ProTego Cybersecurity Educational Framework for healthcare organizations

Salvador García Torrens, Vicent Moncho i Mas

Dpto. Sistemas y Tecnologías de la Información. Marina Salud

Abstract.

Often Cybersecurity is mainly approached and tackled from a technical perspective by deploying IT tools to prevent or mitigate the impact of potential attacks. But the human and organizational side of cybersecurity should also be addressed, since the human behavior is the weakest link within the cybersecurity chain and incorrect human behaviors could bypass and invalidate the technical measures deployed [1]. Furthermore, current regulations stated that each organization should put in place the appropriate organizational measures to protect personal data, and this makes even more sense in healthcare since they treat, massively, the most sensitive type of personal data: health data.
In ProTego an educational framework has been designed and deployed that does not only offer such educational material to the final end users (health staff), but also addressed the dissemination strategy to maximize penetration and adherence of the ProTego toolkit. That has been achieved by involving clinical managers in the training activities which is a novel and effective approach.

Besides this, the Protego educational framework has been designed from an holistic approach and also tackled the organizational and regulatory side of the deployment of the technical toolkit, by identifying all the stakeholders involved and offering specific material for each of them, in order to facilitate the toolkit adoption.

1. Introduction

The ProTego project has provided a toolkit for health care organizations to better assess and reduce cybersecurity risks related to remote devices access to Electronic Health Record data, including risks assessment and risks mitigation tools. The ProTego Educational Framework provides tools to raise awareness and educate stakeholders in how they can reduce or prevent risks, and the required information to each stakeholder to assess the ProTego adoption.

This stakeholder education is crucial, especially if we consider non IT personnel, mostly clinical but also administrative. After all, it has been demonstrated that people are the weakest link of an organization's security and they are the most exploited vulnerability by attackers.
Although it is feasible to compose and distribute protocols and work instructions explaining the correct use of the tools and systems from the cybersecurity perspective, the reality is that all those protocols are perceived by health staff as technical material treating technical issues that are, hence, responsibility of the IT department. Furthermore, any protocol or work instructions set cannot cover all existing risks in a changing environment that offers new functionalities every day, such as Bring Your Own Device (BYOD), Internet Of Medical Things (IO(m)T), telemedicine and remote patient care through cloud services. And all under the

mandatory requirement of interoperability that on the one hand allows the existence of a unified EMR whose benefits are out of the scope of this document, but instead offers attack vectors to reach many interconnected systems.
Therefore, the educational framework created in ProTego has as fundamentals the following objectives for each target audience:

- healthcare industry / regulators: to describe the adherence to the cybersecurity standards of the ProTego toolkit. Choosing the NIST CSF [2] as reference the document elicits which items are facilitated by the toolkit.

- healthcare staff and patients: to improve situational awareness of healthcare staff and patients, increasing correct behaviours regarding cybersecurity and making them more receptive to future recommendations or protocols.

- external providers: to explain how to create ProTego compliant applications and services, to take advantage of the features offered by ProTego.

- healthcare IT: to understand the basics of the ProTego toolkit, allowing to assess the ProTego adoption in the healthcare organization, provide the required infrastructure and overview the deployment and management of the toolkit.

2. Scope and structure

The general scope of the educational framework is to provide tools to each stakeholder that contribute to reduce risks and to improve the overall security. The following are the stakeholders identified and its main objectives to reach:

Health staff

Description: This group includes the most of the final users of the corporate applications and devices. They systematically treat sensitive data of patients from interconnected systems. They make use of BYOD strategies introducing risks to the working environment that were caused by behaviors in the private sphere. They don't know all the types of attacks in which they act as potential victims.

Objectives: Raise cybersecurity awareness. Let them know the consequences of incorrect behaviors, even from private context and with their own devices.

Patients

Description: Final users of applications offered from healthcare organizations. Lower impact in the overall security due to restricting permissions, but very low level of cybersecurity awareness. Difficult to make training reach them.

Objectives: Increase situational awareness by reaching them with concrete messages through the limited communication channels.

IT staff

Description: Technical staff with responsibilities in the management of corporate applications and the design and management of the technological infrastructure.

Objectives: Provide enough information to make possible to assess the adoption of the ProTego toolkit. Describe the features and requirements of each component and which would be the tasks they would have to perform to deploy and manage the toolkit.

External providers

Description: External hardware and software providers of healthcare applications and

IO(M)T devices that have historically focused on clinical functionality but less in information security.

Objectives: Describe the requirements for those hw/sw elements to be ProTego compliant, that is, to be able to integrate with ProTego taking advantage of the functionalities that the toolkit offers in fields as authentication, authorization, encryption or real time monitoring.

Regulators

Description: Regulators that may have interest or responsibility derived of the fact that the healthcare organizations accomplish with international cybersecurity standards.

Objectives: Explain to what extent the toolkit is compliant with the standards, helping to perform the controls that those standards recommend.

Based on that, this is the structure of the Educational Framework:

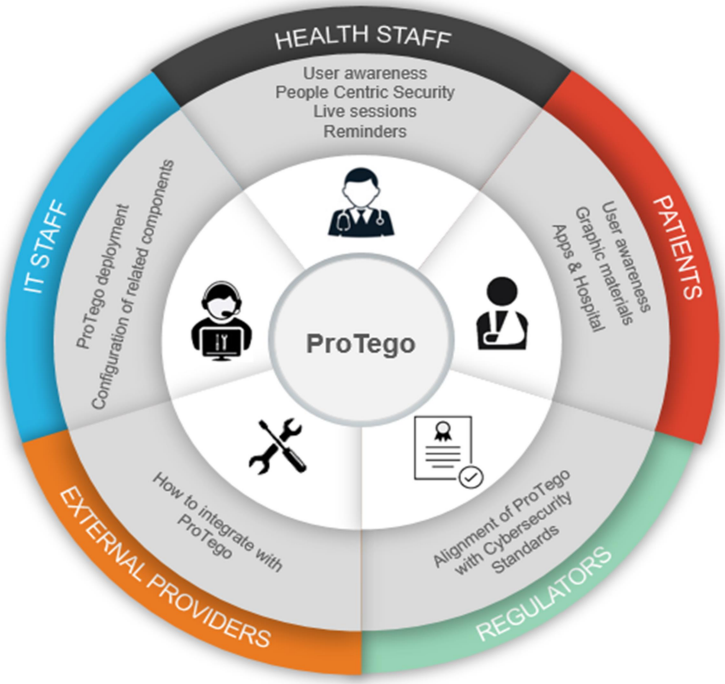

Figure1: Structure of the ProTego Educational Framework

The following sections explain the concrete educational material created for each of them to reach the previously defined objectives.

3. Educational material for Health staff

Educational Material

In the design of the educational material for health staff, the following principles have been observed:

- Designing the right content: selected and covered those contents considered more relevant. Shape the selected contents in a shape that make them easy to consume and understand.
- Demanding the right effort: health staff perceive any issue outside of healthcare as an extra content that should probably not be addressed to clinical personnel. Therefore it is needed to minimize the effort demanded to consume the material.

- Making messages persistent in time: cybersecurity awareness programs should not be a sort of technical training where you are teaching someone about how to do a concrete task to reach a touchable or a least countable objective. This is about impress the necessity of perform correct behaviors. This idea brings up the necessity that the messages transferred become persistent in time.

The final result has been an educational website[3], where the contents have been divided into four main sections:

1. The good employee, covering general topics that hospital employees could face during their normal job activities like not accessing sensitive data through public networks, avoid passwords written or printed in paper, encrypt files containing sensitive data before transmitting them, or avoid the use of unauthorized cloud services to share health data.
2. Safe Passwords, in which the importance of a correct password management is explained. It introduces the concept of password management tools to easy the creation of strong and non-guessable passwords, and the multi-factor identification to increase the level of security. It also highlights the benefits of using different passwords for different services.
3. Social engineering, where it is explained that it is the more used way to overcome security measures put in place. It explains the necessity of ensure the source of any information or digital request, don't follow links included in emails or SMSs, don't attend urgent requests as urgency is a commonly exploited factor from attackers. It also explains that social engineering techniques are becoming most sophisticated and user-oriented, so the awareness and common sense is the main tool to prevent that kind of attacks.
4. Mobile devices, treating the importance of this kind of devices, where everything happens more "under the hood". It is explained the importance of checking the source of apps before installing, and of ensuring the permissions given to a certain app, preventing them having permissions that are out of the scope of its intended functionality. This is an important section because of the BYOD trend, that can make incorrect behaviors in the private scope bring cybersecurity risks to the working sphere.

In each section have been included the following items:

i. A short and easy-to-consult video, as the main item, specifically designed to make it easy to understand for non-technical attenders, and adjusted to three minutes of duration. The videos make use of '*personas*' archietipical users from various groups so not only health staff but any of the employees can feel identified
ii. A printable PDF containing the main tips explained on each video, that can be physically printed and placed as remainder at the workplace
iii. Links to external internet sites where the attender can go deeper on those concepts introduced in the videos. The following table explains the topics covered in links provided for each section

Dissemination strategy

For clinicians in general and physicians in particular it is a proven fact that their perception and understanding of any matter gets better if it is transmitted from a colleague, this is, from another physician. This strategy has been followed in many healthcare organizations by involving clinical key users in relevant IT committees, where they are the receptors of the change requests, prioritize them and communicates to the rest of the health staff. It has been also followed in ProTego, involving the heads of clinical services in the communication strategy, so the final users perceive this awareness program more related to their clinical responsibilities.

This top-down dissemination has been performed in three steps:

1. During a kick-off meeting with the organization managers (CEO level), the IT department presented the awareness training plan to ensure all the resources needed will be available, precisely the engagement of the clinical managers that will collaborate in the dissemination activities.
2. In a second phase, a meeting between the IT department and the clinical managers was arranged. The training plan was presented and explained, asking them to disseminate to the health staff teams under their responsibility during their periodic team meetings.
3. As the third and last phase each clinical manager introduced the training program during the next team meeting, explaining the importance of consuming the provided material and assessing it through the execution of a short survey, available from the educational website.

As a complement posters in paper format has been created and placed in public allocations along the hospital. These posters include a QR code that can be scanned with mobile phones and take the user directly to the educational website, to make easy to access it.

4. Educational material for Patients

The educational material addressed to patients should focus on the improvement of specific cybersecurity behaviors that may overcome technical measures put in place. It should be easy to understand, as no expertise can be assumed for 'patient' architype since it refers to the general population. In this sense, the same educational material designed for the health staff is also appropriate for patients.

But the main handicap about extending cybersecurity awareness education to patients is to find the appropriate ways to reach them.
In the case of the health staff, and as it has been previously explained, the educational program has been introduced by clinical managers. But in the case of patients most of them have fleeting contacts with the healthcare organization and the time is used to give the requested cares and services, with no possibility to place any extra activity.
In this context the way to reach patients should be to introduce them in parallel with the "normal" healthcare activity and allow them to deepen into it by easily accessible contents.
Following this strategy, the posters in paper format has been used as the main tool to reach patients and let them access to the educational material.

5. Educational material for IT staff

The following figure illustrates the location of ProTego in terms of interaction with users and applications:

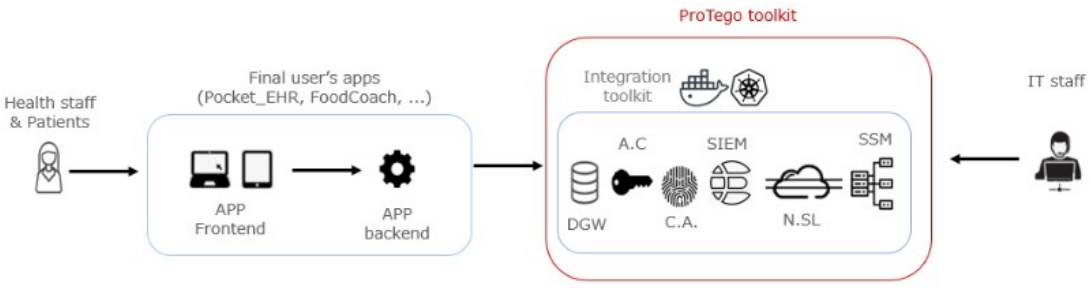

Figure2. User interaction with the ProTego toolkit

Health staff and patients will interact with front-end user applications that will interact with its own backend, and that backend is which will interact with the ProTego toolkit. From this point of view there is no direct interaction between end-users and the ProTego toolkit, and the IT staff could be considered as the end user of the ProTego toolkit since it is the user group that will have direct interaction with it.

IT staff will be the responsible of:

1. Assess ProTego adoption: understand the functionality of the ProTego toolkit and its containing components to assess the suitability of including the ProTego toolkit in the Hospital IT map
2. Provision of requirements: provide the required infrastructure to deploy the ProTego toolkit
3. Deployment of ProTego: deploy and configure the ProTego toolkit
4. Use o ProTego: Manage and use the ProTego toolkit, reacting to the threats raised by the system

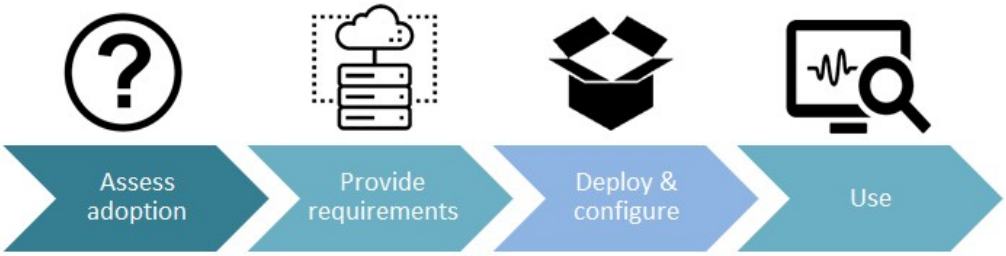

Figure3. Phases for ProTego adoption

The Educational material addressed to the IT staff includes the required information the IT staff would need to preform each of these four main tasks. From the assessment of the toolkit adoption to the provision of IT requirements, deployment tasks and further use of the toolkit. All the information and tasks have been split between the two main personas identified as the main roles participating in those activities:

- IT infrastructure manager
- Network operator

IO(m)T (Internet Of Medical Things) has been also addressed, as it is agreed as a main source of cybersecurity risks for healthcare organizations[4], and health-related data leaks. Aligned with the ENISA[5] procurement guides for medical devices, some concretes guidelines have been depicted, based on three main factors:

- Involve the IT department in the procurement process, allowing technical considerations to be assessed during the decision phase
- Help to understand that integration capabilities of medical devices are relevant for cybersecurity, as they may help to reduce the data silos and prevent isolated systems out of the corporate policies
- Ensure an appropriate maintenance (SLA) including update and protection tasks

6. Educational material for External providers

The ProTego toolkit is a set of components that provide core cybersecurity features to

applications executing over it. In that sense, the application developers need to know how to make use of such features, that is, how to integrate their provided applications with the toolkit.
The toolkit does not offer a single point of integration, but rather allows external applications or devices to be integrated with each of its components. This minimizes incompatibilities since each application or device can "choose" the degree of integration according to its possibilities (architecture, base platform, data model, etc.).

The following points summarize the integration between an external application and the different components of the Protego toolkit:

System security Modeller (SSM): The SSM provides a mean to identify the strength of the external system in terms of cybersecurity. By describing the system the SSM will identify the risks intrinsic to the architecture, and allows assessing the improvements that could be applied by putting in place suggested controls. So, the task for the external provider consist in describe the elements that are part of their system, precisely:

- The applications or processes, describing the functionality they perform, the need of an application server and hardware requirements
- The data assets, describing the data format, sensitivity, need for a database server and intended use.
- The communications between processes and the network requirements

Besides this first description, the external provider must collaborate with the IT staff to find the best possible configuration of the system, identifying the possible controls that each component of the system allows to put in place to lower the intrinsic risks of the provided system.

Data Gateway (GW) + Access Control Framework (AC): The DGW and A.C. components together act as the interface to the data or, in other words, the persistence layer offered by ProTego. They will be considered jointly as it makes no sense to use one without the other. To integrate with it, external providers should avoid using its own persistence layer and make use of them instead.
The basic request flow for an application making use of this is illustrated in the following figure:

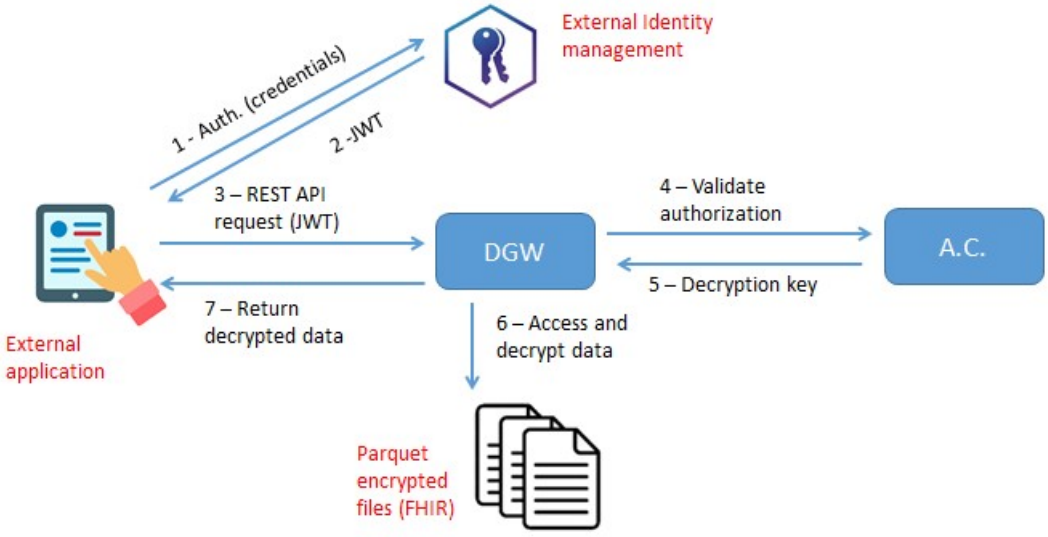

Figure 1: Dataflow for authorization in data access

To make possible such behavior, external providers need to adapt their application to make use of that persistence layer. Precisely:

i. Use JWT as credentials management.

ii. Make use of the external IAM offered by the healthcare organization

iii. Perform data requests through the REST API exposed by the Data Gateway

iv. Ensure the application is FHIR compliant and is able to manage FHIR data objects

The integration with the DGW and the A.C. offers advantages for both the external provider and the healthcare organization:

1. The use of an external IAM prevents the external providers the need of implementing an authentication system, as it has been delegated to an external one.
2. The permissions to access the medical data will be managed by the healthcare organization's IT staff from a centralized point, so the external application will not be impacted if the grant policies change the visibility that each role must have over the data.
3. The external application will no longer need internal data sources, so the external provider will not be asked to provide mechanisms to ensure data safety. As it will reside in an external data source governed by ProTego, the IT staff will be in charge of ensuring the appropriate security measures to that data.

Continuous authentication (C.A.) The C.A. provides a mean of authenticate the person operating a mobile device, that is, ensure that the person operating the device is who it is meant to be. Because of that, its scope is limited to application with mobile frontends installed as mobile applications.
It has two main components:

- C.A. agent, installed in the frontend (mobile device) retrieves behavioral data of the user and sends it to the C.A. API
- C.A. API is the backend component. It builds IA models from the data sent by the C.A. agent and obtains a trustworthiness level of the users.

Therefore, the integration with the C.A. component is constructed at two levels:

1. Frontend: The C.A. agent is a mobile JAVA app that should be installed in the mobile device. The frontend of the external app must integrate whit if by sending the JWT obtained from the IAM once the user has logged in. From this point, the C.A. app must be allowed to collect keyboard data, since this is going to be the source of data used by the C.A. backend to build the IA model and calculate the trust level of the user
2. Backend: The C.A. API is the IA engine. By receiving the behavioral data collected by the A.A. agent, it will periodically rebuild the model for the user, and calculate the trustworthiness level, which will be a value between 0 (total distrust) and 1 (total trust). This value could be requested via a REST API and may be used both by the C.A. agent, to perform any action at the frontend level, or by the external application, to invalidate the user and discontinue the session by expiring user's JWT token and, with that, his possibilities to access the data.

It is worth to mention that the presence of the C.A. can be informed as a control for the "mobile device" kind of elements in the SSM model and it will be considered and will reduce the risk of the system.

The C.A. offers the external providers an extra security layer, not tackled by current mobile apps, to ensure their mobile frontends are used by authenticated users. And also allows detecting fraudulent uses and reacting to avoid further damages. In addition, if the evaluation of the external application is performed taking into account the risk level offered by the SSM, the use of the C.A. will increase the chances of the external application to be approved and adopted.

Security information and event management (SIEM): The SIEM acts as the central risk monitoring point and is the channel through which any threat or risk detected in the external applications will be informed to the IT staff, as responsible to take appropriate response actions. More than that, it is even possible that those potential risks or threats may not be detected by events within the external application and could only be detected by correlation of their logs with those provided by different elements of the IT map.
To perform this surveillance and log correlation, the external providers will be in charge of:

- identify the log sources provided by the application
- describe the type of log sources, so an appropriate SIEM agent could be deployed and connected to the log source to gather the data. As an example, if the application provides its logs in a plain text format, a ”Filebeat” agent should be deployed and connected to the log text file, while if the external application is a cloud application that provides logs via S3 bucket, a WAZUH agent would be the correct one to collect those logs. Apart from this type of integration, the ProTego SIEM covers the possibility that it would the external application who sends the logs to the SIEM, by exposing KAFKA topics that may be used by making use of REST services to send the events (logs) gathered by the application.
- Identify those *patterns* that, if found in the application logs, could lead to discover a potential threat.
- Identify those patterns that, despite may not suppose any threat by themselves, may be risky if combined with certain events in external elements.

Network Slicing (NSL): NSL is the most transparent component of the ProTego toolkit from the perspective of external providers. Its functionality consists on create virtual networks (slices) over the physical network, and provide isolation and appropriate resources allocation to each slice, in a way that an event occurred in one slice will not affect the others, even sharing the same physical infrastructure.
External providers should describe the communications that their applications will perform in terms of origin, destination, ports used and protocols. They will need to describe the required bandwidth allocation as well. From this information, the network operator will create the slices needed and allocate the resources to grant a successful deployment of the external application.

7. Educational material for Regulators

The part of the Educational Framework devoted to regulators is oriented to elicit how the ProTego toolkit is aligned with the cybersecurity standards and facilitates to perform the controls included.
There are two main motivations behind it:

- The cybersecurity standards provide a set of controls widely studied and agreed as appropriate to assess the cybersecurity level of a system.

- The GDPR's recital 81 states: "*The adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller*". In other words, by proving the adherence to a recognized cybersecurity standard, the penalty fees derived from a potential cybersecurity incident may be reduced.

In the Protego Educational Framework the NIST CSF has been selected as the standard regulation to perform the assessment, due to its practical approach and state of development. As a result, it has been stated that the Protego toolkit covers the five different categories the NIST controls is divided into, allowing to perform 18 of the controls included in the standard.

8. Conclusions

The Educational Framework developed in ProTego has been designed from a holistic approach, covering those aspects that can maximize the success of the technical toolkit.

If helps to easy the toolkit adoption by offering the information needed to assess it and also describes how external providers should integrate their applications with the provided toolkit.

It also covers the human behavior that is always a key factor since it can bypass the security technical measures, and finally states the alignment of the toolkit with the cybersecurity standards.

All this has been achieved by identifying the toolkit stakeholders and creating specific content for each of them.

The ProTego Educational Framework can be used as a model of cybersecurity educational frameworks in the healthcare sector.

Acknowledgements: This project has received funding from the European Union's Horizon 2020 Research and Innovation Program under grant agreement No. 826284 (ProTego).

References

[1]Rachid Ait Maalem Lahcen, Bruce Caulkins, Ram Mohapatra & Manish Kumar, https://cybersecurity.springeropen.com/articles/10.1186/s42400-020-00050-w

[2] NIST CSF, https://www.nist.gov/cyberframework/framework

[3] ProTego Educational website, https://protego-project.eu/cybersecurity/

[4] Vihar Soni, https://www.einfochips.com/blog/cybersecurity-of-iomt-devices-what-healthcare-professional-should-know/

[5] ENISA procurement guides, https://www.enisa.europa.eu/publications/report-files/translation-procurement-guidelines-for-cybersecurity-in-hospitals/procurement-guidelines-full-version-es.pdf