Poster Support for an Obeya-like Risk Management Approach

Stéphane Paul[1][0000-0003-2123-5370], Paul Varela[2][0000-0001-9953-5360]

[1] Thales Research & Technology, 91767 Palaiseau, France
[2] Thales SIX GTS FRANCE, 92230 Gennevilliers, France
stephane.paul@thalesgroup.com, paul.varela@thalesgroup.com

Abstract. Lean management is trendy. This trend is also reaching risk management. It has become very concrete in France following the EBIOS-Risk Manager method publication by the French National Agency for cybersecurity (ANSSI) in October 2018. However, if the new method fosters an agile approach of risk management, it does not provide the tools to support the mandated brainstorming workshops. In this paper we propose a set of A0 posters (and A5 cheat-sheets) to support the efficient and user-friendly organisation of the EBIOS-Risk Manager brain-storming sessions. The workshop participants are given sticky notes and felt pens to actively contribute to the data collection work. A facilitator helps organise the emergence of contributions. This approach is inspired from the Japanese Obeya form of project management, with the goal of making risk management simple, dynamic and attractive, or in one word, fun!

Keywords: Risk Management, Agile, Collaborative, Workshops, Brainstorming, Posters, Sticky Notes (Post-Its®), EBIOS.

1 Introduction

In Oct. 2018, the French National Agency for Cybersecurity (ANSSI) published a new version of the EBIOS risk management method called EBIOS-Risk Manager [1]. The first version of the EBIOS method dates back to 1995. It was significantly updated in 2004 and 2010. EBIOS-2010 established itself as the main risk management method used in France. The new version of the method brings some significant changes, amongst which the following:

- It explicitly targets populations beyond the classical cybersecurity experts, including company directorates, risk managers, Chief Information Security Officers (CISOs), Chief Information Officers (CIOs), and business / operational experts, such as Architects (ARCs), Product Line Architects (PLAs), Design Authorities (DAs) and System Engineering Managers (SEMs).
- It mandates securing by conformity, prior to securing by scenario. Securing by conformity means that a Minimal Set of Security Controls (MSSC), based on best

practices, is selected prior to risk identification. Then risks are identified taking into account existing controls. ANSSI’s hypothesis is that accidental events should normally be covered by the MSSCs, so that the analysis can focus on malevolence. In other words, only a few incident scenarios[1] should be necessary, either to prove that the solution is secure, or to highlight some rare holes in the system.

- It is run as a set of ½-day workshops (i.e. brainstorming sessions), with 2 to 4 participants per session.
- It is an agile approach, providing quick results for decision-makers. Typically it is possible to start outputting grosgrain risks after only three workshops, corresponding to 1½ days work. To go in depth, it is possible to iterate on the workshops. It is also recommended to iterate through operational and / or strategical cycles, to keep the system in secure conditions throughout its lifecycle. The operational cycle deals with fast changing facts, e.g. vulnerabilities. The strategic cycle deals with slower changing facts, e.g. system missions.
- It is configurable. It is not required to run all five workshops in sequence. The choice to run a workshop depends on the team objectives.
- Its scope is extended to include the ecosystem, a.k.a. system stakeholders. The assumption here is that many attacks do not target directly the system, but first target a stakeholder (e.g. a sub-contractor), then move laterally.

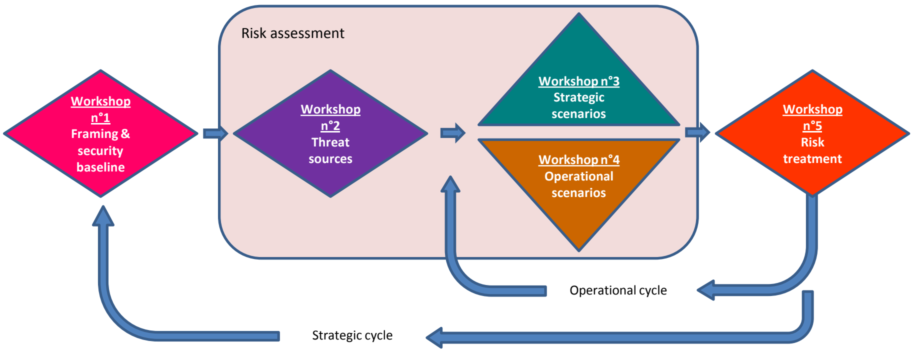


Fig. 1. The five workshops of the EBIOS-Risk Manager method

The novelty of EBIOS-Risk Manager that is of interest to us in this paper relates to the organisation of the risk management work in the form of workshops. The goal of this paper is not to present or promote the EBIOS-Risk Manager method. However, since it is only available in French at the day of writing this paper, we provide some insight and personal translation to allow the reader to understand the relevance of our work. To be brief, let us just say that, as pictured in **Fig. 1**, the EBIOS-Risk Manager method proposes five workshops called: (1) Framing and security baseline; (2) Risk sources; (3) Strategic scenarios; (4) Operational scenarios; and (5) Risk treatment.

[1] According to ISO, an incident scenario is the description of a threat exploiting a certain vulnerability or set of vulnerabilities in an information security incident.

The method specifies the objectives of each workshop, the expected attendees, the expected outputs, and how to proceed. However the guidance is technical in the sense that it typically specifies what data to collect, and how to assess / classify it. The method does not guide on how to organise and conduct the workshop, e.g. how to interact with the participants, collect and document the information, or reach a consensus between the participants.

In this paper, we propose a set of A0 posters (and A5 cheat-sheets) to support the efficient and user-friendly organisation of the EBIOS-Risk Manager brain-storming sessions. A facilitator helps organise the emergence of contributions. This approach is inspired from the Japanese Obeya form of project management, with the goal of making risk management simple, dynamic and attractive, or in one word, fun!

Section 2 describes the content of the different poster templates supporting the five EBIOS-Risk Manager workshops. Section 3 discusses scalability, method efficiency and briefly explains how a final cybersecurity report can be generated following the workshops. The conclusion recalls the history of the creation of the posters, and how their maturity was increased through a series of case studies; we also provide some hints on the way forward. Extensive appendixes provide examples of how the posters have already been used on real live case-studies.

2 A Set of Posters to Support Cybersecurity Risk Identification, Assessment and Treatment

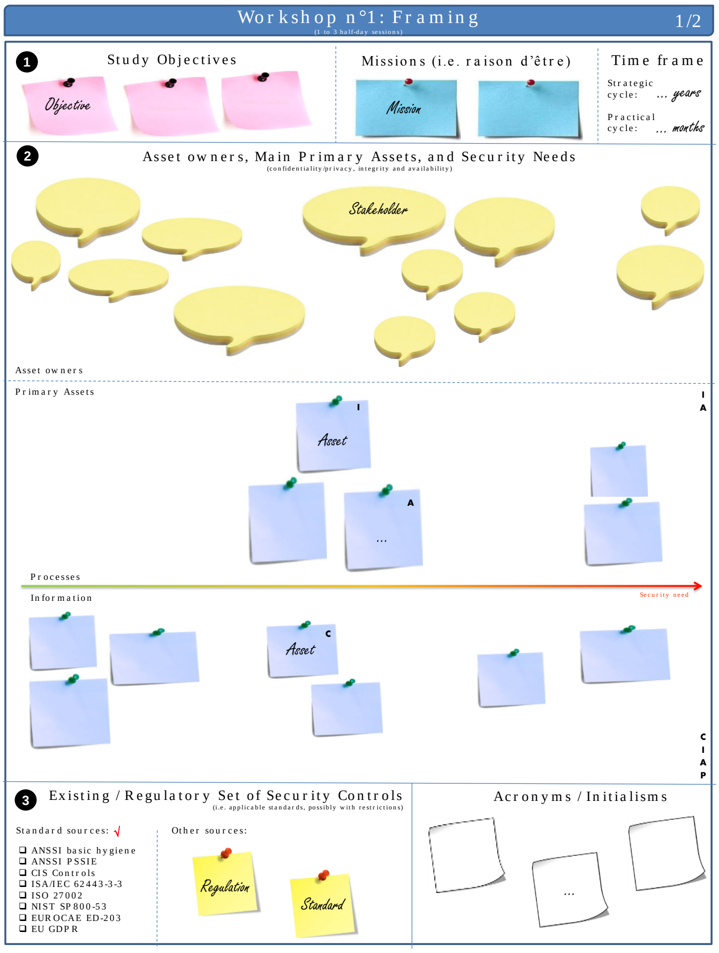
In this section we present our material to organise the EBIOS-Risk Manager [1] brainstorming sessions in a user-friendly way. We will proceed workshop per workshop. However, we start by explaining some organisational elements that are common to all brainstorming sessions.

EBIOS brainstorming sessions typically involve between 2 and 4 persons, in addition or including the facilitator. Each participant is given a single A5 cheat-sheet that recalls the workshop objectives and provides some hints as to how the session is going to be run. Sheets may define terms, scales, small knowledge bases, etc. In practice, we noted that participants spent very little time reading the cheat-sheets. However, the cheat-sheets have a reassuring psychological effect: "*I can always refer to the sheet if I get lost*". The cheat-sheets we developed are not further discussed within this paper.

Filling posters with sticky notes during brainstorming sessions is the most productive part of the work. However, our approach also requires significant back-office work to produce "clean" versions of the posters. By clean, we mean that the hand-written sticky notes collected during the workshop are typed in using PowerPoint. During back-office work, care is taken to place the electronic copies of the sticky notes at the same place as they were set during the workshop, to leverage the visual memory of the participants. In between workshops, the clean poster(s) are sent to the participants by email, for validation. At this stage, feedback is generally very low. This is not an issue because before beginning a workshop, the poster(s) of the previous workshop are submitted for live review. We noted that the reviews classically require no more than 5 to 10 minutes. It is quite frequent that some small amount of corrections and addendums are performed during the reviews. The facilitator responsible for the back-office work may also have spotted some inconsistencies or incompleteness, which he should bring up for discussion during the reviews.

2.1 Workshop n°1: Framing and Security Baseline

Framing and Security Baseline is the first workshop of the EBIOS-Risk Manager method. Its goals are to frame the system-under-study, identify its missions, security needs, and start building a cybersecurity engineering strategy. Its participants should be a top manager, a domain expert, the CISO and the CIO.



Workshop n°1: Framing

(1 to 3 half-day sessions)

1/2

1 Study Objectives

Missions (i.e. raison d'être)

Time frame

Strategic cycle: ... years

Practical cycle: ... months

2 Asset owners, Main Primary Assets, and Security Needs

(confidentiality/privacy, integrity and availability)

Asset owners

Primary Assets

Processes

Information

Security need

3 Existing / Regulatory Set of Security Controls

(i.e. applicable standards, possibly with restrictions)

Standard sources: √

- ❑ ANSSI basic hygiene
- ❑ ANSSI PSSIE
- ❑ CIS Controls
- ❑ ISA/IEC 62443-3-3
- ❑ ISO 27002
- ❑ NIST SP800-53
- ❑ EUROCAE ED-203
- ❑ EU GDPR

Other sources:

Acronyms / Initialisms

Fig. 2. First poster template supporting workshop n°1

The expected outputs are some framing elements, e.g. study objectives, roles and responsibilities, the domain and technical perimeter, including business / operational assets, the feared (a.k.a. undesired) events and their severity, and the Minimal Set of Security Controls (MSSC) to be applied. To support this workshop, we propose two mandatory A0 posters, plus some optional A0 posters. The first poster that we propose is pictured in **Fig. 2**.

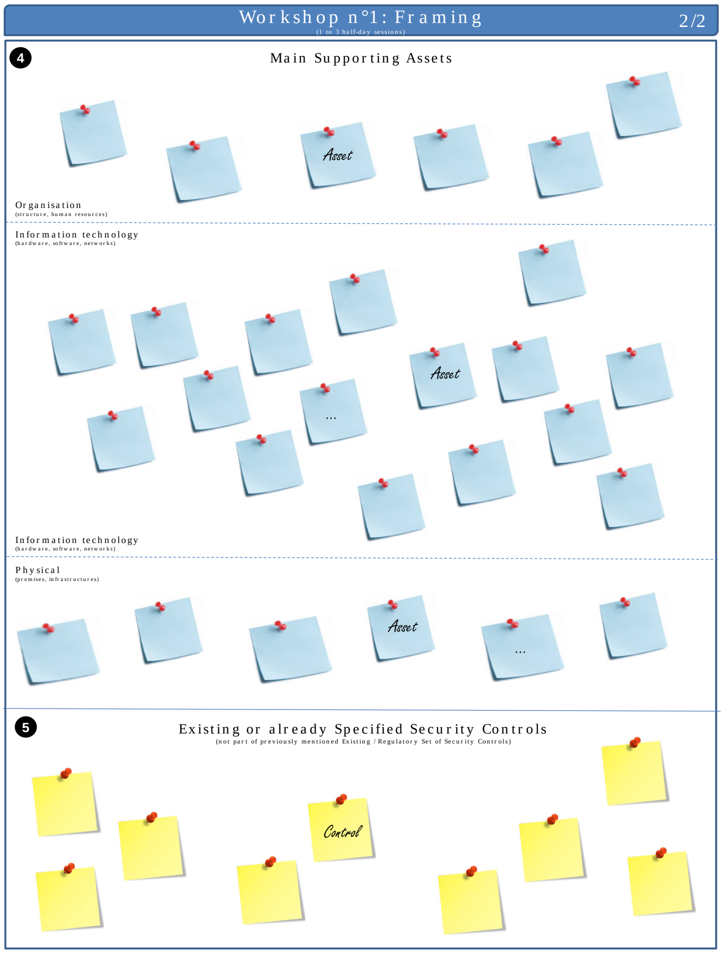
As a first step, the poster allows to capture the study objectives, the missions of the system-under-study and the time frame for the strategic and operational / practical cycles. These cycles refer to the time governing the workshop iterations (cf. **Fig. 1**), to ensure maintenance in secure conditions during the whole system lifecycle.

As a second step, the poster allows to capture the asset owners, primary assets (a.k.a. business or operational assets), and their security needs. The asset owners are represented by comic strip speech bubbles to underline the fact that these stakeholders have their word to say. Blue sticky notes are used for primary assets. They are split in two: processes and information, as defined in ISO 27005 Annex B [2], and arranged on either side of a security need axis. The security need axis is represented by a horizontal arrow whose colour spans from green, meaning low security need, to red, meaning high security need. It can be used as an asset valuation [2]. Above the axis, the area is earmarked for valued processes, below for information. The security needs are usually expressed in terms of Confidentiality (C), Integrity (I) or Availability (A), to which we have added Privacy (P) due to the recent entering in force of the European General Data Protection Regulation (GDPR). We recommend marking the security need by a capital letter on the upper right part of each sticky note.

In practice, we noted that participants care more about the relative position of a sticky note, rather than its absolute position, because it allows setting priorities, so that the risk management process can quickly focus on the most important primary assets. If a primary asset has multiple security needs, but with a different sensitivity for each need, then we recommend the use of multiple sticky notes. E.g., if the integrity and availability need of an information is high, whilst its confidentiality need is low, then two post-is should be created, one with the “IA” marking (for integrity & availability) on the red part of the security need axis, and one with the “C” marking (for confidentiality) on the green part of the security need axis.

As a third and last step, the poster allows capturing the name of security control standard(s) which may be mandated on the study. To ease the capture, some common international standards are already listed, but more can be added. At this stage only the names of the standards are listed. In the next poster, some space is dedicated to listing already existing or specified security controls. Finally, since all businesses come with their specific jargon, space is also given to define some key acronyms or initialisms. A filled example of this poster is given in **Fig. 12** (appendixes).

The second A0 poster that we propose to support the first EBIOS-Risk Manager workshop is pictured in **Fig. 3**. Since this poster follows the previous one (cf. **Fig. 2**), it directly starts with step n°4, as indicated in the black circle at the upper left side of the poster. Step n°4 is dedicated to the identification of supporting assets. The poster offers three areas dedicated respectively to organisational assets (i.e. personal, organisation’s structure), Information Technology assets (i.e. hardware, software, network), and physical assets (i.e. premises and infrastructure) as defined in ISO 27005 Annex B [2]. The fifth and last section of the poster relates to existing or already specified security controls. A filled example of this poster is given in **Fig. 13** (see appendixes).



Workshop n°1: Framing 2/2

(1 to 3 half-day sessions)

4 Main Supporting Assets

Organisation

(structure, human resources)

Information technology

(hardware, software, networks)

Information technology

(hardware, software, networks)

Physical

(premises, infrastructures)

5 Existing or already Specified Security Controls

(not part of previously mentioned Existing / Regulatory Set of Security Controls)

Fig. 3. Second poster template supporting workshop n°1

Some projects may need to assess the implementation status of the different security controls, in particular projects that build on an existing systems or infrastructures. Typically, one may need to assess if the existing and / or specified security controls are currently fully implemented, partially implemented or not implemented. To support this assessment work, we have developed an additional poster presented in **Fig. 11** (see appendixes). Note however that this poster has not yet been used in any real life case-study, so its maturity may be significantly lower than the poster templates presented in this section.

In the above, we have not yet explained how the existing or already specified security controls are defined. In practice, the baseline may be defined by the customer, regulation, standards, engineering best practices, or it may be derived through a process known as *System Security Categorisation* in NIST SP 800-64 [3] and in the Thales Engineering Baseline [4]. To support System Security Categorisation, we propose an optional A0 poster that allows for the assessment of the severity of the impacts of the feared events. This optional poster template is shown in the appendixes, in **Fig. 10**, with a filled in example in **Fig. 14**.

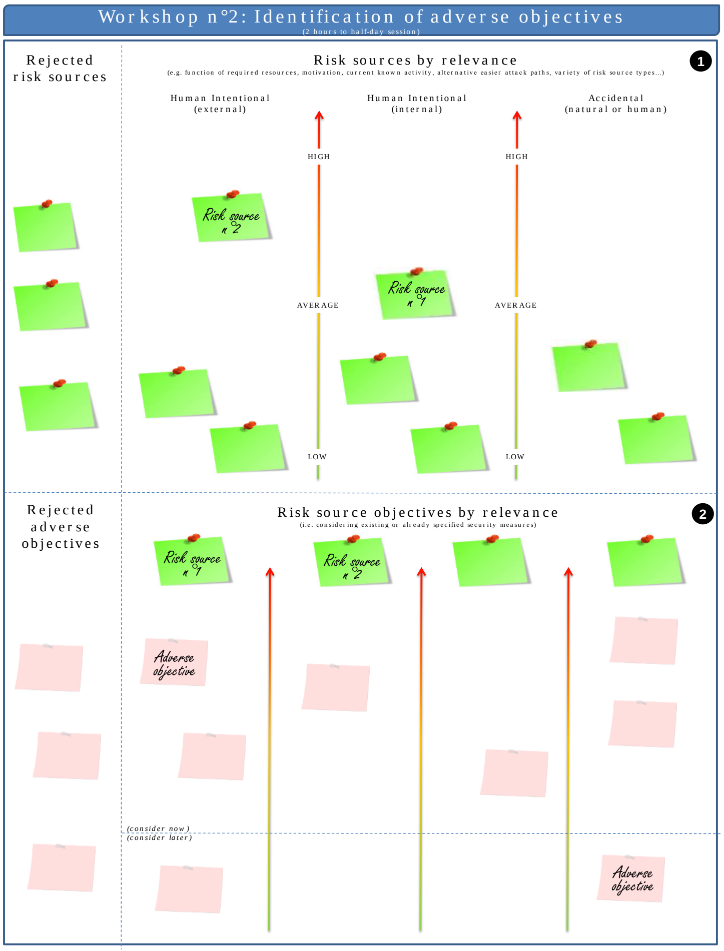
Overall, four A0 poster templates are proposed to support the method's first workshop, of which two poster templates are optional.

2.2 Workshop n°2: Risk Sources

The second workshop of the EBIOS-Risk Manager method is called Risk Sources. Its goals are to identify who or what may jeopardise the primary assets identified during the previous workshop, and to what ends. Its participants should be a top manager, a domain expert, the CISO and, if possible, a Threat Intelligence (TI) expert. The expected output is a prioritised map of the risk sources, and their objectives. To support this workshop, we propose a single A0 poster, presented **Fig. 4**.

As a first step, the poster allows to capture risk sources (green sticky notes), classified as: (i) intentional external; (ii) intentional internal; (iii) accidental, whether human or natural, internal or external to the system-under-study. The risk sources can be sorted by relevance, where relevance is generally assessed taking into account resources available to the risk source, the risk source motivation and its activity history (i.e. precedents). A column on the far left, allows for the capture of rejected risk sources.

As a second step, the most relevant risk sources are selected and repeated using green sticky notes on the lower part of the poster. Below each risk source are represented associated adverse objectives. Once again, the objectives can be sorted by relevance. A dashed horizontal line cuts through the area dedicated to the adverse objectives. All adverse objectives above that line will be studied in the following workshops; the study of the adverse objectives below the dashed horizontal line will be delayed until the next risk management cycle. The leftmost column allows for the capture of rejected adverse objectives. A filled example of this poster is provided in **Fig. 16**. If more than four risk sources need to be considered, we propose a poster extension (see **Fig. 15**). In terms of scalability, the method recommends dealing with an average of 3 to 6 adverse objectives per cycle, so as to keep it manageable during brainstorming.



Workshop n°2: Identification of adverse objectives

(2 hours to half-day session)

Rejected risk sources

Risk sources by relevance

(e.g. function of required resources, motivation, current known activity, alternative easier attack paths, variety of risk source types...)

1

Human Intentional (external)

Human Intentional (internal)

Accidental (natural or human)

HIGH

AVERAGE

LOW

Rejected adverse objectives

Risk source objectives by relevance

(i.e. considering existing or already specified security measures)

2

(consider now)

(consider later)

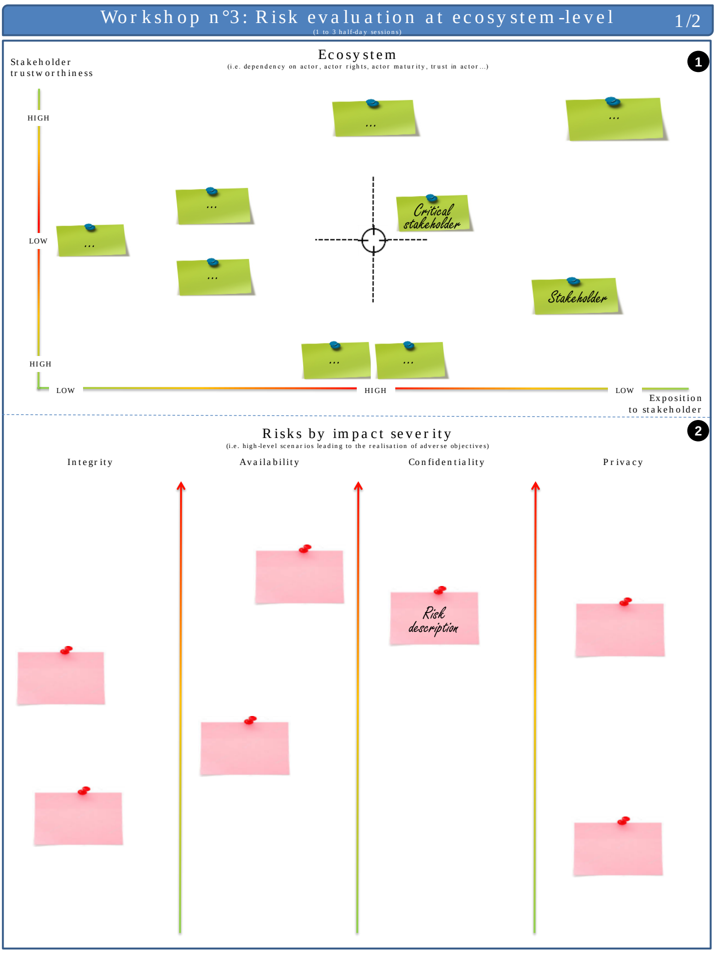
Fig. 4. Poster template supporting workshop n°2

2.3 Workshop n°3: Strategic Scenarios

The goal of the third workshop is to describe high-level scenarios stating how the previously identified risk sources (cf. §2.2) can attack the system-under-study. ANSSI asserts that a significant part of cybersecurity attacks do not target the system directly, but first target some system stakeholder, and then move laterally to attack the system. Thus, before describing strategic scenarios, EBIOS-Risk Manager mandates the mapping of the ecosystem, i.e. external stakeholders interacting with the system-under-study, and the identification of critical stakeholders, i.e. those most likely to be targeted by a risk source. The workshop participants should be a domain expert, an architect, the CISO and, if possible, a cybersecurity expert. The expected outputs are a mapping of the ecosystem, a list of critical stakeholders, a prioritized list of strategic scenarios and a proposal of complementary security controls. Feared events may also be studied during this workshop if they were not studied during workshop n°1.

To support this workshop, we propose two mandatory A0 posters, plus one optional A0 poster. The workshop n°3 optional poster is identical to the workshop n°1 optional poster (cf. **Fig. 10** and **Fig. 14**), to allow for the assessment of the severity of the impacts of the feared events. It is therefore not further discussed herein.

In terms of wording, we have introduced the term *risk* instead of the EBIOS *strategic scenario* expression. It is our feeling that this is a more natural concept for non-cybersecurity experts, and up to now, the case-studies that we have run have not shown any distortion due to this wording simplification.



Workshop n°3: Risk evaluation at ecosystem-level 1/2

(1 to 3 half-day sessions)

Ecosystem

(i.e. dependency on actor, actor rights, actor maturity, trust in actor...)

Risks by impact severity

(i.e. high-level scenarios leading to the realisation of adverse objectives)

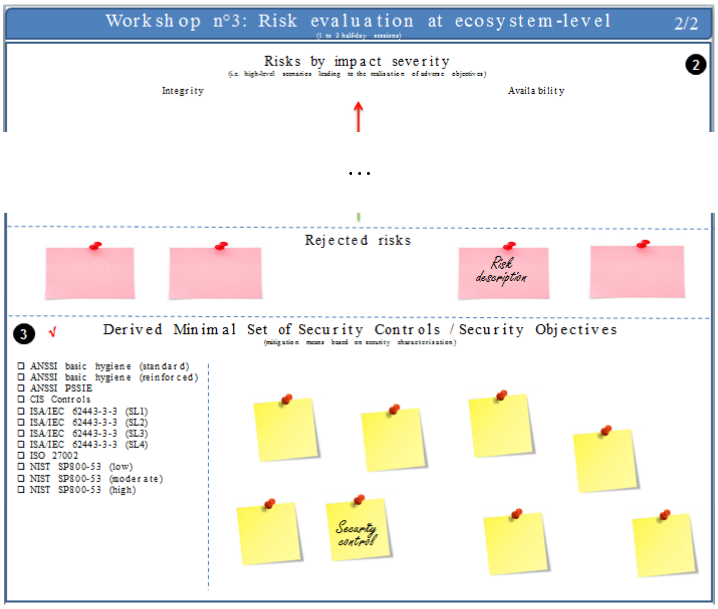
Fig. 5. First poster template supporting workshop n°3

The first poster template that we propose is pictured in **Fig. 5**. The top part of the poster is dedicated to the mapping of the ecosystem. The schema presents two scales:

(a) horizontally, the scale relates to the system's exposition to the stakeholder; (b) vertically, the scale relates to the trustworthiness of the stakeholder. Initially, the schema is a bit difficult to get used to because the axes are bidirectional. This complex layout, which was recommended to us by ANSSI, has several ergonomic advantages: the stakeholders who are untrustworthy and to which the system is significantly exposed are pictured in the *centre of the diagram*. Naturally they are at the *centre of attention*. Hopefully such stakeholders should be scarce. A filled example of this poster is provided in **Fig. 18**.

In terms of colour, we reused the green colour to capture the ecosystem. This colour is similar to the colour used for the risk sources during workshop n°2. We do not mean by that that the ecosystem should be considered as risk sources but we do mean that those stakeholders are potential threat actors used by a risk source to perform the attack. The difference between threat source (a.k.a. risk source) and threat actor is well captured in the HMG IA standard [5] [6].

The lower part of the poster (cf. **Fig. 5**) is used to capture high-level descriptions of the risks. Pink sticky notes are used here once again, as it was done for the risk source objectives in workshop n°2 (cf. §2.2). Indeed, the risks described herein are possible attack paths, which describe how the risk sources will proceed to reach their objective(s), at a high level. The facilitator should make sure that at least one scenario is described for each adverse objective identified during the previous workshop.



Workshop n°3: Risk evaluation at ecosystem-level 2/2
(1 to 3 half-day sessions)

2 Risks by impact severity
(i.e. high-level scenarios leading to the realisation of adverse objectives)

…

Rejected risks

3 √ Derived Minimal Set of Security Controls / Security Objectives
(mitigation means based on security characterisation)

- ☐ ANSSI basic hygiene (standard)
- ☐ ANSSI basic hygiene (reinforced)
- ☐ ANSSI PSSIE
- ☐ CIS Controls
- ☐ ISA/IEC 62443-3-3 (SL1)
- ☐ ISA/IEC 62443-3-3 (SL2)
- ☐ ISA/IEC 62443-3-3 (SL3)
- ☐ ISA/IEC 62443-3-3 (SL4)
- ☐ ISO 27002
- ☐ NIST SP800-53 (low)
- ☐ NIST SP800-53 (moderate)
- ☐ NIST SP800-53 (high)

Fig. 6. Second poster template supporting workshop n°3(cropped)

In this diagram, the high-level risk descriptions are sorted by impact severity, according to a vertical severity axis, from low impact severity at the bottom and in green, to high severity at the top and in red. As for the previous diagrams, it is again a relative positioning that is important, in order for the risk assessment team to rapidly focus on the most severe risks. A filled example of this poster is given in **Fig. 18**.

The second poster template supporting workshop n°3 (**Fig. 6**) extends the previous poster (the upper part, similar to the previous poster, was cropped out), and also allows for the capture of rejected risks. Capturing rejections asserts that those risks were considered, and not simply forgotten.

Normally risk descriptions will be rather extensive: for this section, we recommend large sticky notes. In the follow-up, risks can be numbered, and referred to by their number. A special sheet has been prepared to serve as risk register (cf. **Fig. 17**).

Finally, the lower part of the poster supports the last step of the EBIOS-Risk Manager workshop n°3, i.e. the identification of additional security controls to deal with intrinsic vulnerabilities of critical stakeholders. As in workshop n°1, yellow sticky notes are used to capture the security measures. And here again, the poster template presented in **Fig. 11** (see appendixes) can be used to assess the implementation status of the ecosystem-related security controls.

2.4 Workshop n°4: Operational Scenarios

The goals of the fourth workshop are to describe *how* the strategic scenarios will be realised, using an ad-hoc version of the Lockheed Martin Cyber Kill Chain® [7], and assess their likelihood. Thus, this workshop requires a good knowledge of the supporting assets (as captured during workshop n°1) and their vulnerabilities. The workshop participants should be the CISO, the CIO and preferably, a cybersecurity expert. The expected output is a list of operational scenarios with their likelihood of occurrence. To support this workshop, we propose an A0 poster template to capture the cyber kill-chains (cf. **Fig. 7**), plus another poster to synthetize the risks. This last poster is in fact shared between workshops n°4 and n°5, the top part being filled in during workshop n°4, and the bottom part during workshop n°5.

The poster template to capture the cyber kill-chains is one of our most complex posters, but when the brainstorming participants reach this workshop, they have become familiar with the poster principles; none of the participants we had on our case-studies seemed destabilised by the poster complexity.

The main structuring element of the poster is an ad-hoc version of the Lockheed Martin Cyber Kill Chain® comprising 5 steps, instead of the 7 steps of the original version. As step representation we used a symbol resembling the *task definition* icon standardised in SPEM [8]. Our 5 steps are: (i) External reconnaissance; (ii) Intrusion; (iii) Internal reconnaissance; (iv) Move laterally; and (v) Exploitation. The general idea is that the brainstorm participants detail the way an attacker can achieve his objective going through the five steps listed above. This description should at least encompass (from top-down on the poster):

- The system mode, because an attack scenario depends on the system's state and mode. E.g., an attack which is possible during system development will probably not be possible during system operation. A specific space is earmarked above the Cyber Kill Chain to capture this system mode information.

- The estimated likelihood of the scenario. This poster shows the likelihood captured as a cumulative percentage just below the Cyber Kill Chain, but it is of course possible to use a qualitative scale instead, leveraging a colour-coding mechanism.
- The risk source or risk actor involved in each part of the attack scenario. They are captured using green coloured sticky notes.
- The existing security controls that may prevent the attack from happening, protect against it, or detect and respond to the attack. Existing security controls are captured using yellow coloured sticky notes located above the attack scenario description.
- The description of the attack scenario itself. E.g., reverse-engineering hardware equipment, then installing a root kit. This is done using red coloured sticky notes.

The detailed descriptions provided on this poster should correspond to at least one high level risk description captured during workshop n°3. To establish the link, the reference to the high level risk description is recalled on the upper left part of the poster, using a pink sticky note.

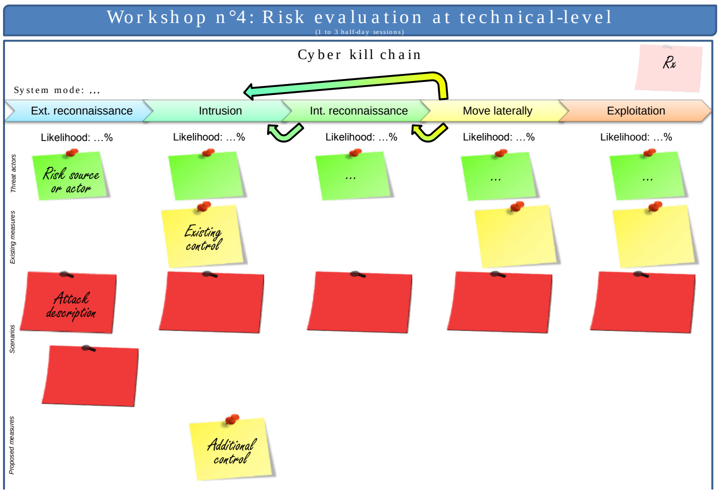


Fig. 7. Poster template to support capturing cyber kill-chains, workshop n°4 (cropped)

According to the EBIOS-Risk Manager method, risk treatment is performed during workshop n°5. However, when we run this workshop for our case-studies, we witnessed a natural behaviour of the participants to immediately provide countermeasures. Thinking about an attack scenario is a strenuous mental activity. Splitting the work in a description activity during workshop n°4, followed by a treatment activity during workshop n°5 is inefficient and mentally exhausting. We therefore extended our poster to allow for the capture of additional security measures, which will eventually be reviewed during the risk treatment workshop (n°5). The additional security measures are captured using yellow coloured sticky notes located below the attack scenario description. At this stage, these additional security measures are obviously not (yet) taken into consideration when computing the scenario likelihood. The Cyber

Kill Chain poster template should be used as often as required to describe all relevant attack scenarios. The work mandated by the EBIOS-Risk Manager method stops here for workshop n°4. A filled example of this poster is given in **Fig. 19** (appendixes).

From our perspective, we feel that it is important to conclude this workshop by a synthesis of the inherent (a.k.a. initial) risks – whereas it is part of workshop n°5 according to the EBIOS method. The reason for our position is that at this stage we have both the severity and the likelihood of the scenarios, allowing for the positioning of the risks on a risk aversion matrix. To support this synthesis of inherent risks, we propose a new poster, illustrated in **Fig. 8**.

This poster is split in two identical sector representations. Each schema presents two scales: (a) horizontally, the risk likelihood scale; (b) vertically, the risk severity scale. During this workshop, we only fill in the top part of the poster, related to inherent risks. During the next workshop, dedicated to risk treatment, we will synthetize the residual risks. The poster will then offer a comprehensive view of risks, before and after treatment.

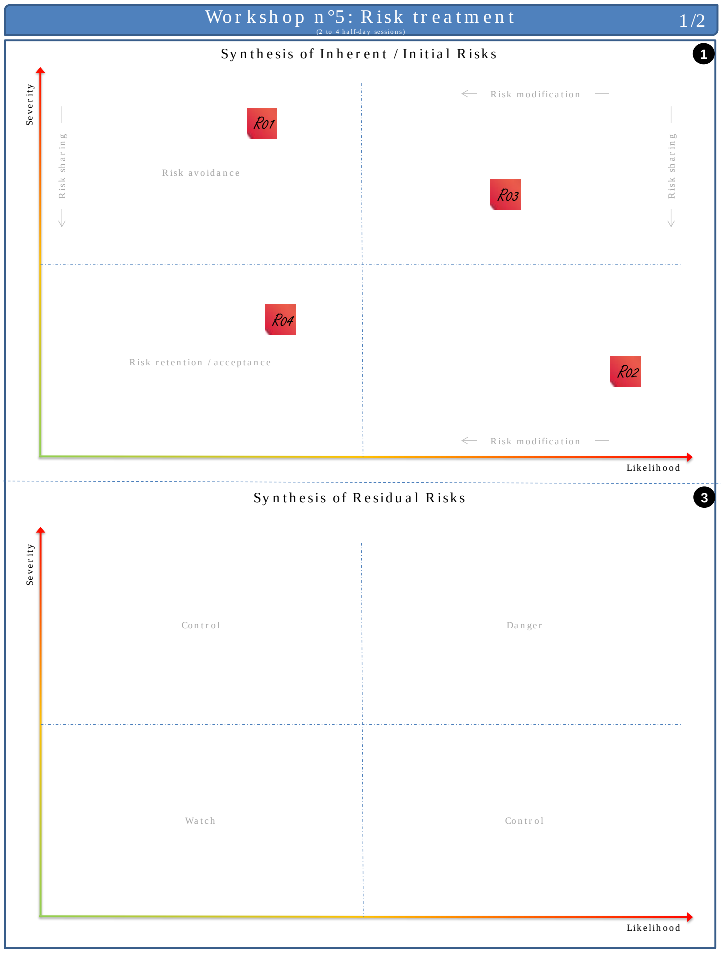

Workshop n°5: Risk treatment
(2 to 4 half-day sessions)
1/2

Fig. 8. Poster template to capture the synthesis of inherent & residual risks (workshops 4 & 5)

To help beginners, the poster also provides risk management hints, in support of workshop n°5. For example, on the top part, the most obvious risk treatment options are listed within the different sectors. Typically, if a risk is very likely and severe, one should essentially consider risk modification, to reduce risk likelihood, or risk sharing to reduce risk severity. By contrast, if the risk is in the bottom-left part of the diagram, one should probably consider risk acceptance / retention.

2.5 Workshop n°5: Risk Treatment

The objectives of workshop n°5, called Risk Treatment, are to synthetize the inherent risks, define a risk treatment strategy, derive the corresponding security measures, integrating them in a continuous improvement plan, and assess / manage the residual risks.

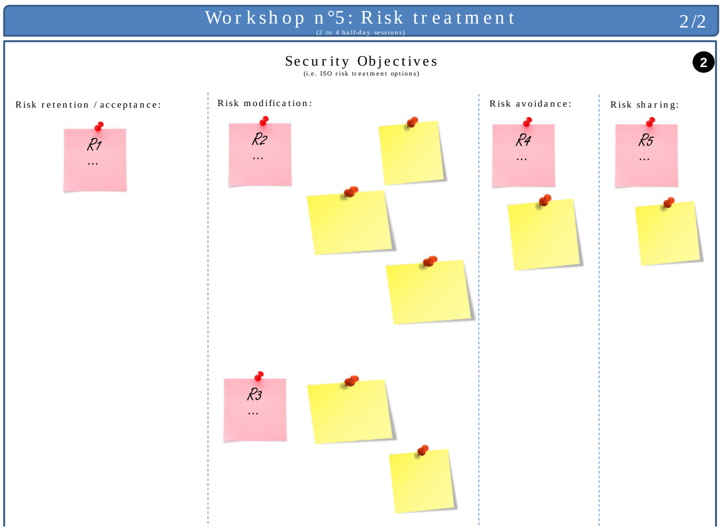

Workshop n°5: Risk treatment
(2 to 4 half-day sessions)
2/2
Security Objectives
(i.e. ISO risk treatment options)
2
Risk retention / acceptance:
Risk modification:
Risk avoidance:
Risk sharing:
R1
...
R2
...
R3
...
R4
...
R5
...

Fig. 9. Poster template to support risk treatment as part of workshop n°5 (cropped)

The workshop participants should be, as for workshop n°1, a top manager, a domain expert, the CISO and the CIO. To support this activity, we propose a final A0 poster dedicated to risk treatment (cf. **Fig. 9**). The synthesis of residual risks is performed on the poster already presented as part of workshop n°4, cf. **Fig. 8**.

Our poster proposal for risk treatment is pretty straightforward. It simply presents four columns, corresponding to the four risk treatment options proposed in ISO 27005 [2], i.e. risk retention / acceptance, risk modification, risk avoidance, and risk sharing. In each column, we propose to reference a risk scenario, using a pink or red sticky note, and then, except for the risk retention option, list the proposed additional security measures, using yellow sticky notes. A filled example of this poster is given in **Fig. 20**.

Risk treatment involves cost-benefit analysis for different risk treatments. To make rational decisions, one may for example need to know what insurance policies are available on the market for the particular identified risks. As workshops are rather short, a thorough economic analysis of treatment alternatives is not feasible during the allotted time; it must be prepared in advance. This statement is also valid for all previous workshops: the brainstorming and poster-based approach is not a magical wand. To be efficient, the workshops need to be prepared and relevant data collected beforehand.

3 Discussion

3.1 Scalability

Our approach is meant to be use during the project bid phase and / or during the early development phases of the project. During the early development phases of the project, the brainstorming sessions can be organised with or without customer representatives, possibly both, thus exercising two iterations.

The approach has obvious limitations in terms of scalability. To start with, the posters offer a limited surface to stick sticky notes. Next, people in brainstorming sessions can only take so much information at a time. This is clearly intrinsic to the method. For example, for workshop n°2, ANSSI suggests to limit the number for selected threat source objectives to something between 3 and 6. Finally, as the complexity grows, the back office work grows to disproportionate amounts, typically to print and manipulate the A0 posters.

Thus, our recommendation is to realise one or two iterations with this approach, to gain a collaborative momentum and establish a high-level consensus on the risk management priorities and, then switch to more traditional software tools. ANSSI has launched an accreditation process for tool vendors: eight French companies and one Dutch company have already registered [9]. It will therefore not be a problem to find a computer tool to edit the collected data in a more formal framework.

3.2 Methodological evaluation

It is difficult for us to objectively discuss the efficiency of the method, as it is rare that people run two parallel risk assessments on real industrial programmes, just to compare the results.

However, in our case, our interlocutors on the VLLAM / UTM case-study (see section 6.1) had already run a cybersecurity risk assessment with the Thales Digital Factory. The feedback we collected is that our approach was interesting in that is really addressed the business value, by contrast with the work done with the Thales Digital Factory, which was much more technical.

3.3 Final Report Generation

All the posters presented above have been design under PowerPoint using a set a fonts that allow for acceptable legibility during a workshop, when printed in A0 format, and acceptable legibility for individual reading, in A4 format. Thus, when all the posters resulting from the workshops have been edited electronically, it is possible to generate a final cybersecurity report by printing the PowerPoint file. Our workshop participants found it easy to review the documents because the data was presented in the report in exactly the same way as it was during the workshop.

In addition to the posters themselves, we have added a cover page, and a conclusion page to the PowerPoint file. The conclusion page is the sole *text-only* page of the document: it summarizes the results and recalls the names of the workshop participants, their affiliation and role in the study. As a reference, the report generated for our SCADA IoT case-study is 16 pages in length, cover and conclusion pages included.

4 Conclusion

Lean management is trendy. This also concerns risk management, in particular in France, with the recent publication of the EBIOS-Risk Manager method by the French National Agency for Cybersecurity. However, if the new method fosters an agile approach of risk management, it does not provide the tools to support the mandated brainstorming workshops. In this paper we have proposed an innovative set of A0 posters to support the collection of risk management information during brainstorming workshops. By using these posters on a Thales internal cybersecurity course and on two real business case-studies, we have developed the optimal number and the content of each poster, bringing them to a level of maturity that is compliant with operational business cases. We have noticed during those case-studies that risk management using this technique is fun. It is a way of demystifying risk management, making it easier to understand, whilst remaining highly time-efficient. This format is especially appropriate during bid activities, or project kick-off. It also fosters a collaborative state of mind, recalling that system architecture securing is not the sole business of cybersecurity experts, but the result of a collaborative work involving the management, domain experts, the CISO and CIO.

On the posters, the allocated space for an activity, the scale axes, the positions and colours of sticky notes have all been fine-tuned to allow for the efficient capture of information, and also convey some subconscious messages and links between different bits of data. For example, if there is no more space to put your sticky note, then it is maybe time to move forward with the next activity, leaving whatever you still wanted to add for the next iteration.

We are currently promoting this set of posters for use in Thales by our Business Units as a possible tooling of the EBIOS-Risk Manager method. Our aim is to use this set of posters to support at least a first round of risk identification, assessment and treatment. Our case-studies show that initial results can be obtained after only 3 to 6 workshops of 2 hours each. Iterations can then be run anew to go in more depth.

Beyond Thales internal uses, our poster templates will be made available to anyone requesting them under a Creative Commons CC BY-NC-SA licence.

We are fully aware that this approach will probably not scale to very large studies, on which the completeness and consistency of the risk management data need to be checked by electronic means. Beyond some 15 posters, the back office works becomes unacceptable. However, even on large studies, we believe that it is possible to start the study using this poster-based approach, to gain a momentum and community adherence to the risk management process, and then shift to some EBIOS compatible electronic software tool, like for example the RiskOversee products [10], to document the complete architecture, specific vulnerabilities and detailed attack scenarios.

As way forward, we are also considering the porting of this approach on a visual management tool, like iObeya© [11] or Framemo [12]. This improvement should allow for electronic sticky note support, decreasing the amount of back office work, and proposing a dynamic way of adjusting the layout regarding the workshop context. It should even be possible to use dedicated tactile screens to improve the user experience. An electronic visual management tool would also bring the possibility to perform this workshop remotely. However, we will be careful that electronic tooling does not override the intellectual approach and the dynamics of human collaboration. The licencing costs may also be an issue with some electronic sticky notes commercial frameworks.

We plan to continue to mature our approach on additional Thales internal case-studies, and on the upcoming H2020 Foresight research project (due to start in September 2019).

5 References

[1] ANSSI, "EBIOS Risk Manager, version 1.0 (in French)," Agence Nationale de la Sécurité des Systèmes d'Information, Paris, 2018.

[2] ISO/IEC 27005, "Information technology — Security techniques — Information security risk management," International Organization for Standardization / International Electrotechnical Commission, Geneva, 2018.

[3] NIST SP800-64r2, "Security Considerations in the System Development Life Cycle," National Institute of Standards and Technology, Gaithersburg, 2008.

[4] 87210647-DDQ-GRP-EN, "Cybersecurity Engineering Guide (commercial-in-confidence)," Thales Chorus 2.0, 31/01/2018.

[5] CESG, "HMG IA Standard Numbers 1 & 2, Information Risk Management," National Technical Authority for Information Assurance, Cheltenham, Gloucestershire, UK, 2012.

[6] CESG, "HMG IA Standard Numbers 1 & 2 – Supplement, Technical Risk Assessment and Risk Treatment," National Technical Authority for Information Assurance, Cheltenham, Gloucestershire, UK, 2012.

[7] Lockheed Martin, "The Cyber Kill Chain," [Online]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. [Accessed 06 03 2019].

[8] OMG, "Software & Systems Process Engineering Metamodel (SPEM)," Object Management Group, 2008.

[9] ANSSI, "EBIOS Risk Manager Accrediation: Tools to support Cybersecurity Risk Management (in French only)," 2019. [Online]. Available: https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/label-ebios-risk-manager-des-outils-pour-faciliter-le-management-du-risque-numerique/. [Accessed 16 05 2019].

[10] RiskOversee, "Tool-up your EBIOS analysis," ALL4TEC, 2019. [Online].

Available: https://www.riskoversee.com/en/cyber-architect-en/. [Accessed 16 05 2019].

[11] KapIt, “Digital Visual Management for Lean & Agile companies,” [Online]. Available: https://www.iobeya.com/. [Accessed 22 03 2019].

[12] Framasoft, “Framemo,” 22 03 2019. [Online]. Available: https://framemo.org/demo.

[13] IEC 62443-3-3, “Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels,” International Electrotechnical Commission, 2013.

[14] IEC 62443, “Industrial communication networks - Network and system security,” Industrial Automation and Control System Security Committee of the International Society for Automation (ISA).

[15] NIST SP 800-53, “Security and Privacy Controls for Federal Information Systems Federal Information Systems, Special Publication 800-53, Revision 4,” National Institute of Standards and Technology, Gaithersburg, 2013.

[16] DMD-TC, “WAEA Specification 0395, Content Delivery for In-Flight Entertainment,” Digital Media Distribution Technical Committee of the World Airline Entertainment Association Technology Committee (WAEA-TC), Virginia, USA, 2001.

6 Appendixes

These appendixes provide the template of some posters which were only rapidly discussed in the main part of this paper, as well as multiple examples of filled in posters from two case-studies. To allow for a better understanding of the posters, we first provide an overview of the two case-studies.

6.1 Overview of the Case-Studies

The A0 posters were designed and validated using a running example of a Thales internal cybersecurity course and two real business case-studies. These case-studies are presented below.

IFE case-study. The In-Flight Entertainment (IFE) case-study was constructed for a Thales Learning Hub (TLH) adult professional training course on cybersecurity. Therefore, by contrast to the other two case-studies, the IFE case-study does not claim to provide a comprehensive framing of the system. This case is a toy case built to support educational goals.

According to the specifications given in the cybersecurity course, the IFE must provide free games, music and films to the airline passengers. “Free” means that there is neither credit card nor financial issues. The scope limited to games, music and films means that there are no connections with the avionics (and thereof limited safety-related issues), and no connections to the internet. It is therefore a very basic IFE. There is however a performance requirement: IFE availability should be above 99%.

VLLAM / UTM case-study. The poster templates presented in this paper were used to run a Very Low Level Airspace Management (VLLAM) and Unmanned Traffic Management (UTM) case-study. This case-study, run during the first semester of 2018, was very useful to raise the maturity of the workshop n°1 to workshop n°3 poster templates. Indeed, the workshops 1 to 3 were run twice: once for the overall system of systems, and once for the geofencing capability. The outputs of this case-study are not shown in this paper.

SCADA IoT case-study. Thales Ground Transportation intends to introduce Internet of Things (IoT) devices in its Metro Supervisory Control And Data Acquisition (SCADA) system. This obviously raises some questions about IoT cybersecurity. This case-study, run during the second semester of 2018, was very useful to raise the maturity of the workshop n°4 and workshop n°5 poster templates. The results of this case-study are extensively showed in the appendixes of this paper.

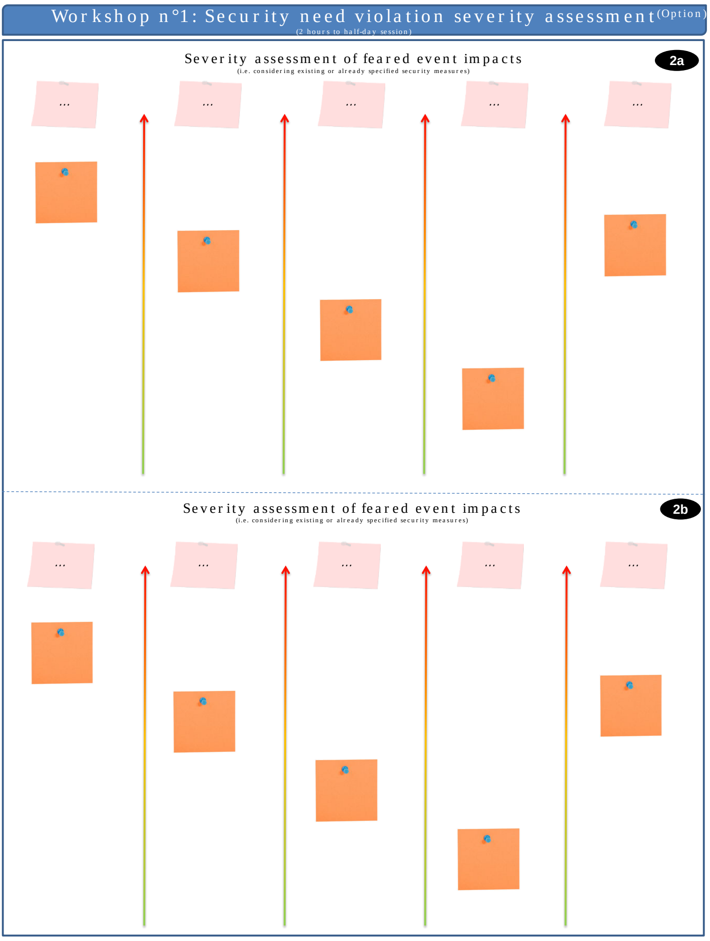
6.2 A bit more about logistics

As mentioned in the core part of this paper, EBIOS brainstorming sessions typically involve between 2 and 4 persons, in addition or including the facilitator. When paper versions of posters are used, this means that the sessions can (and should) be organised in relatively small rooms, with at least one wall where posters can be hanged, at a reasonable distance (i.e. 2 to 4 metres) from the workshop participants.

Before each session, the facilitator should hang the set of A0 posters required for the session (see next sections for details), and distribute to each participant: (i) a single A5 cheat-sheet that recalls the workshop objectives and provides some hints as to how the session is going to be run; some cheat-sheets also provide tips, or knowledge bases, such as a list of classical threat sources; (ii) a set of colour sticky notes; the choice of colours depends on the workshop, as explained in the core part of this paper; and (iii) a felt pen; we recommend a different colour felt pen per participant, so that it authenticates the contributor; we also recommend a medium-sized felt pen tip, so that the writing remains readable up to a distance of 4 metres.

6.3 Complementary Poster Templates in support of Workshop n°1

A feared event is the negation of a security need on a primary asset. The proposed poster template allows for the study of up to ten feared events, represented by the pink sticky notes. Below the feared events, the impacts of the event may be listed, using orange sticky notes, against a severity scale represented by a vertical arrow, spanning from low severity (in green) to high severity (in red). As for the security need scale on the first poster (cf. **Fig. 2**), it is important to capture here the relative severity of the impacts, rather than their absolute severity value. **Fig. 14** shows an extract of this poster filled in for the IFE case-study.



Workshop n°1: Security need violation severity assessment(Option)

(2 hours to half-day session)

Severity assessment of feared event impacts

(i.e. considering existing or already specified security measures)

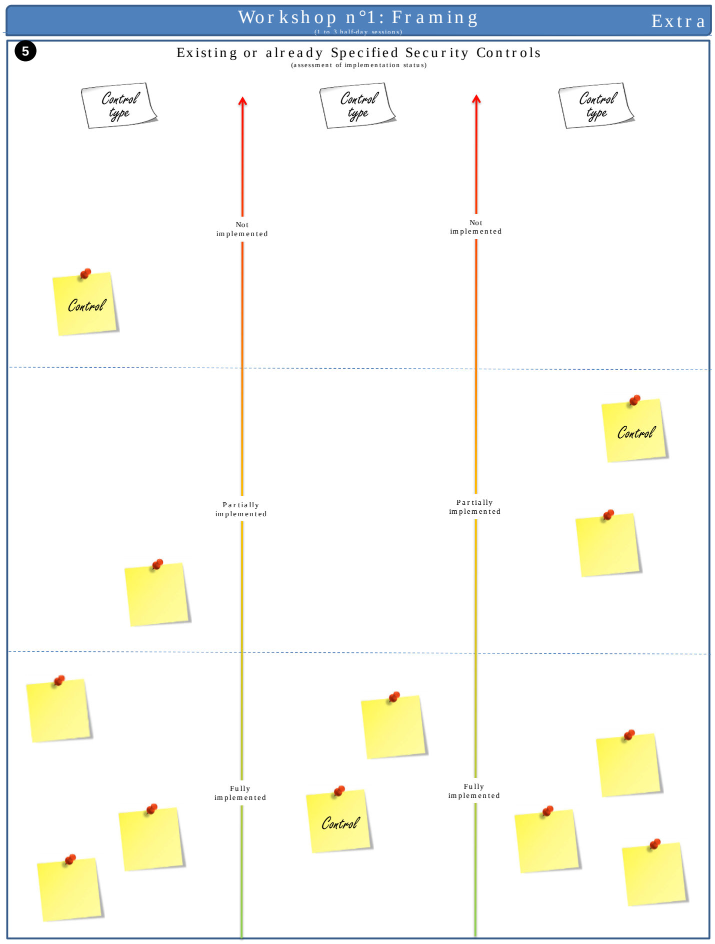
Severity assessment of feared event impacts

(i.e. considering existing or already specified security measures)

Fig. 10. Poster template for the severity assessment of feared events

The poster template in **Fig. 11** supports the assessment of the implementation status of security controls. The poster is split in three sections corresponding to fully implemented controls, partially implemented controls and controls not implemented (from bottom-up).

In addition, the poster is split in three columns to allow for the classification of security controls. Thus, one would need three poster instances to cover the 7 families of functional requirements defined in IEC 62443-3-3 [13]… but we do not recommend dealing with too many details with the poster-based approach. An exhaustive analysis of hundreds of security controls will best be managed using some dedicated electronic tool.



Workshop n°1: Framing

(1 to 3 half-day sessions)

Extra

5 Existing or already Specified Security Controls

(assessment of implementation status)

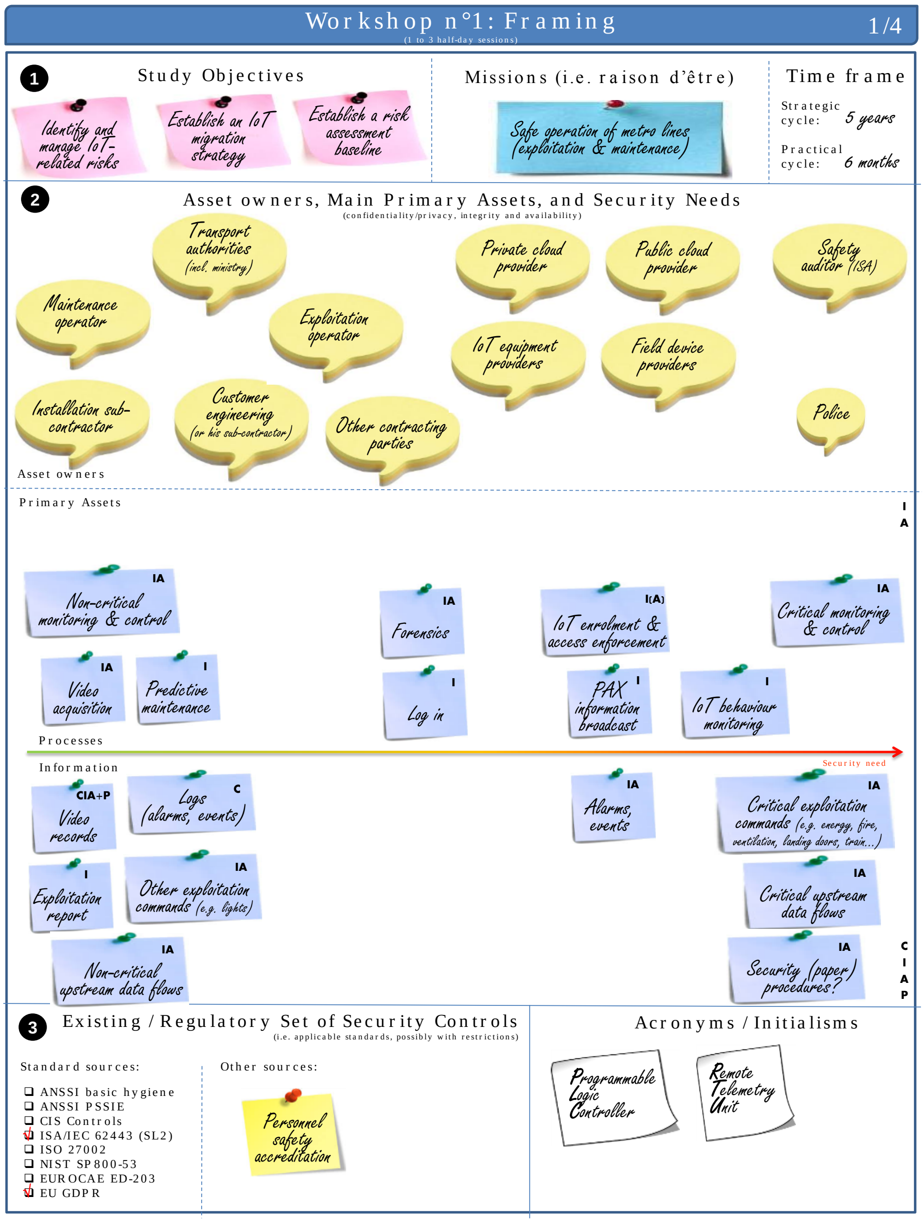
Fig. 11. Poster template for the assessment of the implementation status of security controls

6.4 Examples of Posters produced during Workshop n°1

Fig. 12 shows the first poster supporting workshop n°1 as it was filled in for the SCADA IoT case-study. To begin with, the study objectives were capture: (i) Identify and manage IoT-related risks, in particular to help design the future IoT devices in a secure manner; (ii) Establish a risk assessment baseline; and (iii) Establish an IoT migration strategy.

On this poster, we can see here that quite a large number of stakeholders have been captured, including regulatory bodies and public services.

In terms of primary assets, we can clearly see two large groups: on the right side of the security need axis, a group of assets with very strong integrity and availability needs to ensure the core mission of the system; on the left side, non-critical services and data. On the latter, the integrity and availability needs remain predominant, but some confidentiality and privacy needs also appear.



Workshop n°1: Framing

(1 to 3 half-day sessions)

1/4

1 Study Objectives

Identify and manage IoT-related risks

Establish an IoT migration strategy

Establish a risk assessment baseline

Missions (i.e. raison d'être)

Safe operation of metro lines (exploitation & maintenance)

Time frame

Strategic cycle: 5 years

Practical cycle: 6 months

2 Asset owners, Main Primary Assets, and Security Needs

(confidentiality/privacy, integrity and availability)

Transport authorities (incl. ministry)

Private cloud provider

Public cloud provider

Safety auditor (ISA)

Maintenance operator

Exploitation operator

IoT equipment providers

Field device providers

Installation sub-contractor

Customer engineering (or his sub-contractor)

Other contracting parties

Police

Asset owners

Primary Assets

I
A
IA Non-critical monitoring & control
IA Forensics
I(A) IoT enrolment & access enforcement
IA Critical monitoring & control
IA Video acquisition
I Predictive maintenance
I Log in
I PAX information broadcast
I IoT behaviour monitoring
Processes
Security need
Information
CIA+P Video records
C Logs (alarms, events)
IA Alarms, events
IA Critical exploitation commands (e.g. energy, fire, ventilation, landing doors, train...)
I Exploitation report
IA Other exploitation commands (e.g. lights)
IA Critical upstream data flows
IA Non-critical upstream data flows
IA Security (paper) procedures?
C
I
A
P

3 Existing / Regulatory Set of Security Controls

(i.e. applicable standards, possibly with restrictions)

Standard sources:

- ☐ ANSSI basic hygiene
- ☐ ANSSI PSSIE
- ☐ CIS Controls
- ☑ ISA/IEC 62443 (SL2)
- ☐ ISO 27002
- ☐ NIST SP800-53
- ☐ EUROCAE ED-203
- ☑ EU GDPR

Other sources:

Personnel safety accreditation

Acronyms / Initialisms

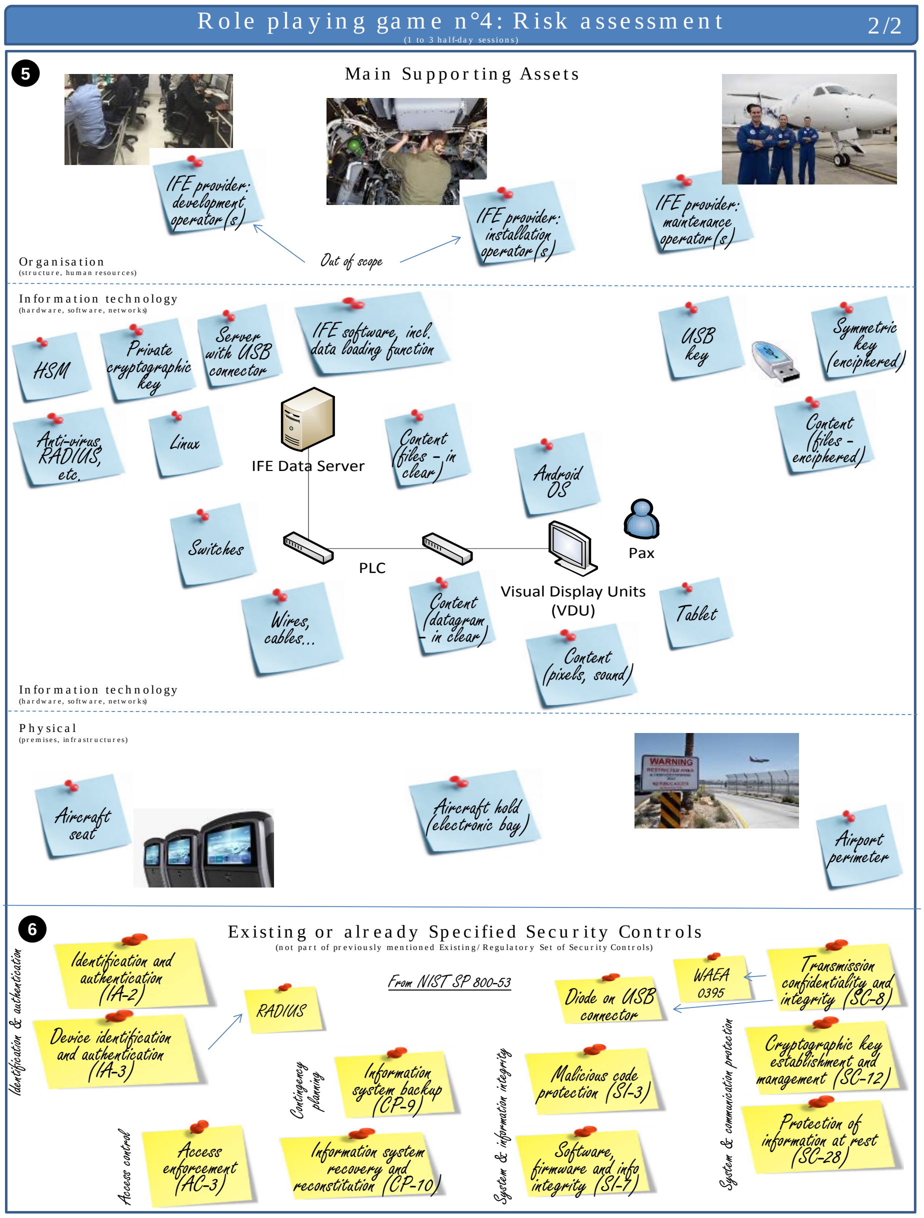
Programmable Logic Controller

Remote Telemetry Unit

Fig. 12. First poster supporting workshop n°1, applied to a SCADA IoT case-study

Upon starting the study, we were given one important input. The SCADA currently complies and should continue to comply with Security Level 2 (SL2) of the IEC

62443 standard [14]. This regulatory constraint was registered at the bottom left of the poster.



Role playing game n°4: Risk assessment 2/2

(1 to 3 half-day sessions)

5 Main Supporting Assets

Organisation
(structure, human resources)

IFE provider: development operator(s)

IFE provider: installation operator(s)

IFE provider: maintenance operator(s)

Out of scope

Information technology
(hardware, software, networks)

HSM

Private cryptographic key

Server with USB connector

IFE software, incl. data loading function

USB key

Symmetric key (enciphered)

Anti-virus, RADIUS, etc.

Linux

Content (files – in clear)

Android OS

Content (files – enciphered)

Switches

Wires, cables…

Content (datagram – in clear)

Content (pixels, sound)

Tablet

Information technology
(hardware, software, networks)

Physical
(premises, infrastructures)

Aircraft seat

Aircraft hold (electronic bay)

Airport perimeter

6 Existing or already Specified Security Controls

(not part of previously mentioned Existing/Regulatory Set of Security Controls)

From NIST SP 800-53

Identification & authentication

Identification and authentication (IA-2)

Device identification and authentication (IA-3)

RADIUS

Access control

Access enforcement (AC-3)

Contingency planning

Information system backup (CP-9)

Information system recovery and reconstitution (CP-10)

System & information integrity

Malicious code protection (SI-3)

Software, firmware and info integrity (SI-7)

Diode on USB connector

WAEA 0395

System & communication protection

Transmission confidentiality and integrity (SC-8)

Cryptographic key establishment and management (SC-12)

Protection of information at rest (SC-28)

Fig. 13. Second poster supporting workshop n°1, applied to an IFE case-study

Fig. 13 presents an example of the second poster supporting workshop n°1, applied this time to the IFE case-study. The IFE case-study is focused on the operational exploitation of the IFE, i.e. it excludes the development and installation parts of the system's lifecycle. Thus, we have only identified the IFE maintenance operator(s) as organisational supporting assets. For IT supporting assets the list is more extensive. To keep the story short, let us just focus here on the supporting assets of the copyrighted content, i.e. films, music and games. In the IFE case-study, copyrighted content is a primary asset with obvious confidentiality needs. The copyrighted content exists physically in many forms, e.g.: (i) as an enciphered file in the USB stick that the IFE maintenance operator carries to perform content update; (ii) as a file in clear on the disk of the IFE data server; (iii) as a datagram in the cables and switches between the IFE data server and the Visual Display Units (VDUs); and (iv) as pixels and sound on the VDUs. Last but not least, we have identified three physical supporting assets: the aircraft seat, the electronic bay in the aircraft hold, and the airport perimeter.

The fifth and last section of the poster relates to existing or already specified security controls. In the IFE case-study, the NIST SP 800-53 standard [15] has been used, therefore the poster shows the NIST identifiers of the security controls, e.g. Device Identification and Authentication (IA-3), and Transmission confidentiality and integrity (SC-8).

For some controls, the poster also shows how these controls are / will be implemented. For example, IA-3 will be ensured using a classical Remote Authentication Dial-In User Service (RADIUS), whilst Transmission Confidentiality and Integrity (SC-8) will be ensured using the (now obsolete) domain-specific WAEA 0395 standard [16], and a diode on the USB connector of the IFE server.

The identification of supporting assets is important to later identify how the security needs of the primary assets may be breached. Each supporting asset has its vulnerabilities and may be attacked in its own way. If we stick to the example of the copyrighted content it is possible to: (i) mug the maintenance operator and snatch the USB key with the enciphered files of the copyrighted content during a maintenance operation; (ii) to steal the removable disk in the IFE data server with the copyrighted content in clear; (iii) to sniff the network; or (iv) film the VDU with a smart phone, whilst recording the sound via the jack plug.

The existing or already specified security controls are also important to later assess the likelihood of the aforementioned security breaches. For example, the existence of a RADIUS makes it a bit less likely for an attacker to spoof a VDU with its own recording device.

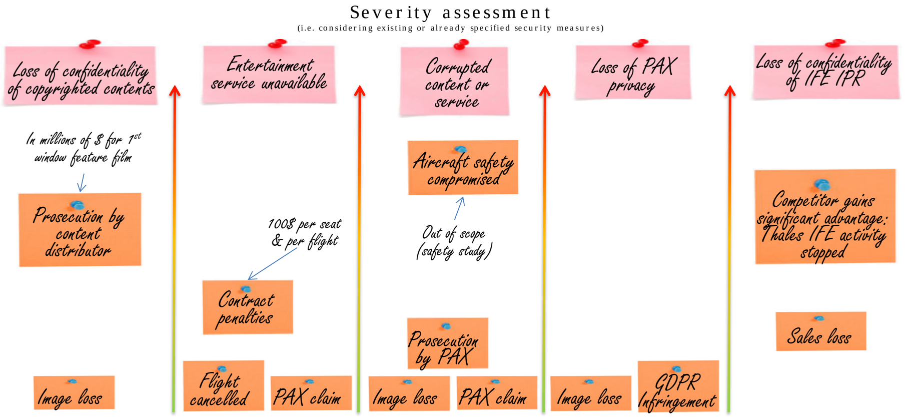
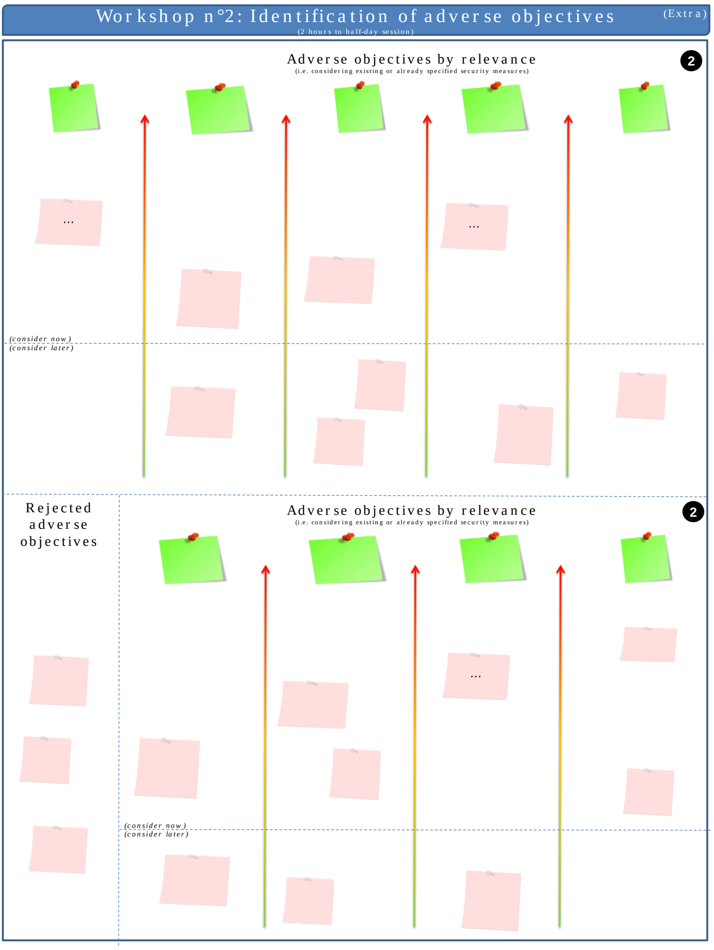

Severity assessment
(i.e. considering existing or already specified security measures)
Loss of confidentiality of copyrighted contents
In millions of $ for 1st window feature film
Prosecution by content distributor
Image loss
Entertainment service unavailable
100$ per seat & per flight
Contract penalties
Flight cancelled
PAX claim
Corrupted content or service
Aircraft safety compromised
Out of scope (safety study)
Prosecution by PAX
Image loss
PAX claim
Loss of PAX privacy
Image loss
GDPR Infringement
Loss of confidentiality of IFE IPR
Competitor gains significant advantage: Thales IFE activity stopped
Sales loss

Fig. 14. Severity assessment of the IFE feared events

Fig. 14 shows an extract of the workshop n°1 optional poster, filled-in for the IFE case-study. This cropped poster illustrates five feared events. For example, if we consider that copyrighted content needs to be confidential in the IFE case-study, then "loss of the confidentiality of the copyrighted content" or "a first-window feature films becomes freely accessible on the Internet" make two perfect examples of feared events. It can be seen here that the most severe feared event impacts relate to the violation of the confidentiality of the copyrighted content (1st column) and to the violation of the confidentiality of the IFE developer's know-how (5th column). This is because the corruption of the content or the service leading to a safety event, e.g. the display of a malicious message such as "All passengers, please move to the rear of the aircraft" with its probable dramatic effect on the aircraft balance, is considered out of scope of this study, as it is normally already covered by the safety case. Following this work, the IFE system has been categorized as "Moderate" according to the NIST SP 800-53 standard [15]. This categorisation pulls a significant set of security controls, some of which are listed on the poster discussed above (cf. **Fig. 13**).

6.5 Complementary Poster Template in support of Workshop n°2

Fig. 15 shows the extra poster for workshop n°2. This poster extends the main workshop n°2 poster (cf. **Fig. 4**) to cope with additional risk sources. This poster may be used as often as required, however, up to now, in all our case-studies, a single instance of this extra poster proved sufficient.



Workshop n°2: Identification of adverse objectives (Extra)

(2 hours to half-day session)

Adverse objectives by relevance

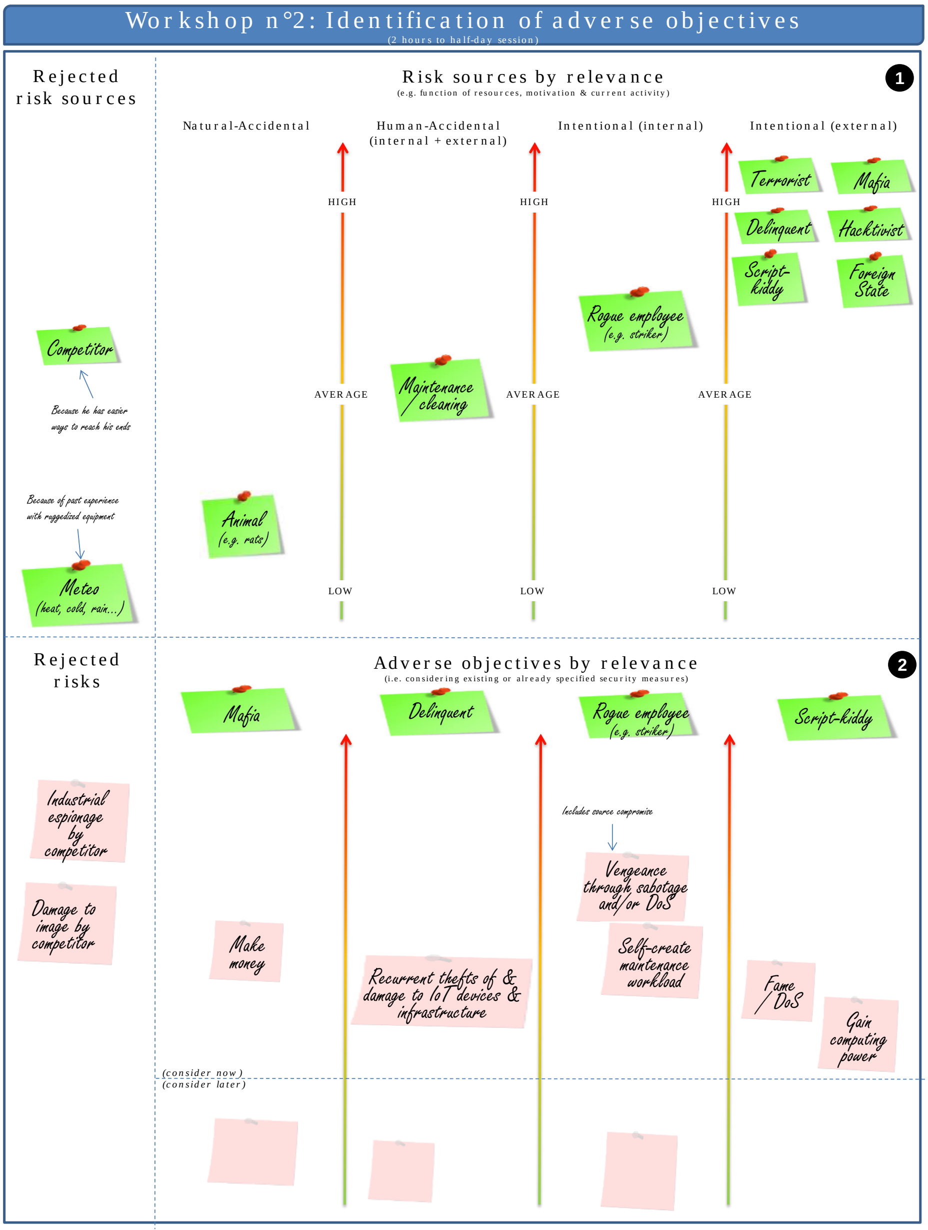
(i.e. considering existing or already specified security measures)

Fig. 15. Template of the extra poster for workshop n°2

6.6 Example of Poster produced during Workshop n°2

Fig. 16 shows the main poster for workshop n°2 filled in for the SCADA IoT case-study. It can be seen here that the most relevant risk sources are malevolent ones, essentially external, but the internal rogue employee is also highly considered. In the lower part of the poster, the objectives of the latter even appear as the most relevant adverse objective, i.e. Vengeance through sabotage and / or Denial of Service (DoS), and the self-creation of maintenance workload.

The poster also shows that two risk sources have been rejected: the competitor because he would have easier ways of acting, and the meteorological conditions, because of past experience with ruggedized equipment. As a consequence, the objectives of the competitor have been listed but obviously rejected.



Workshop n°2: Identification of adverse objectives

(2 hours to half-day session)

Rejected risk sources

Risk sources by relevance

(e.g. function of resources, motivation & current activity)

Natural-Accidental

Human-Accidental (internal + external)

Intentional (internal)

Intentional (external)

Rejected risks

Adverse objectives by relevance

(i.e. considering existing or already specified security measures)

(consider now)

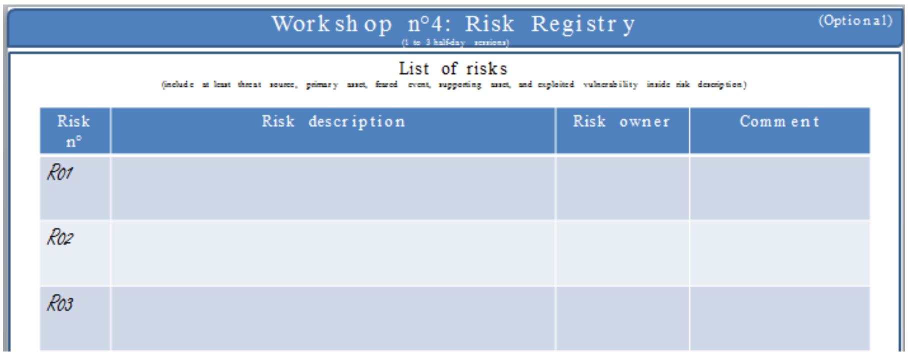
(consider later)

1
HIGH
AVERAGE
LOW
Terrorist
Mafia
Delinquent
Hacktivist
Script-kiddy
Foreign State
Rogue employee (e.g. striker)
Maintenance / cleaning
Animal (e.g. rats)
Competitor
Because he has easier ways to reach his ends
Because of past experience with ruggedized equipment
Meteo (heat, cold, rain...)
2
Mafia
Delinquent
Rogue employee (e.g. striker)
Script-kiddy
Industrial espionage by competitor
Damage to image by competitor
Make money
Recurrent thefts of & damage to IoT devices & infrastructure
Includes source compromise
Vengeance through sabotage and/or DoS
Self-create maintenance workload
Fame / DoS
Gain computing power

Fig. 16. Poster of workshop n°2 filled-in for the SCADA IoT case-study

6.7 Complementary Poster Template in support of Workshop n°3

Fig. 17 proposes a poster template to register all risks, as identified during workshop n°3. The main objective of this register is to allow for the referencing of risks by their number, under the format Rxx, rather than pull the often long description of the scenarios. In addition, the template allows capturing additional comments for each risk, which is something that was very much restricted with our poster-based approach up to now.



Workshop n°4: Risk Registry (Optional)

(1 to 3 half-day sessions)

List of risks

(include at least threat source, primary asset, feared event, supporting asset, and exploited vulnerability inside risk description)

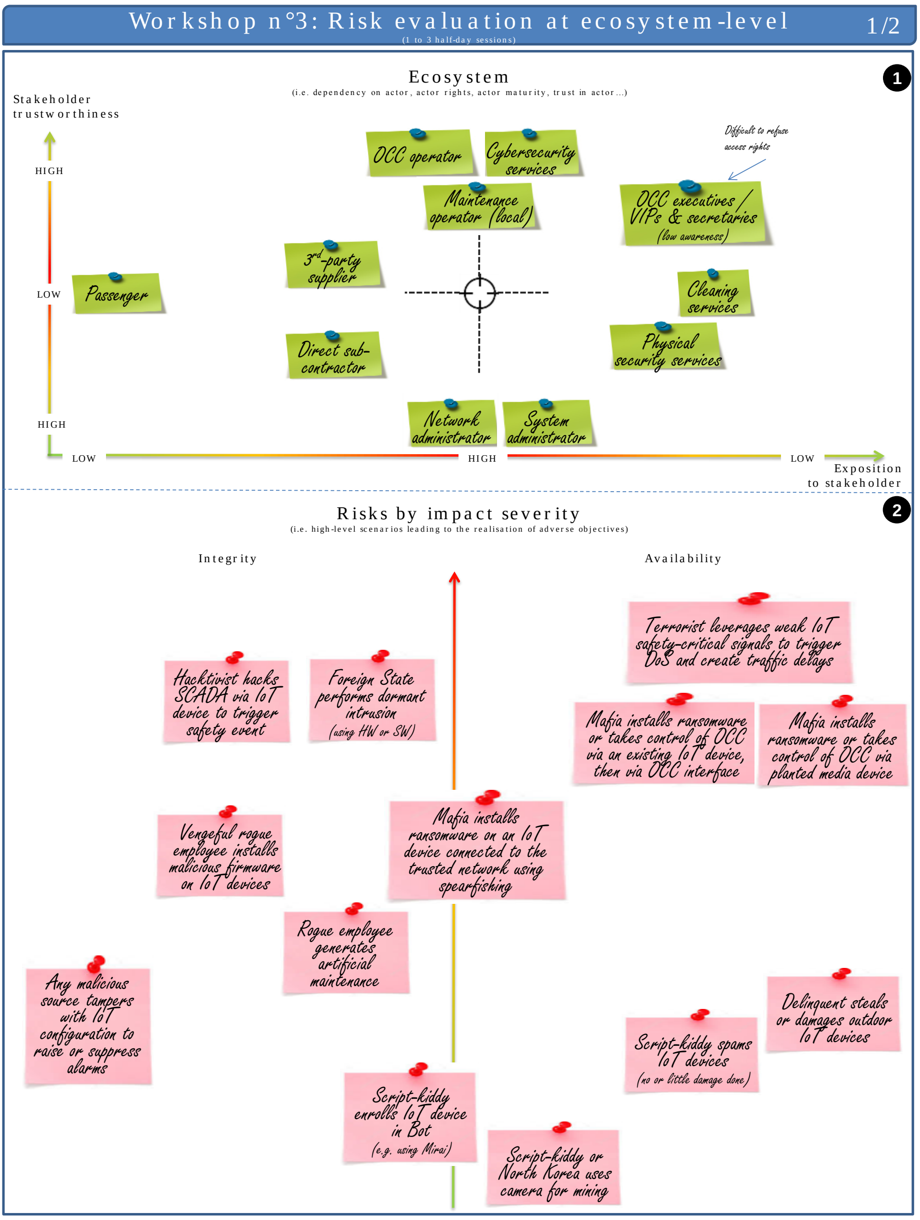
Risk n°	Risk description	Risk owner	Comment
R01			
R02			
R03			

Fig. 17. Poster template to be used as risk register (cropped)

6.8 Example of Poster produced during Workshop n°3

Fig. 18 shows the first poster of workshop n°3 filled in for the SCADA IoT case-study. On the upper part of the poster, it can be seen that there are no critical stakeholders: when stakeholders have high privileges on the system, they are trustworthy, and if they are untrustworthy, then they do not have special privileges. Still, attention is called upon the local maintenance operators, third-party suppliers, direct subcontractors, physical security services and company executives. The latter was commented as being particularly difficult to cope with, as it is often difficult to refuse access rights to one’s boss, even if he does not need it.

The lower part of the poster is used to capture how the risk sources will proceed to reach their objective(s), at a very gross-grain level, e.g. in the SCADA IoT case-study, “Mafia installs ransomware on an IoT device connected to the trusted network using spearfishing targeted at the maintenance operator”. It can be seen here that there are quite a few risks with a pretty high severity. Risks that relate to both integrity and availability are located astride the severity axis.



Workshop n°3: Risk evaluation at ecosystem-level

(1 to 3 half-day sessions)

1/2

Ecosystem

(i.e. dependency on actor, actor rights, actor maturity, trust in actor…)

1

Stakeholder trustworthiness

HIGH

LOW

HIGH

LOW

HIGH

LOW

Exposition to stakeholder

OCC operator

Cybersecurity services

Maintenance operator (local)

Difficult to refuse access rights

OCC executives / VIPs & secretaries (low awareness)

3rd-party supplier

Passenger

Cleaning services

Direct sub-contractor

Physical security services

Network administrator

System administrator

Risks by impact severity

(i.e. high-level scenarios leading to the realisation of adverse objectives)

2

Integrity

Availability

Terrorist leverages weak IoT safety-critical signals to trigger DoS and create traffic delays

Hacktivist hacks SCADA via IoT device to trigger safety event

Foreign State performs dormant intrusion (using HW or SW)

Mafia installs ransomware or takes control of OCC via an existing IoT device, then via OCC interface

Mafia installs ransomware or takes control of OCC via planted media device

Vengeful rogue employee installs malicious firmware on IoT devices

Mafia installs ransomware on an IoT device connected to the trusted network using spearfishing

Rogue employee generates artificial maintenance

Any malicious source tampers with IoT configuration to raise or suppress alarms

Delinquent steals or damages outdoor IoT devices

Script-kiddy spams IoT devices (no or little damage done)

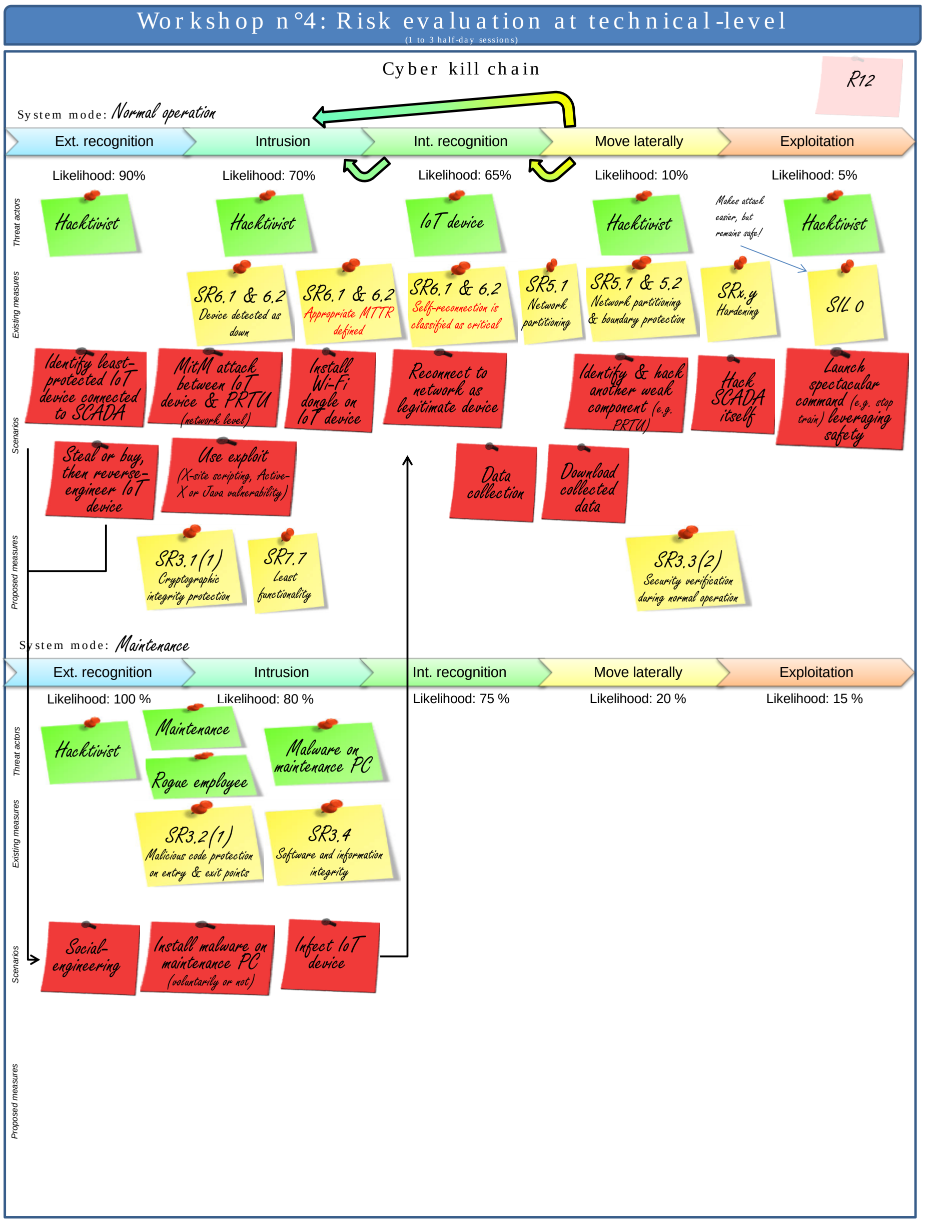
Script-kiddy enrolls IoT device in Bot (e.g. using Mirai)

Script-kiddy or North Korea uses camera for mining

Fig. 18. First poster of workshop n°3 filled-in for the SCADA IoT case-study

It should be reminded here that ultimately the criticality of a risk depends on both the severity of its impacts and the likelihood of its occurrence. At this stage the likelihood has not yet been studied.

6.9 Example of Poster produced during Workshop n°4



Workshop n°4: Risk evaluation at technical-level

(1 to 3 half-day sessions)

Cyber kill chain

System mode: Normal operation

Ext. recognition | Intrusion | Int. recognition | Move laterally | Exploitation

Likelihood: 90% | Likelihood: 70% | Likelihood: 65% | Likelihood: 10% | Likelihood: 5%

Threat actors

Existing measures

Scenarios

Proposed measures

System mode: Maintenance

Ext. recognition | Intrusion | Int. recognition | Move laterally | Exploitation

Likelihood: 100 % | Likelihood: 80 % | Likelihood: 75 % | Likelihood: 20 % | Likelihood: 15 %

Threat actors

Existing measures

Scenarios

Proposed measures

R12
Normal operation
Hacktivist
Hacktivist
IoT device
Hacktivist
Makes attack easier, but remains safe!
Hacktivist
SR6.1 & 6.2 Device detected as down
SR6.1 & 6.2 Appropriate MTTR defined
SR6.1 & 6.2 Self-reconnection is classified as critical
SR5.1 Network partitioning
SR5.1 & 5.2 Network partitioning & boundary protection
SRx.y Hardening
SIL 0
Identify least-protected IoT device connected to SCADA
MitM attack between IoT device & PRTU (network level)
Install Wi-Fi dongle on IoT device
Reconnect to network as legitimate device
Identify & hack another weak component (e.g. PRTU)
Hack SCADA itself
Launch spectacular command (e.g. stop train) leveraging safety
Steal or buy, then reverse-engineer IoT device
Use exploit (X-site scripting, Active-X or Java vulnerability)
Data collection
Download collected data
SR3.1(1) Cryptographic integrity protection
SR7.7 Least functionality
SR3.3(2) Security verification during normal operation
Maintenance
Hacktivist
Maintenance
Rogue employee
Malware on maintenance PC
SR3.2(1) Malicious code protection on entry & exit points
SR3.4 Software and information integrity
Social-engineering
Install malware on maintenance PC (voluntarily or not)
Infect IoT device

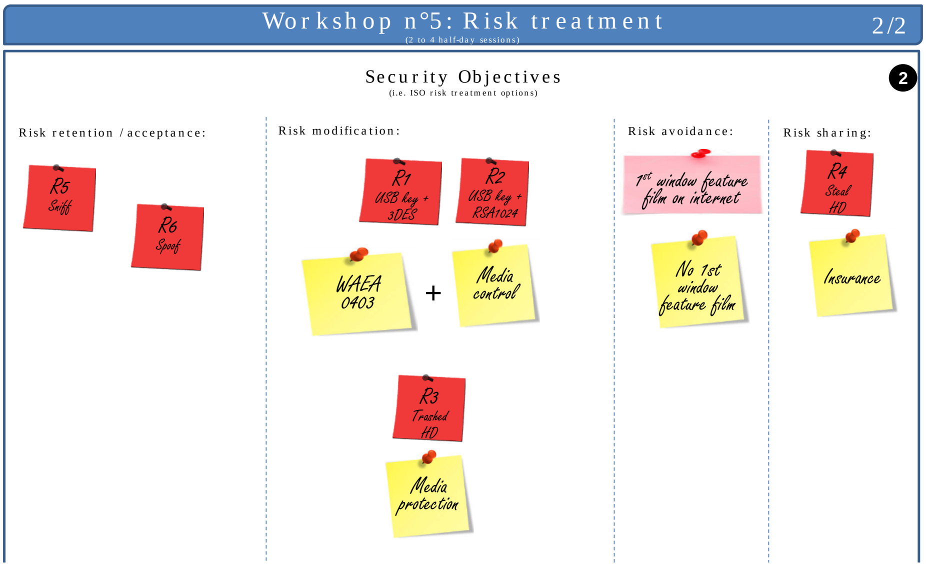
Fig. 19. Example of Cyber Kill Chain defined for the SCADA IoT case-study

Fig. 19 shows a Cyber Kill Chain created for our SCADA IoT case-study. The upper part of the poster shows a full blown scenario, in which the attacker has significant cybersecurity knowledge to reverse-engineer the IoT device and exploit some communication vulnerability. The lower part of the poster shows an alternative path, in which social engineering is used to benefit from the collusion of a rogue employee. The social engineering path has been assessed as more likely.

6.10 Example of Poster produced during Workshop n°5

Fig. 20 presents the risk treatment poster filled in for the IFE case-study. It can be seen here that:

- risks R5 and R6 are accepted;
- risks R1 and R2 are treated by proposing the perform some media control and by changing the obsolete WAEA standard by its newest edition, i.e. WAEA 0403;
- risk R3 is treated by proposing some media protection;
- risk R4 is shared by contracting an insurance.



Workshop n°5: Risk treatment 2/2

(2 to 4 half-day sessions)

Security Objectives 2

(i.e. ISO risk treatment options)

Risk retention / acceptance:

Risk modification:

Risk avoidance:

Risk sharing:

Fig. 20. Example of risk treatment defined for the SCADA IoT case-study (cropped)

We can also see that the event of finding a first-window feature film on internet can be avoided by not showing any first-window feature film. Here, the airline may not agree with the treatment option and plan.

7 Acknowledgements

This research was partially funded by the French DGA CoSS-2 RAPID project. We wish to thank Sébastien Lhuillier and Thomas Baudillon from Thales SIX GTS FRANCE for their lead in the SCADA IoT case-study and Christophe Alix and Hélène Bachatène for their lead in the VLLAM/UTM case-study. Many thanks also to Fabien Caparros of ANSSI for his review of the poster templates, and to all the Thales engineers who made constructive comments on this work.