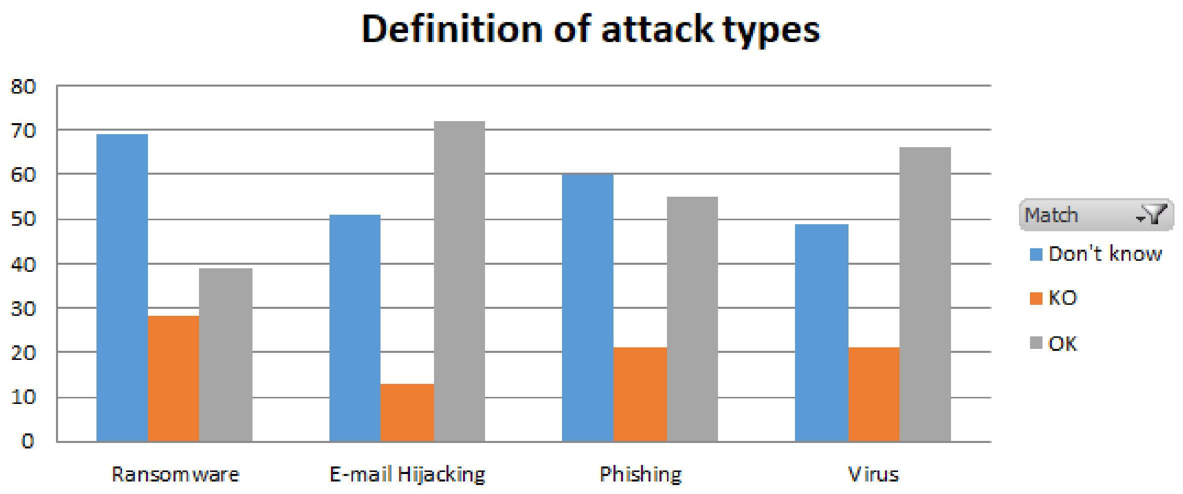
Responses:

Definitions:

1. Attack that implies personal data subtraction (e.g. credit card number) through a fraudulent e-mail sent by an untrusted source
2. Attack that implies the spread of malicious codes through computer files
3. Attack that implies the block access to personal data that can be restored only through a payment
4. Attack that implies the unauthorized access of an e-mail account

Attack types:

1. Phishing
2. Virus
3. Ransomware
4. E-mail Hijacking

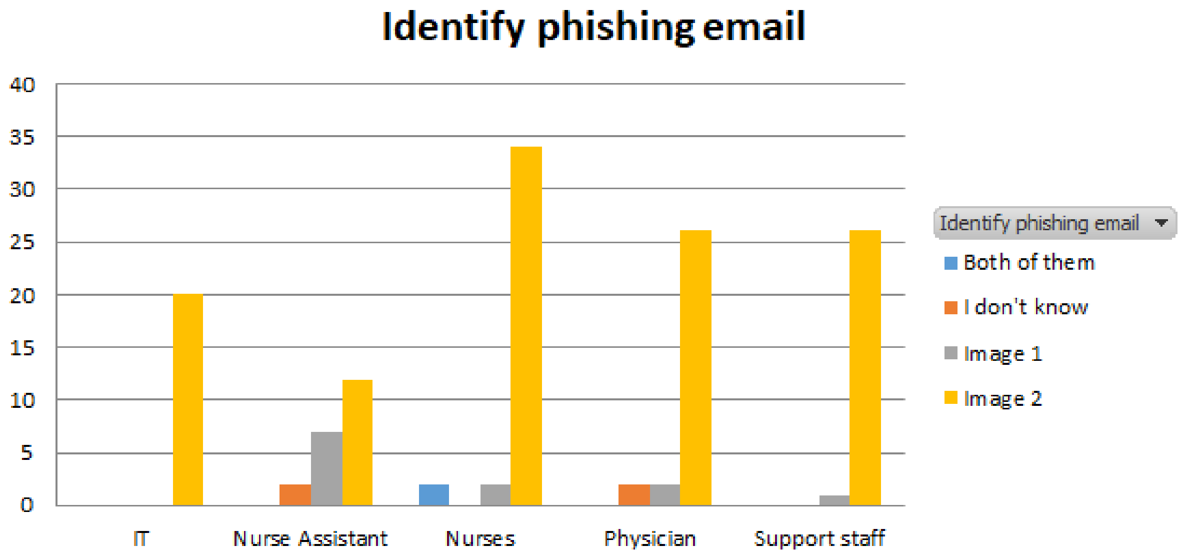


Comments: There is still a high number of users that either admit that can't recognize the attack type based on the definition or actually didn't know what each attack type is.

Question 4: Which of the two screens do you think is potentially risky in terms of cybersecurity?

Responses:

1. Normal email → Incorrect response
2. Phishing email → Correct response
3. Both of them → Incorrect response
4. I don't know → Incorrect response



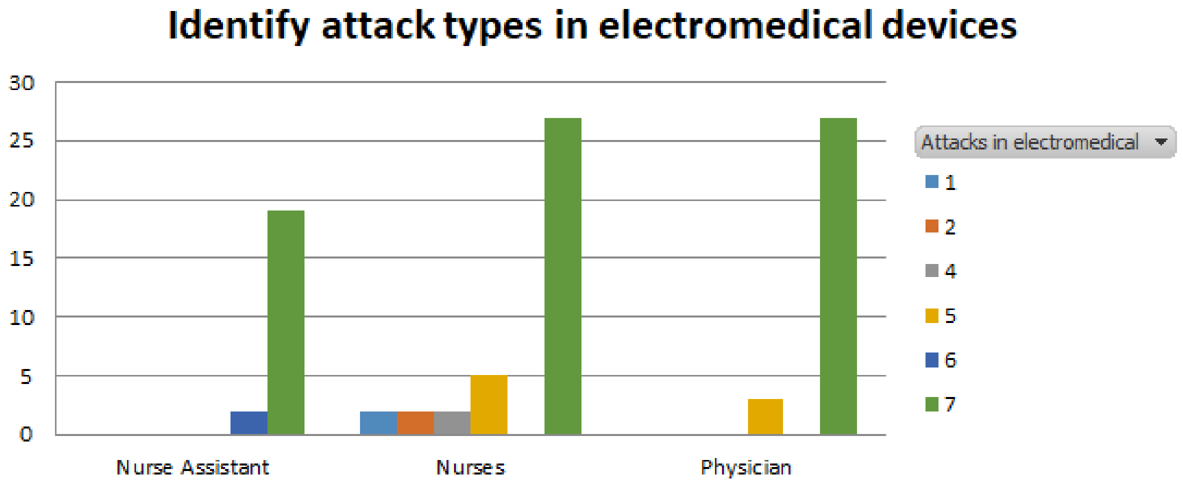
Comments: In this question two emails have been shown to users, the first is a regular "password caducity" email and second a phishing email asking the user to click a link to change password whit a little change in the email of the sender respect to the real help desk email.

The first point to notice is that 100% of IT users identified the phishing email. Out of this group only Nurse Assistants have a relevant number of incorrect responses. This group of users has lower education level and less contact with IT systems.

Question 5: Which of the following cyber attacks may occur on electromedical devices?

Responses:

1. Denial of Service
2. Man in the Middle
3. Malware
4. SQL Injection
5. None of these
6. All of these
7. I don't know

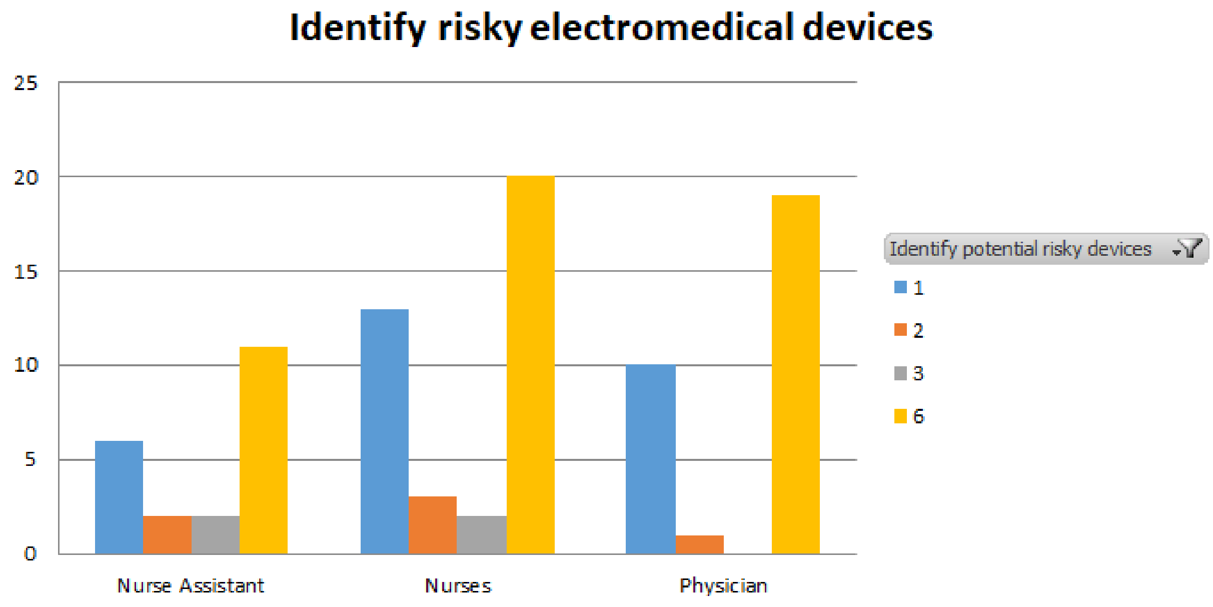


Comments: This question has been only responded by clinical users. By reviewing the responses we can assert that the major part of users didn't know the type of cyber attack they face while using electromedical devices.

Question 6: Which of the following implantable medical devices could potentially be at risk of cyber-attacks?

Responses:

1. Insulin pump connected to the WiFi
2. Pacemaker not connected to the WiFi
3. Cochlear Implant not connected to the WiFi
4. Intraocular lens
5. Catheter
6. I don't know



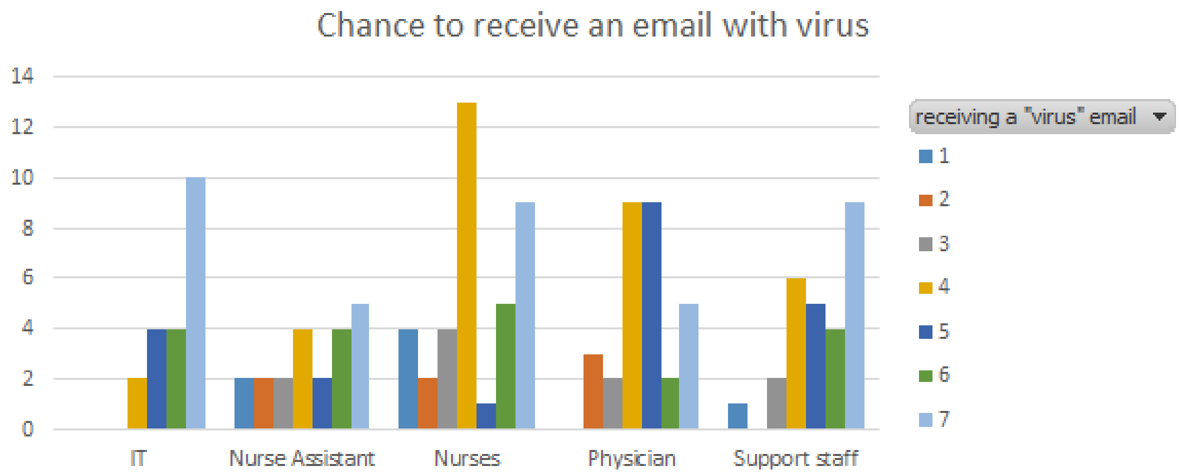
Comments: Due to survey configuration, this question has been only responded by clinical users. We can see that the most chosen response to it has been "I don't know". The interpretation we make is that although most of the users has the perception that Insulin pumps (and other devices such as EGC) are potentially risky, there are other smaller and less used devices that users don't know how much risky they are.

Domain 10: Awareness Health Belief Model (2)

Question 1: I feel that my chance of receiving an email attachment with a virus is high

Responses:

Totally disagree			Neither disagree nor agree			Totally agree
1	2	3	4	5	6	7

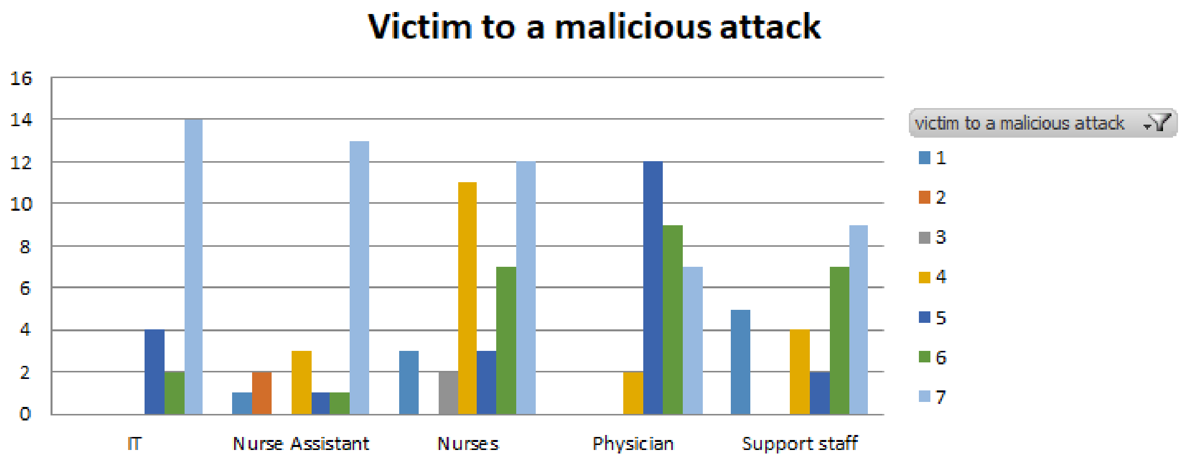


Comments: Most of the users think that the probability to receive an email with a virus is quite high.

Question 2: I feel that I could fall victim to a malicious attack if I failed to comply the regulation for the usage of computing resources

Responses:

Totally disagree			Neither disagree nor agree			Totally agree
1	2	3	4	5	6	7

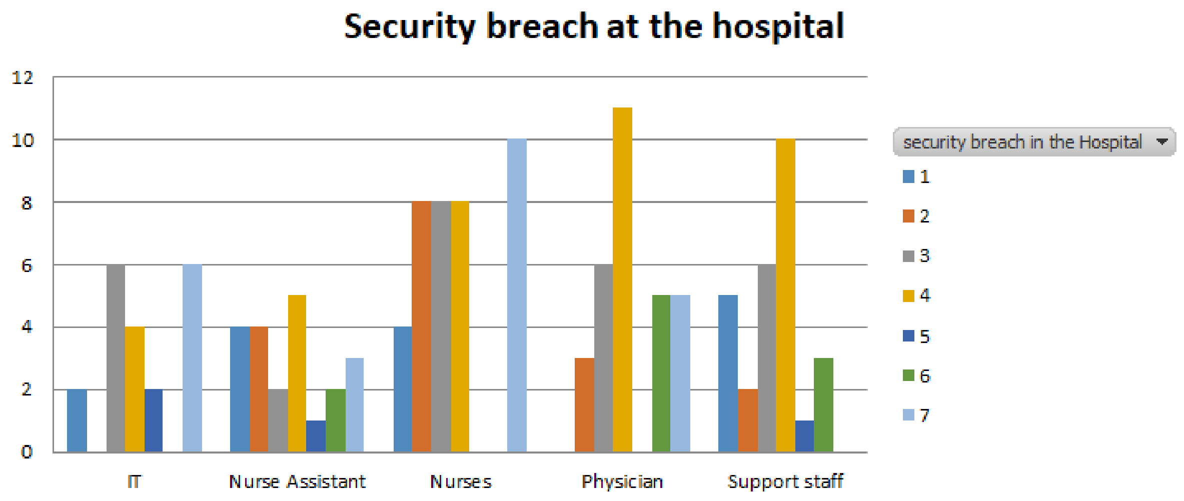


Comments: With the only exception of nurses that gave a neutral response in more cases, the most of users understand that there is a real risk if they do not accomplish the regulation for the usage of computing resources.

Question 3: I feel that an information security breach may occur in the Hospital I work for

Responses:

Totally disagree			Neither disagree nor agree			Totally agree
1	2	3	4	5	6	7



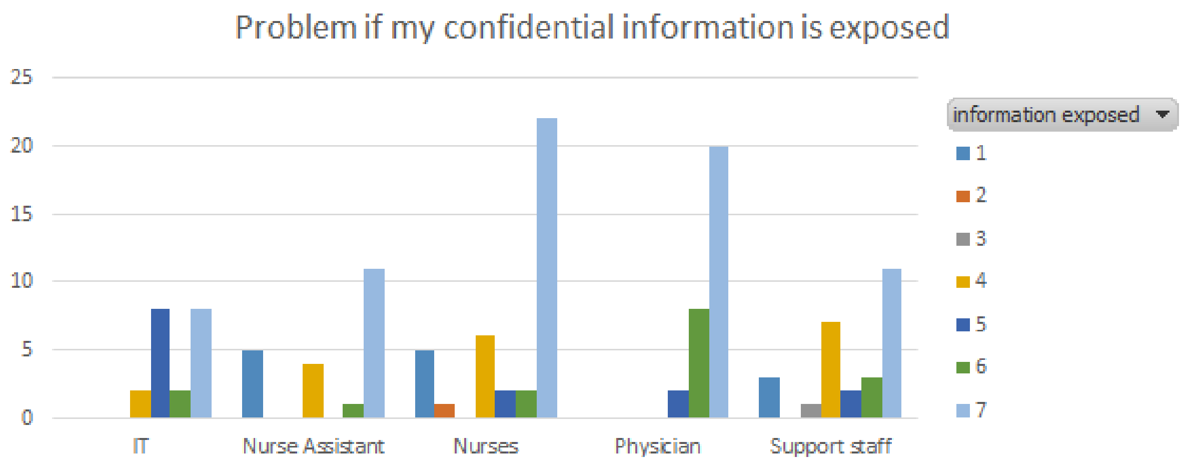
Comments: The responses to this question are more divided. We can resume that as “may or may not” for both the clinical and not clinical users. This is not because they don’t perceive that cyber risks are out there, but they think that the Hospital they work for has a powerful IT system, and tend to think that the cyber security is at the same level.

And It is important to remark that with “security breach” they think about a disrupting event that stops the normal activity of the hospital (Wannacry, …), but not the simple event that can be the origin of that event, like clicking a phishing email and give the password to a hacker. That conclusion can be extracted if we cross the responses of Question 1 and Question 3.

Question 4: It would be a serious problem for me if someone got access to my confidential information without my consent

Responses:

Totally disagree			Neither disagree nor agree			Totally agree
1	2	3	4	5	6	7

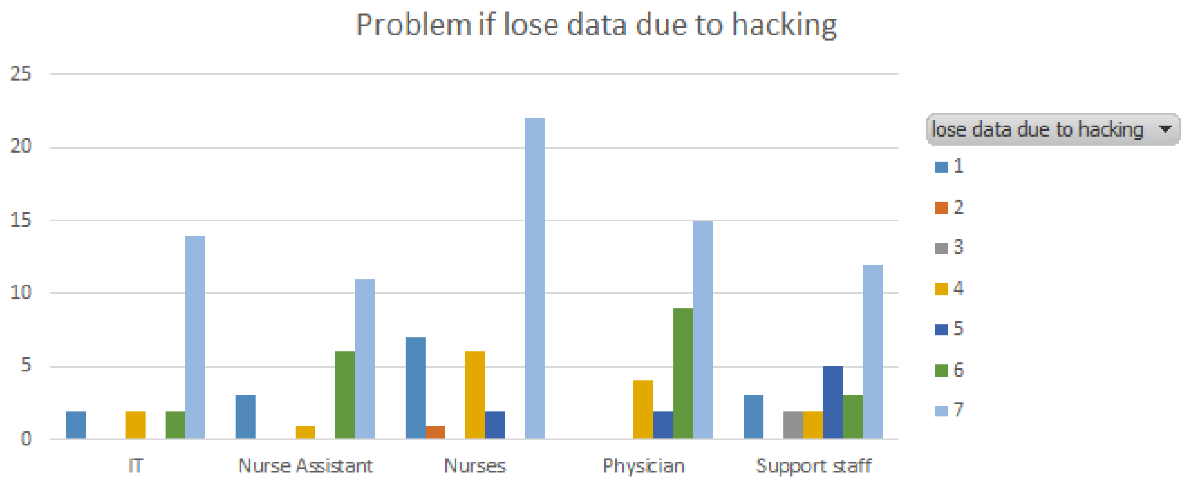


Comments: It's a generalized feeling that It would be a problem the fact that the personal information would get exposed.

Question 5: It would be a serious problem for me if I lose data resulting from hacking

Responses:

Totally disagree			Neither disagree nor agree			Totally agree
1	2	3	4	5	6	7

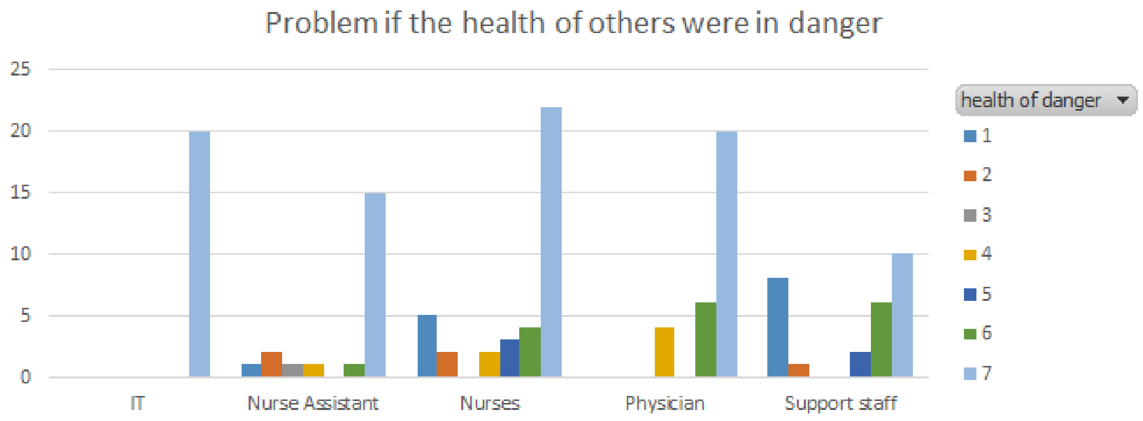


Comments: In the same way as the previous question, users perceive the loss of data as an important problem.

Question 6: It would be a serious problem for me if the health of others were in danger due to a cyber-attack

Responses:

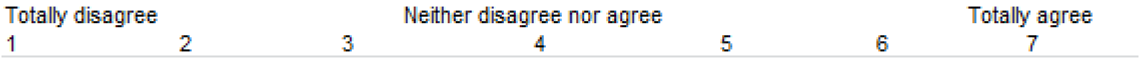
Totally disagree			Neither disagree nor agree			Totally agree
1	2	3	4	5	6	7



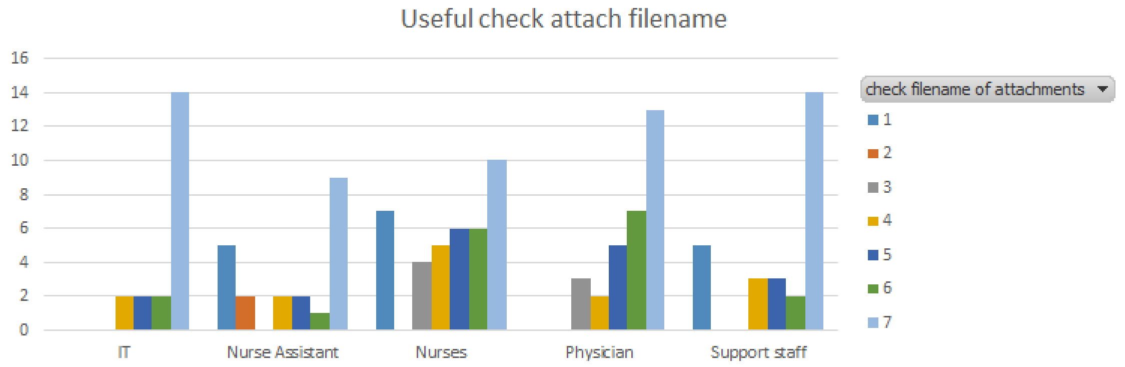
Comments: As expected, expose the safety of patients due to a cyber-attack would be a problem for almost all users from all types.

Question 7: I believe that checking the filename of the emails' attachments is useful

Responses:



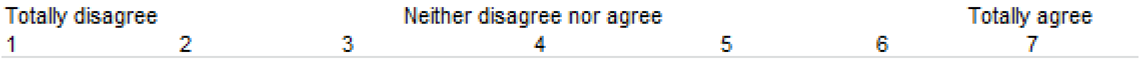
Totally disagree			Neither disagree nor agree			Totally agree
1	2	3	4	5	6	7



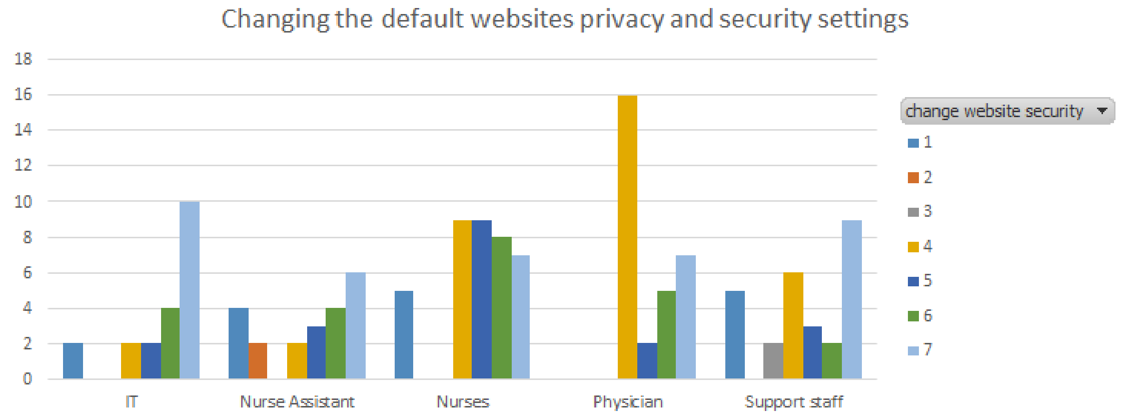
Comments: Checking the names of attachments is the perceived as useful. Only Physicians and nurses groups have a significant percentage of users that don't express clearly this idea.

Question 8: I believe that changing the default privacy and security settings of the website I visit is useful

Responses:



Totally disagree			Neither disagree nor agree			Totally agree
1	2	3	4	5	6	7

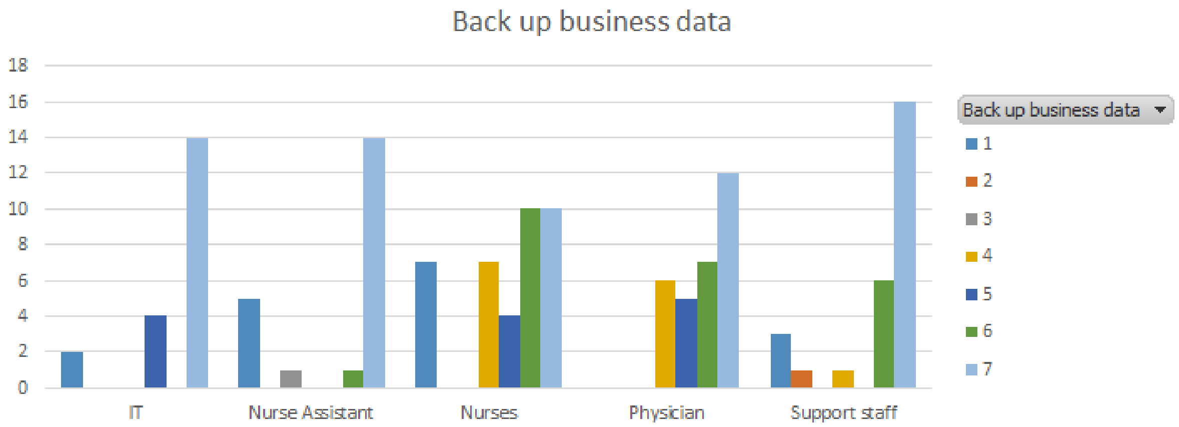


Comments: Despite users can respond as that this action would be useful to protect against cyber risks, it's an action they never perform in their workplace because they are not allowed by the security policies.

Question 9: I believe that backing up business data on business network drives is useful

Responses:

Totally disagree			Neither disagree nor agree			Totally agree
1	2	3	4	5	6	7

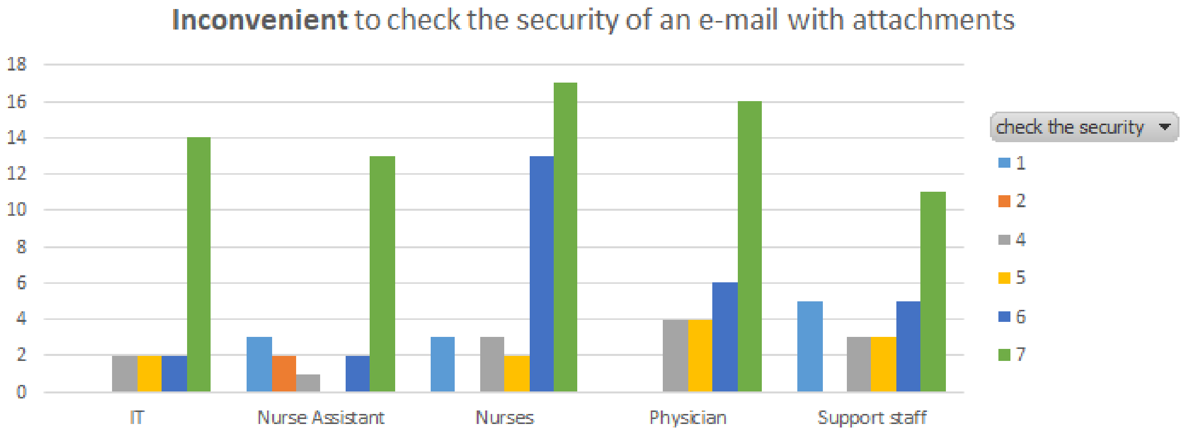


Comments: Backing up business data on business network is a common activity that users perform and so they think is useful. Anyway in Marina Salud patient's data is stored in patient's EMR and so no manual backup is needed, it is done by the backup policies of corporate applications and databases.

Question 10: It is inconvenient to check the security of an e-mail with attachments

Responses:

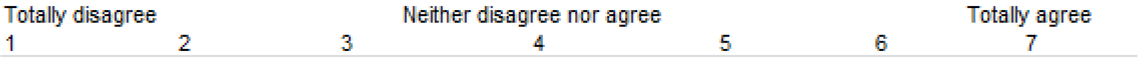
Totally disagree			Neither disagree nor agree			Totally agree
1	2	3	4	5	6	7



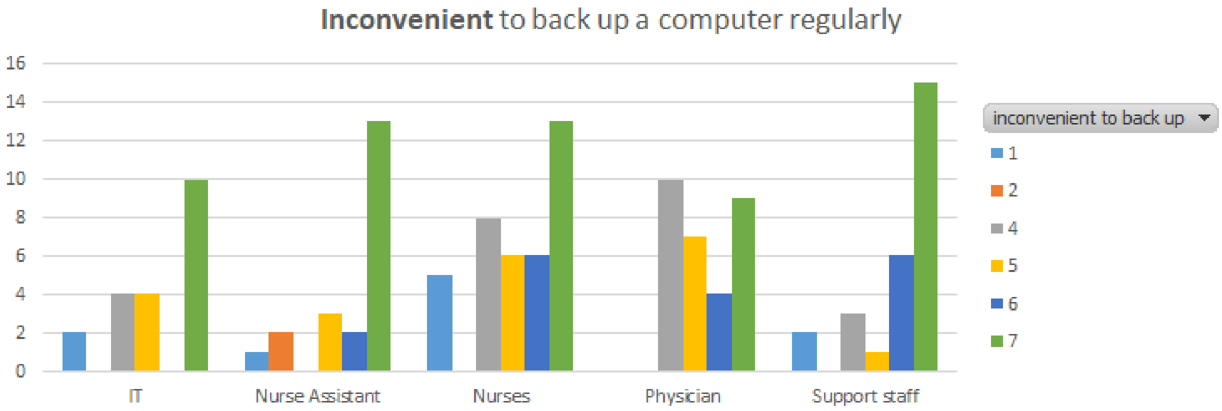
Comments: Almost all users from all groups understand that checking the security of an e-mail with attachments is inconvenient. The reason is that they consider it is an extra task that can slow down their job. They expect that it would be done somehow automatically. It's not the objective of the action what they consider as inconvenient, it's the effort needed to do that.

Question 11: It is inconvenient to back up a computer regularly

Responses:



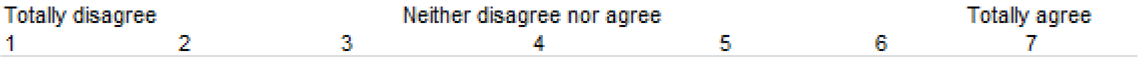
Totally disagree			Neither disagree nor agree			Totally agree
1	2	3	4	5	6	7



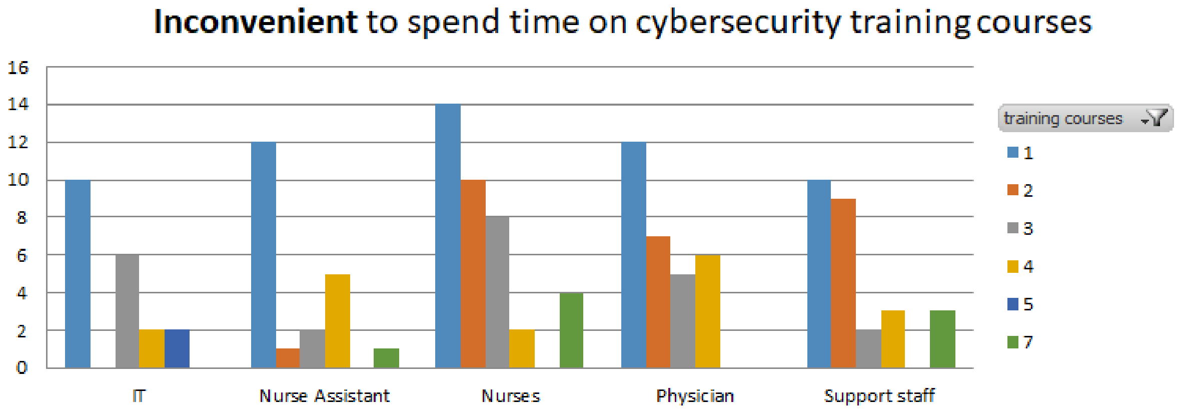
Comments: Almost all users from all groups understand that it is inconvenient to back up a computer regularly. They expect that this regular backup would be done automatically.

Question 12: It is inconvenient to spend time on cybersecurity training courses

Responses:



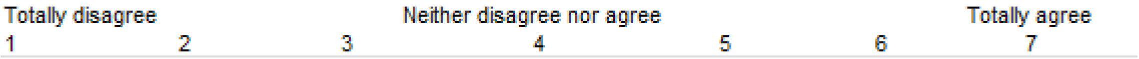
Totally disagree			Neither disagree nor agree			Totally agree
1	2	3	4	5	6	7



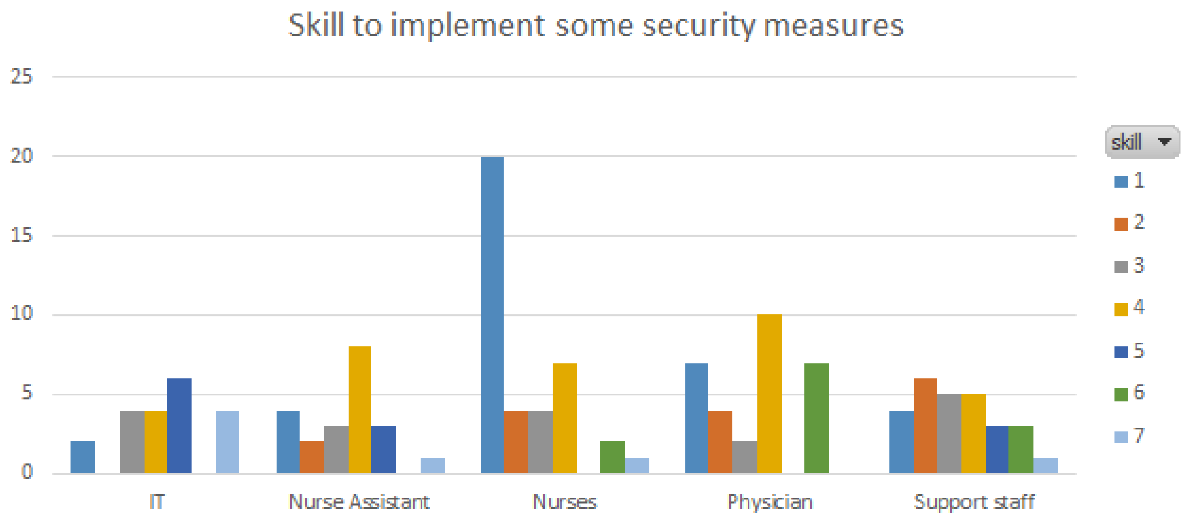
Comments: Most of the users don't see as an inconvenient to spend time in cybersecurity training courses. But some physicians and nurses are more ambiguous, maybe because they think cyber security is not part of their role.

Question 13: I have the skills to implement security measures to stop people from getting my confidential information

Responses:



Totally disagree			Neither disagree nor agree			Totally agree
1	2	3	4	5	6	7

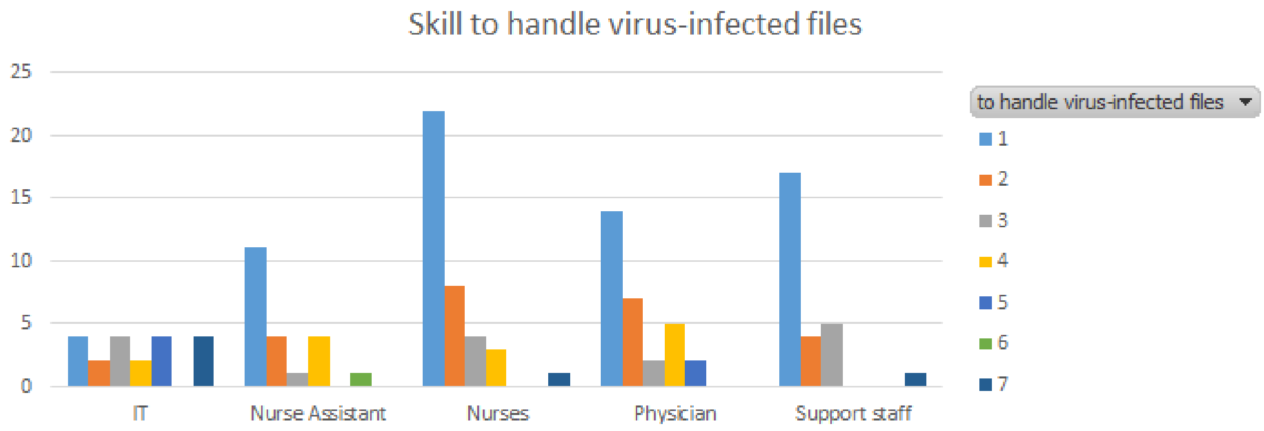


Comments: Users mostly think that they are no able to implement measures that prevent others to access their confidential information.

Question 14: I have the skills to handle virus-infected files

Responses:

Totally disagree			Neither disagree nor agree			Totally agree
1	2	3	4	5	6	7

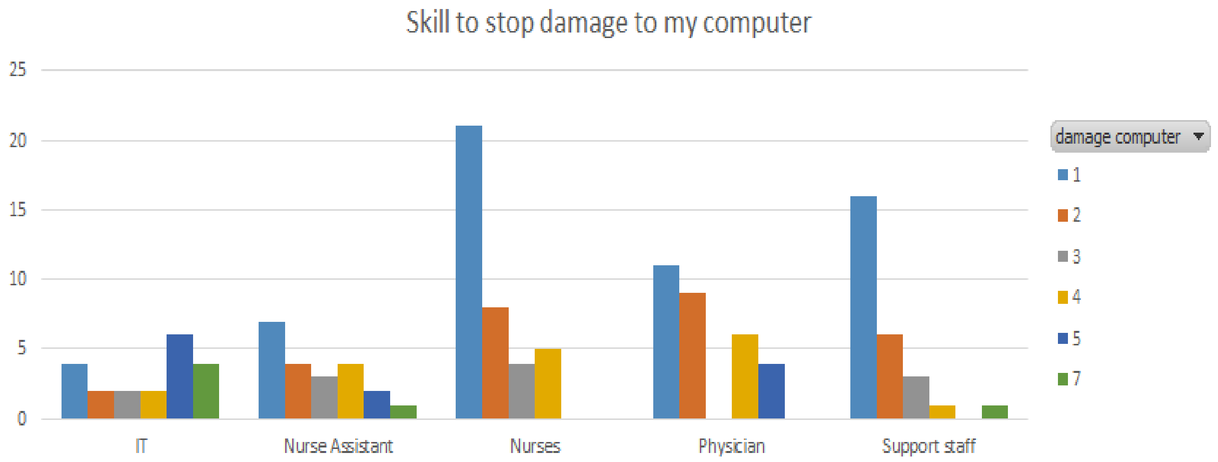


Comments: Most users, even inside the IT department, don’t think they have the correct skill to handle virus-infected files.

Question 15: I have the skills to implement security measures to stop people from damaging my computer

Responses:

Totally disagree			Neither disagree nor agree			Totally agree
1	2	3	4	5	6	7

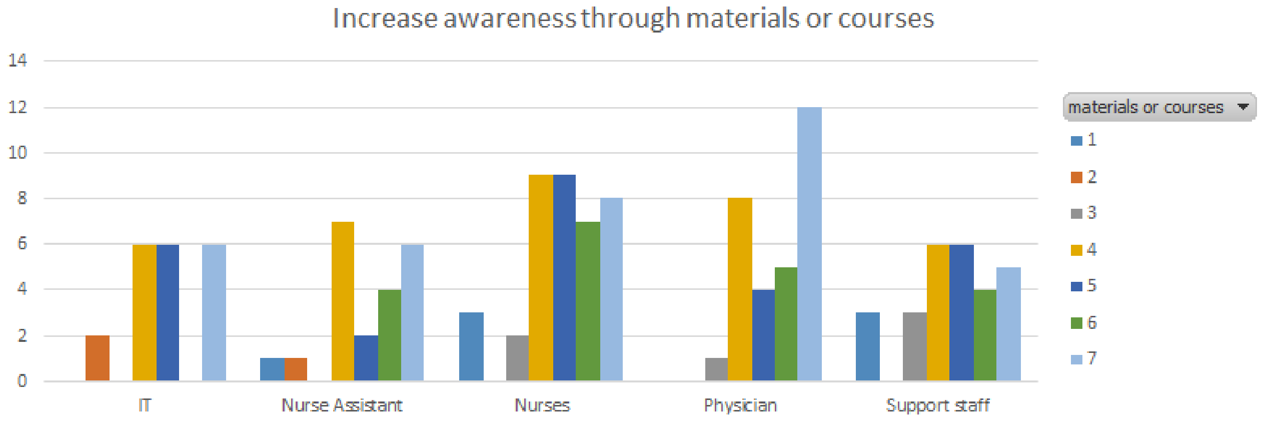


Comments: As expected, the responses pattern follows the previous one, that is, users don’t feel they are able to implement measures that stop others damage their computers.

Question 16: I would be more aware of cybersecurity risks if the Hospital provided me with informative materials or cyber security training courses

Responses:

Totally disagree			Neither disagree nor agree			Totally agree
1	2	3	4	5	6	7

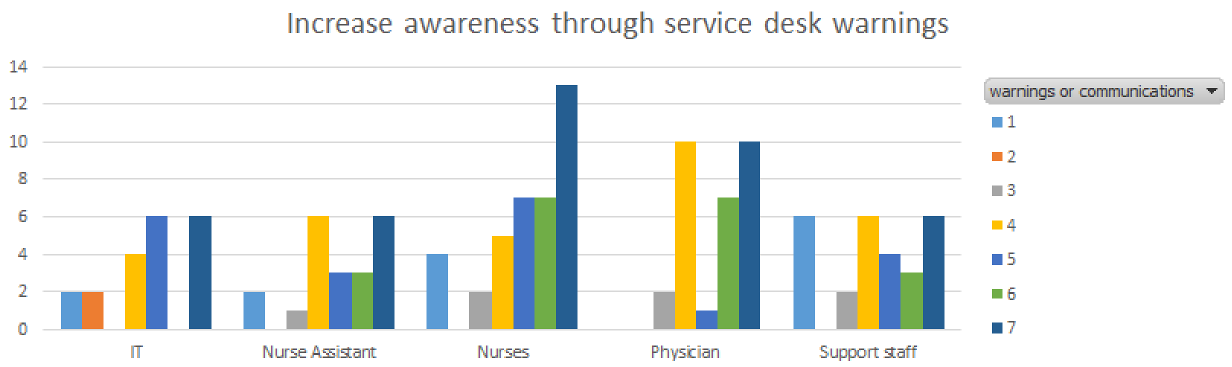


Comments: Users are slightly favourable to the possibility of receiving cyber security education, but the responses have been still quite neutral.

Question 17: I would be more aware of cybersecurity risks if the Hospital's Service Desk sent me warnings or communications on cybersecurity

Responses:

Totally disagree			Neither disagree nor agree			Totally agree
1	2	3	4	5	6	7

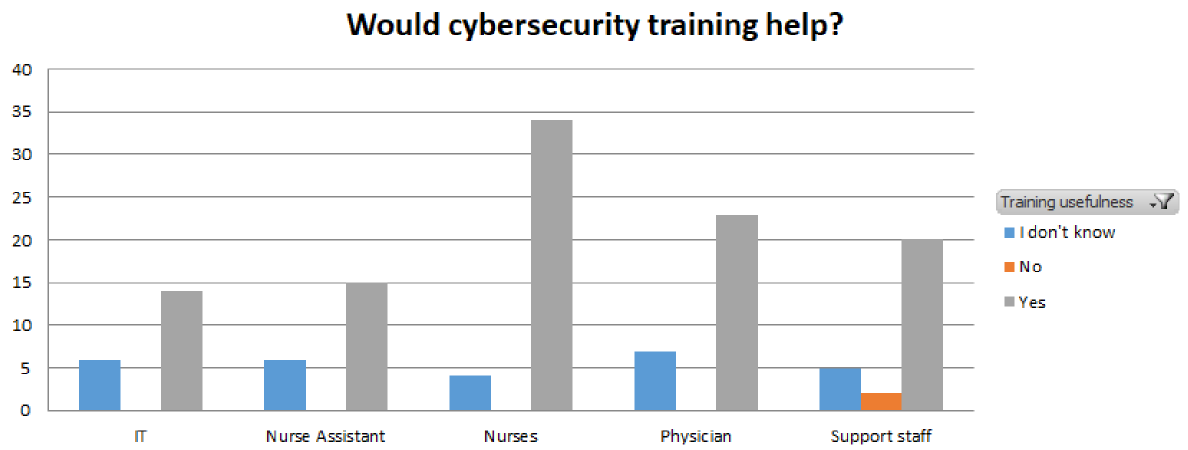


Comments: Users seem to be more receptive to service desk warnings than to specific trainings.

Domain 11: Attitude toward possible training course

Question 1: Do you believe that a cybersecurity training course would help you to prevent and face cyber-attacks?

Responses:

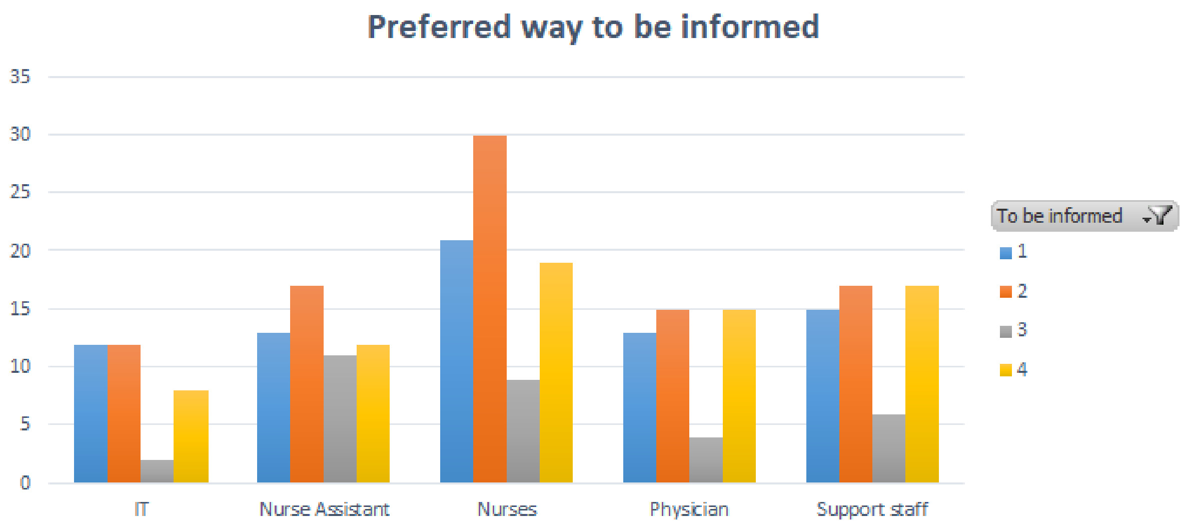


Comments: The response to this question is almost unique: users think that cyber security training would help to prevent cyber-attacks.

Question 2: How would you like to be informed on cybersecurity?

Responses:

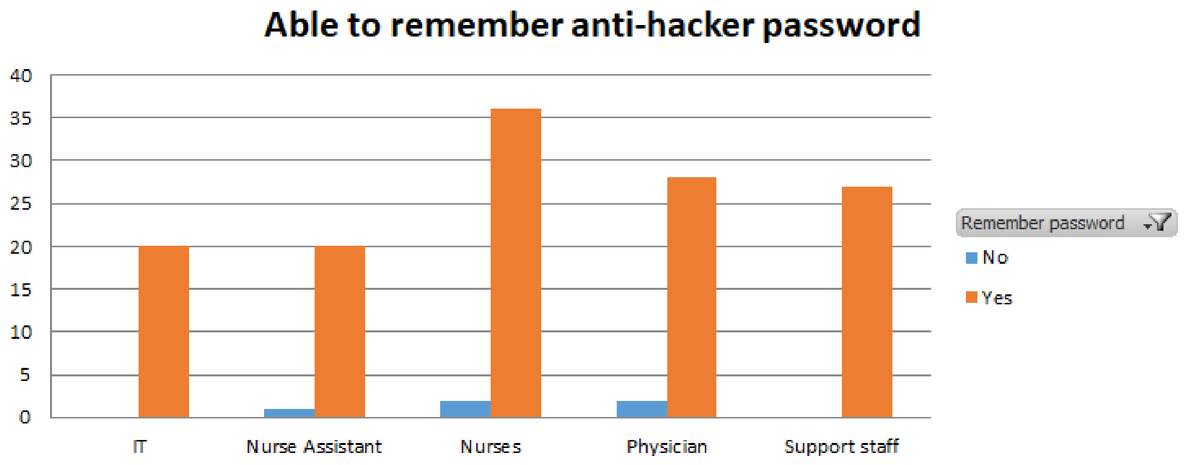
1. Classroom training courses
2. Online training courses
3. Printed informative materials (e.g. poster, flyer, brochure, etc.)
4. Online informative materials (e.g. poster, flyer, brochure, e-mail informative, etc.)



Comments: From the responses we can highlight that the less preferred way to be informed is through printed informative materials. Any of the other options to keep users informed would have a good response, as online or classroom training courses.

Question 3: Can you rewrite your "hacker resistant" password?

Responses:



Comments: Most of users were able to remember the password created previously. As explained before the reason is that the current password policy in Marina Salud constrains users to create these kind of passwords.

ProTego