# EBIOS
## RISK MANAGER

# GOING FURTHER

# METHODOLOGICAL SHEETS

# INTRODUCTION:
## POSITIONING OF WORKSHOPS
## IN THE RISK ASSESSMENT APPROACH

The diagram below presents the various notions addressed by EBIOS Risk Manager in the framework of a risk assessment approach.



Key:
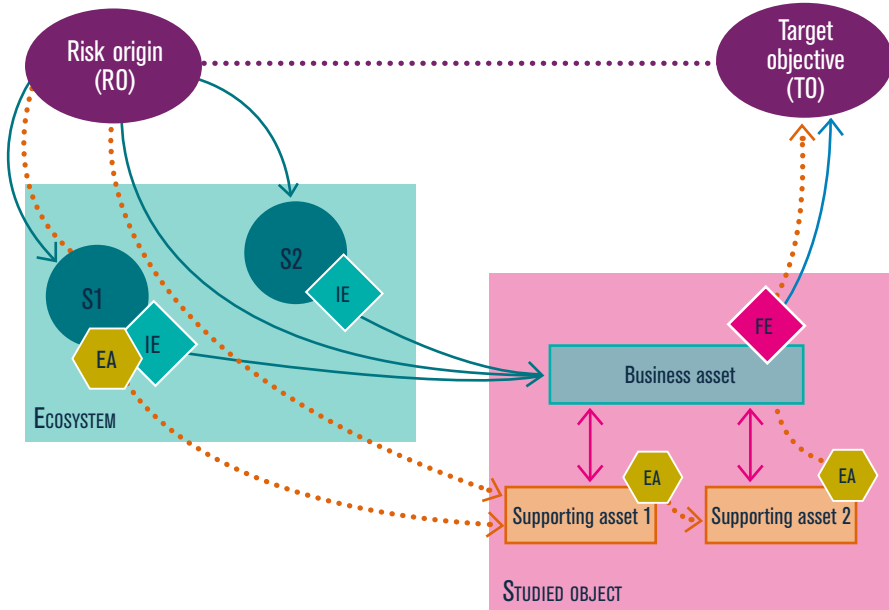
| | |
|---|---|
| → (teal solid arrow) | Attack path of a strategic scenario |
| ⋯⋯▷ (orange dotted arrow) | Method of attack of an operational scenario |
| EA | Elementary actions on supporting assets |
| IE | Intermediate event concerning a business asset of the ecosystem |
| FE | Feared event concerning a business asset of the studied object |
| S | Stakeholder of the ecosystem |

During **workshop 1**, participants identify the business and technical scope of the studied object, which corresponds to **business assets** and **supporting assets**. They also define the feared events associated with the business assets and their level of severity.

**Workshop 2** makes it possible to identify the most pertinent **risk origin /target objective** (RO/TO) pairs for the rest of the study. Certain target objectives (from the attacker's point of view) will be related to certain feared events (from the organisation's point of view). For example, we can relate the target objective "exfilter information in order to obtain a competitive advantage" to the feared event "leakage of the company's R&D information". Making this relation is a first step towards building strategic scenarios.

At the beginning of **workshop 3**, participants identify the **stakeholders** of the ecosystem of the studied object and assess their threat level. Following this assessment, the participants define strategic scenarios stemming from the risk origin in order to move towards the target objective. These scenarios implement **attack paths** during which the risk origin generates one or several feared events on the business assets of the studied object. In a logic of least effort from the point of view of the risk origin, certain attack paths are able to pass through stakeholders of the ecosystem by generating **so-called intermediate events**.

In **workshop 4**, participants establish **operational scenarios** that describe the technical **methods of attack** able to be used by the risk origin to carry out the strategic scenarios identified in **workshop 3**. An operational scenario is a chain of **elementary actions** concerning the supporting assets of the studied object or of its ecosystem. Each attack path of a strategic scenario gives rise to an operational scenario, which is assessed in terms of likelihood.

METHODOLOGICAL SHEET

# 1

## Defining the business and technical scope (Workshop 1)
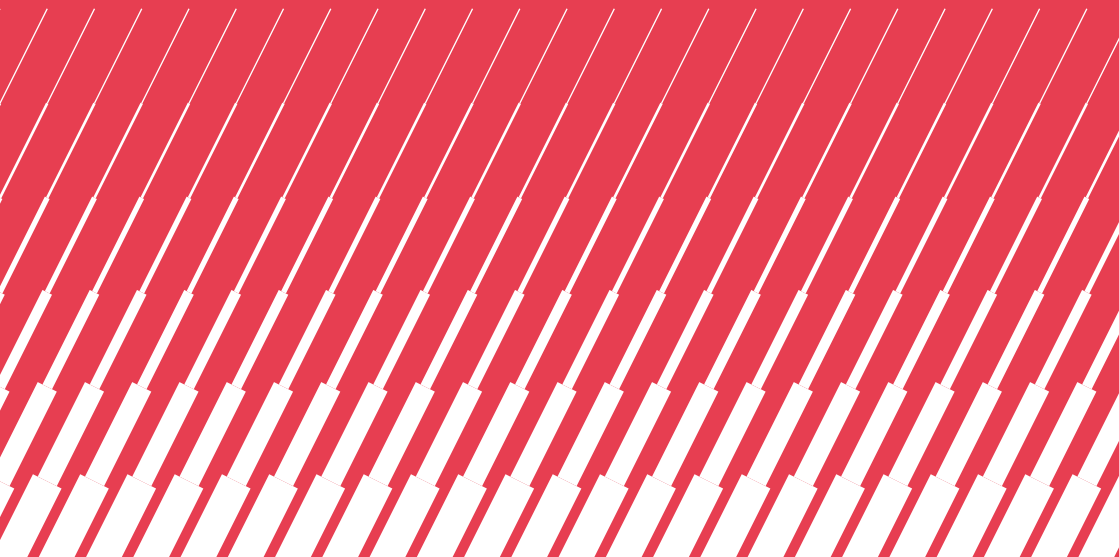
The work of identifying missions, business assets and supporting assets relating to the studied object can be formalised in a table such as proposed hereinbelow:

| MISSIONS | MISSION 1 | MISSION… | | |
|---|---|---|---|---|
| **DENOMINATION OF THE BUSINESS ASSET** | Business asset 1 | Business asset 2 | | Business asset… |
| **NATURE OF THE BUSINESS ASSET (PROCESS OR INFORMATION)** | | | | |
| **DESCRIPTION** | | | | |
| **ENTITY OR PERSON RESPONSIBLE (INTERNAL / EXTERNAL)** | | | | |
| **DENOMINATION OF THE ASSOCIATED SUPPORTING ASSET(S)** | Supporting asset 1 | Supporting asset 2 | Supporting asset 3 | Supporting asset… |
| **DESCRIPTION** | | | | |
| **ENTITY OR PERSON RESPONSIBLE (INTERNAL / EXTERNAL)** | | | | |

**NOTE:** it is possible to associate one or several supporting assets with a business asset.

To each business asset and supporting asset corresponds to an entity or a person responsible. This entity or person can be internal to the organisation or represent an external stakeholder of the ecosystem. The elements related to the ecosystem will be taken into account in **workshop 3**.

# 2

# Identifying the supporting assets (Workshops 1, 4 and 5)

The types of supporting assets represent the major categories of components of an information system on which the business assets or the security measures are based.

This methodological sheet can be useful to you when defining the business and technical scope **(Workshop 1)**, building operational scenarios **(Workshop 4)** or defining security measures **(Workshop 5)**.

The supporting assets can be grouped together according to the following categories:

| SUPPORTING ASSET | EXAMPLES (INCOMPLETE LIST) |
|---|---|
| **INFORMATION AND TELEPHONE SYSTEMS** | |
| **HARDWARE[1]** | |
| **USER TERMINAL** | Computer, laptop, tablet, mobile phone |
| **PERIPHERAL DEVICE** | Printer, scanner, keyboard, mouse, camera, microphone, connected object |
| **TELEPHONE** | Fixed or mobile phone, analogue or IP |
| **STORAGE EQUIPMENT** | USB key, hard drive, CD-ROM, memory card |
| **SERVER** | Mainframe, blade server, rack server |
| **MEANS OF ADMINISTRATION** | Administration station, administration tool servers, bastion |
| **NETWORK EQUIPMENT** | Switch, router, inbound gateways from outside, Wi-Fi terminal |
| **SECURITY EQUIPMENT** | Firewall, intrusion detection system (IDS/IPS), VPN gateway |
| **INDUSTRIAL EQUIPMENT** | Programmable logic controller, sensor, actuator, SCADA system, safety instrumented system |
| **SOFTWARE** | |
| **INFRASTRUCTURE SERVICE** | Directory service, IP address management service (DHCP), domain name service (DNS), domain controller, print server |
| **APPLICATION/APPLICATION SERVICE** | Web server, web service, application server, email server, database server, software packages (HR, customer relations, ERP) |
| **MIDDLEWARE** | Enterprise Application Integration (EAI), Extract-Transform-Load (ETL), Open DataBase Connectivity (ODBC) |

---

1 Hardware most of the time embarks software that is indispensable for their operation.

| | |
|---|---|
| **OPERATING SYSTEM (OS), HYPERVISOR** | Windows, Linux, MacOS, Xen |
| **FIRMWARE** | Basic Input Output System (BIOS), Unified Extensible Firmware Interface (UEFI), mobile phone component manager, program stored in a USB key equipped with a microprocessor |
| **SECURITY SOFTWARE** | Security Information and Event Management (SIEM) |
| **NETWORKS/COMPUTER AND TELEPHONE CHANNELS** | |
| **NETWORK/COMPUTER CHANNEL** | Network cable, fibre optic, radio link (Wi-Fi, Bluetooth, etc.) |
| **NETWORK/TELEPHONE CHANNEL** | Telephone line |
| **ORGANISATIONS** | |
| **INDIVIDUAL** | Employee, trainee, service provider, maintenance personnel |
| **PAPER DOCUMENT** | Handwritten or printed document |
| **VERBAL EXCHANGE** | Meeting, informal exchange |
| **SOCIAL ENGINEERING ELEMENT** | Information shared over the social networks |
| **PHYSICAL INSTALLATIONS AND PREMISES** | |
| **SITE/BUILDING/ROOM** | Head office, plant, storage site, industrial building, meeting room, server room |
| **PHYSICAL SECURITY SYSTEM** | Access systems by badge, intrusion detection system, video-protection system |
| **OPERATING SECURITY SYSTEM** | Air conditioning, fire safety, electrical power supply |

For more information and in particular for more precise definitions of the supporting assets mentioned, please refer to the ANSSI mapping guide[2].

---

2 Map of the information system – Guide to drawing up in 5 steps, ANSSI, 2018.

# 3

# Assessing the severity of the impacts of feared events (Workshops 1 and 3)

# 1 / Which categories of impacts must be taken into account?

The categories hereinafter can be used as a basis to identify the impacts linked to the feared events and facilitate the assessment of the severity:

- impacts on the missions and services of the organisation;
- human, equipment or environmental impacts;
- impacts on governance;
- financial impacts;
- legal impacts;
- impacts on the image and trust.

**NOTE**: according to the context, certain categories can correspond to aggravating factors or to indirect impacts.

| IMPACT | EXAMPLES (INCOMPLETE LIST) |
|---|---|
| **IMPACTS ON THE MISSIONS AND SERVICES OF THE ORGANISATION** | |
| **DIRECT OR INDIRECT CONSEQUENCES ON THE CARRYING OUT OF MISSIONS AND SERVICES** | Inability to provide a service, degradation in operational performance, delays, impacts on production or distribution of goods and services, impossibility of implementing a key process |
| **HUMAN, MATERIAL OR ENVIRONMENTAL IMPACTS** | |
| **IMPACTS ON THE SAFETY OR ON THE HEALTH OF PERSONS** **DIRECT OR INDIRECT CONSEQUENCES ON THE PHYSICAL INTEGRITY OF PERSONS** | Occupational accident; occupational disease, loss of human life, placing in danger, health alert or crisis |
| **MATERIAL IMPACTS** **MATERIAL DAMAGE OR DESTRUCTION OF SUPPORTING ASSETS** | Destruction of premises or installations, damage to means of production, premature wear of equipment |
| **IMPACTS ON THE ENVIRONMENT** **SHORT- OR LONG-TERM, DIRECT OR INDIRECT, ECOLOGICAL CONSEQUENCES** | Radiological or chemical contamination of groundwater or the ground, discharge of pollutants into the atmosphere |

| IMPACTS ON GOVERNANCE | |
|---|---|
| **IMPACTS ON THE CAPACITY FOR DEVELOPMENT OR DECISION-MAKING** DIRECT OR INDIRECT CONSEQUENCES ON THE FREEDOM TO DECIDE, DIRECT, OR IMPLEMENT THE DEVELOPMENT STRATEGY | Loss of sovereignty, loss or limitation of independence of judgement or decision, limitation of trading margins, loss of the capacity of influence, takeover of the organisation, forced change in strategy, loss of key suppliers or subcontractors |
| **IMPACTS ON THE INTERNAL SOCIAL TIES** DIRECT OR INDIRECT CONSEQUENCES ON THE QUALITY OF THE SOCIAL TIES WITHIN THE ORGANISATION | Loss of trust from employees in the sustainability of the organisation, exacerbation of a feelings or tensions between groups, drop in commitment, loss of the meaning of common values |
| **IMPACTS ON THE INTELLECTUAL OR CULTURAL HERITAGE** DIRECT OR INDIRECT CONSEQUENCES ON THE INEXPLICIT KNOWLEDGE ACCUMULATED BY THE ORGANISATION, ON THE KNOW-HOW, ON THE CAPACITIES FOR INNOVATION, ON THE COMMON CULTURAL REFERENCES | Loss of memory of the company (former projects, successes or failures), loss of implicit knowledge (know-how transmitted between generations, optimisation in the execution of tasks or processes), capturing innovative ideas, loss of scientific or technical heritage, loss of key human resources |
| FINANCIAL IMPACTS | |
| **DIRECT OR INDIRECT FINANCIAL CONSEQUENCES.** | Loss of turnover, loss of a market, unplanned expenses, drop in the stock market value, drop in income, imposed penalties |
| LEGAL IMPACTS | |
| **CONSEQUENCES FOLLOWING A LEGAL, REGULATORY, NORMATIVE OR CONTRACTUAL NON-COMPLIANCE.** | Trial, fine, sentencing of a manager, contract amendment. |
| IMPACTS ON THE IMAGE AND TRUST | |
| **DIRECT OR INDIRECT CONSEQUENCES ON THE IMAGE OF THE ORGANISATION, NOTORIETY, CUSTOMER TRUST.** | Publication of negative articles in the press, loss of credibility with customers, discontented shareholders, loss of notoriety, loss of user trust |

# 2 / Which severity scale should be used?

When assessing a scale of impact levels, the main stake is that it shall be understood and able to be used by the persons who need to assess the importance of the consequences of a feared event. It is recommended to develop it in cooperation with the persons who will be estimating these levels – particularly the business teams – in order to facilitate the appropriation thereof and the coherence of the score. The severity scale that should be favoured remains the one that is already in place (if it exists) in order to assess the risks of the organisation in the framework of an overall approach to risk management that includes the financial, legal, etc. risks. The digital risk must indeed be inserted into the overall risk map. On the other hand, a certain number of sector regulations have scales of impact levels that are suitable for use or with which it is suitable to be at least compatible.

If you do not have such a scale, draw up one with the business teams at the beginning of the workshop devoted to feared events. To do this, you can use and adapt the general scale hereinafter. It takes account of the impacts internal to the organisation and any external consequences on the ecosystems.

| LEVEL OF THE SCALE | DEFINITION |
|---|---|
| **G5 – CATASTROPHIC** | **Sector or regulatory consequences beyond the organisation.** Substantially impacted sector ecosystem(s), with consequences that may be long-lasting. And/or: difficulty for the State, and even an incapacity, to ensure a regulatory function or one of its missions of vital importance. And/or: critical impacts on the safety of persons and property (health crisis, major environmental pollution, destruction of essential infrastructures, etc.). |
| **G4 – CRITICAL** | **Disastrous consequences for the organisation with possible impacts on the ecosystem.** Incapacity for the organisation to ensure all or a portion of its activity, with possible serious impacts on the safety of persons and property. The organisation will most likely not overcome the situation (its survival is threatened), the activity sectors or state sectors in which it operates will likely be affected slightly, without any long-lasting consequences. |
| **G3 – SERIOUS** | **Substantial consequences for the organisation.** High degradation in the performance of the activity, with possible significant impacts on the safety of persons and property. The organisation will overcome the situation with serious difficulties (operation in a highly degraded mode), without any sector or state impact. |
| **G2 – SIGNIFICANT** | **Significant but limited consequences for the organisation.** Degradation in the performance of the activity with no impact on the safety of persons and property. The organisation will overcome the situation despite a few difficulties (operation in degraded mode). |
| **G1 – MINOR** | **Negligible consequences for the organisation.** No impact on operations or the performance of the activity or on the safety of persons and property. The organisation will overcome the situation without too much difficulty (margins will be consumed). |

Using a scale with 4 or 5 levels is guided by the following considerations:

■ the need to measure very high impacts which correspond to major crises, even a destabilisation and loss of resilience ranging beyond the organisation involved (examples: paralysis or strong degradation of an entire industrial sector, incapacity for the State to ensure a regulatory function, major health or pollution crises affecting a large area, compromise of highly-classified information). In this case, a 5-level scale is recommended. Otherwise, 4 levels will be enough;

■ coherency in the number of levels between the severity and likelihood scales for the assessment of the risks carried out during workshop 4. If you use a likelihood scale with 5 levels, give preference to a severity scale with 5 levels.

**NOTE**: estimating the importance of the impacts must be contextualised, in such a way that the stakeholders are able to distinguish the impact levels of the scale. A usual way of proceeding is to use examples of the description of each level.

## Example of a severity scale for a production activity

| LEVEL OF THE SCALE | CONSEQUENCES ON THE OPERATIONS |
|---|---|
| **G4 – CRITICAL** | Long-lasting shutdown of operations requiring maintenance intervention. |
| **G3 – SERIOUS** | Temporary shutdown of operations then resuming under a particular procedure (example: additional operator). |
| **G2 – SIGNIFICANT** | Operations continue with an operator action. |
| **G1 – MINOR** | Operations continue with an alarm reporting the fault. |

METHODOLOGICAL SHEET

# 4

◆

# Identifying and characterising the risk origins (Workshop 2)

# 1 / Categories of risk origins (RO) and target objectives (TO)

The following table presents generic categories of intentional risk origins and target objectives that you can use to identify the RO/TO pairs.

**CATEGORIES OF RISK ORIGINS**

**Attacker profiles can be grouped into three main categories:**

- structured organisations that are guided by a logic of efficiency and gain which have sophisticated and substantial means, which may even by practically unlimited (States, organised crime);
- organisations or groups that are guided by ideological motivation which have significant means implemented in a relatively coordinated manner (terrorists, activists);
- attackers that are limited by specialised means (isolated individuals, groups of individuals or outfits).

**These categories can work together in an opportunistic or organised manner** `EXAMPLE` **: terrorist organisation calling upon a specialised outfit.**

◆

| ATTACKER PROFILES | EXAMPLES AND USUAL METHODS OF ATTACK |
|---|---|
| **STATE-RELATED** | States, intelligence agencies<br>*Attacks generally conducted by professionals, working under a calendar and a method of attack that are predefined. This attacker's profile is characterised by its ability to carry out an offensive operation over a long period of time (stable resources, procedures) and to adapt its tools and methods to the topology of the target. By extension, these actors have the means of purchasing or discovering 0-Day vulnerabilities and some are able to infiltrate isolated networks and to conduct successive attacks in order to reach a target or targets (for example by means of an attack aimed at the supply chain).* |

| | |
|---|---|
| **ORGANISED CRIME** | Cybercriminal organisations (mafias, gangs, outfits)<br>*On-line scams or in person, ransom request or attack via ransomware, use of botnets, etc. Due in particular to the proliferation of attack kits that are readily available on-line, cybercriminals are conducting increasingly sophisticated and organised operations for lucrative or fraudulent purposes. Some have the means of purchasing or discovering 0-Day vulnerabilities.* |
| **TERRORIST** | Cyber-terrorists, cyber-militias<br>*Attacks that are usually not very sophisticated but which are conducted with determination for the purposes of destabilisation and destruction: denial of service (aimed for example at making the emergency services of a hospital centre unavailable, untimely shutdowns of an energy production industrial system), exploitation of vulnerabilities of Internet sites and defacement.* |
| **IDEOLOGICAL ACTIVIST** | Cyber-hacktivists, interest groups, sects<br>*The methods of attack and sophistication of the attacks are relatively similar to those of cyber-terrorists but are motivated by less destructive intentions. Some actors will conduct these attacks in order to convey an ideology, a message (example: massive use of social networks as a sounding board).* |
| **SPECIALISED OUTFITS** | "Cyber-mercenary" profile with IT capacities that are generally high from a technical standpoint. Because of this, it must be distinguished from script-kiddies with whom it shares however the spirit of a challenge and search for recognition but with a lucrative objective. Such groups can be organised as specialised outfits that propose veritable hacking services.<br>*This type of experienced hacker is often at the origin of the designing and creating of attack kits and tools[3] that are available on-line (possibly for a fee) which can then be used "turnkey" by other groups of attackers. There are no particular motivations other than the financial gain.* |
| **AMATEUR** | Profile of the script-kiddies hacker or who has good IT knowledge, and motivated by the quest for social recognition, fun, challenge.<br>*Basic attacks but with the capacity of use the attack kits that are available on-line.* |
| **AVENGER** | The motivations of this attacker's profile are guided by a spirit of acute vengeance or a feeling of injustice (examples: employee dismissed for serious fault, discontented service provider following a contract that was not renewed, etc.).<br>*This attacker profile is characterised by its determination and its internal knowledge of the systems and organisational processes. This can make it formidable and provide it with substantial power to do harm.* |
| **PATHOLOGICAL ATTACKER** | The motivations of this attacker's profile are of a pathological or opportunistic nature and are sometimes guided by the motive for a gain (examples: unfair competitor, dishonest client, scammer, fraudster).<br>*Here, either the attacker has a knowledge base in computing that leads him to attempt to compromise the IS of his target, or he himself uses the attack kits available on-line, or he decides to subcontract the IT attack by calling upon a specialised outfit. In certain cases, the attacker can direct his attention to an internal source (discontented employee, unscrupulous service provider) and attempt to corrupt the latter.* |

---

3 Mention can be made of the services of the type Crimeware as a Service (CaaS).

# CATEGORIES OF TARGET OBJECTIVES

| END PURPOSES | DESCRIPTION |
|---|---|
| SPYING | Intelligence operation (state-related, economic). In many cases, the attacker aims for a long-term installation in the information system and with total discretion. Weaponry, space, aeronautics, the pharmaceutical sector, energy and certain activities of the State (economics, finance, foreign affairs) are privileged targets. |
| STRATEGIC PRE-POSITIONING | Pre-positioning generally aims at an attack over the long term, without the end purpose being clearly established (examples: compromising telecom operator networks, infiltration of mass information Internet sites in order to launch an operation of political or economic influence with a strong echo). Sudden and massive compromising of computers in order to form a botnet can be affiliated with this category. |
| INFLUENCE | Operation aimed at diffusing false information or at altering it, mobilising opinion leaders on the social networks, ruining reputations, disclosing confidential information, degrading the image of an organisation or of a State. The end purpose is generally to destabilise or modify perceptions. |
| OBSTACLE TO FUNCTIONING | Sabotage operation aimed for example at making an Internet site unavailable, causing information saturation, preventing the use of a digital resource, making a physical installation unavailable.<br>Industrial systems can be particularly exposed and vulnerable through IT networks with which they are interconnected (example: sending commands in order to generate hardware damage or a breakdown requiring extensive maintenance. Distributed denial of service attacks (DDoS) are commonly-used techniques for neutralising digital resources. |
| LUCRATIVE | Operation aiming for a financial gain, either directly or indirectly. Generally linked to organised crime, mention can be made of: fraud on the Internet, money laundering, extortion or embezzlement, financial market manipulation, forgery of administrative documents, identity theft, etc.<br>Note that certain operations for profit can make use of a method of attack that is part of the categories hereinabove (example: spying and data theft, ransomware in order to neutralise an activity) but the end purpose remains financial. |
| CHALLENGE, FUN | Operation aiming at fulfilling an exploit for the purposes of social recognition, challenge or simply for fun.<br>Although the objective is primarily for fun and without any particular desire to harm, this type of operation can have serious consequences for the victim. |

# 2 / Formalisation of the RO/TO pairs

**The analysis of the RO/TO pairs can be documented in a table, such as the one suggested hereinafter (P1: RO/TO priority pair, P2: secondary pair):**

| IDENTIFICATION | | SCORING | | | CHARACTERISATION | | | | ASSESSMENT | |
|---|---|---|---|---|---|---|---|---|---|---|
| Risk origin (RO) | Target objective (TO) | Moti-vation | Re-sources | *Acti-vity* | *Me-thods of attack* | *Activity sectors* | *Attack arsenal* | *Exploits* | Perti-nence of the RO/TO pair | Selec-tion P1/P2 |

The resource include both the financial and hardware capacities of the risk origin, and its level of skill in terms of cyber-attacks. This skill can also be sought from specialised outfits **(sophistication of the methods of attack, arsenal of attack tools, etc.)**

Information in *italics* is optional. It makes it possible to better characterise the risk origins and generally requires the support of advanced expertise or solid knowledge in threat analysis.

The level of pertinence of a RO/TO pair can be accessed from the level of motivation, resources and the activity. In the absence of enough information on the activity of the risk origin in your sector, you can assess each RO/TO pair based solely on its motivation and its resources, by using for example the metric hereinafter:

| | | Motivation | | |
|---|---|---|---|---|
| | | **+** | **+ +** | **+ + +** |
| **Resources** | **+ + +** | MEDIUM | HIGH | HIGH |
| | **+ +** | LOW | MEDIUM | HIGH |
| | **+** | LOW | LOW | MEDIUM |

A representation on visual maps of the radar type is also recommended in order to facilitate selecting priority RO/TO pairs and enhancing the results of the workshop. In the illustration hereinafter, two viewing angles are shown (by risk origins and by target objectives), which makes it possible to refine the use of the workshop results. The radial distance corresponds to the level of pertinence assessed for the element (the closer the circles are to the centre, the more dangerous they are considered to be for the organisation). Selecting RO/TO pairs is done by favouring pairs that are located near the centre and which are sufficiently separated from one another, in order to obtain a panel of risk origins and target objectives that is varied.

METHODOLOGICAL SHEET

# 5
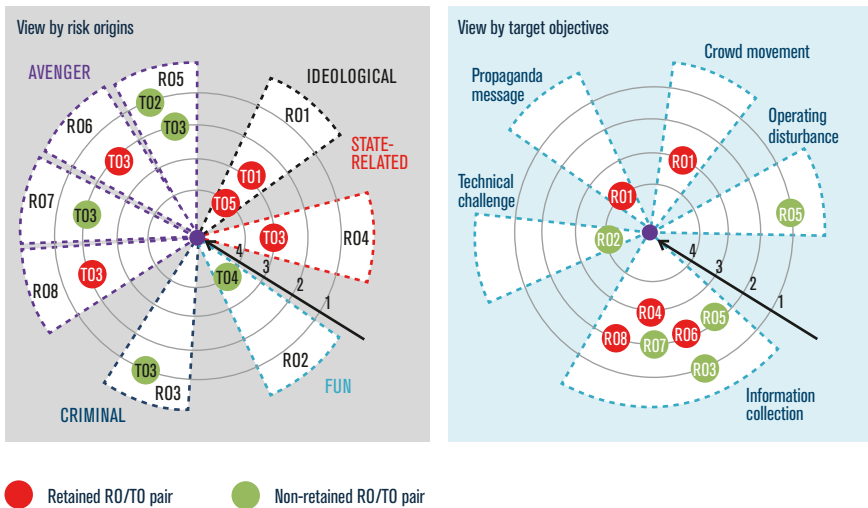
**Building the digital threat mapping of the ecosystem (Workshop 3)**

# 1 / Who are the stakeholders to be taken into account?

The stakeholders to be taken into consideration can be of two types:

**EXTERNAL STAKEHOLDERS:**
- clients;
- partners, co-contractors;
- service providers (subcontractors, suppliers);

**INTERNAL STAKEHOLDERS:**
- technical related services **(example: support services proposed by IT department / Information management team);**
- business related services **(example: commercial entity using business data);**
- subsidiaries (in particular located in other countries).

The number of stakeholders within an ecosystem can be very high and therefore difficult to manage. The project manager, with the assistance of the CISO, is responsible for defining the categories of stakeholders to be assessed first and foremost and as such make a first selection. For example, the project manager can choose to include only some stakeholders internal to the organisation in the analysis scope. We recommend that you establish separate maps for the stakeholders that are internal to your organisation and those that are external to it, because the security measures will certainly be formalised differently in contracts.

**EXAMPLE** : **support services, business services.**

We also recommend, if it is relevant, that you establish a map of the stakeholders by life or mission phase, which will make it possible on one hand to segment the assessment efforts, and on the other hand to identify the stakeholders that constantly induce a threat with regards to the studied object and those that represent a threat only during certain steps.

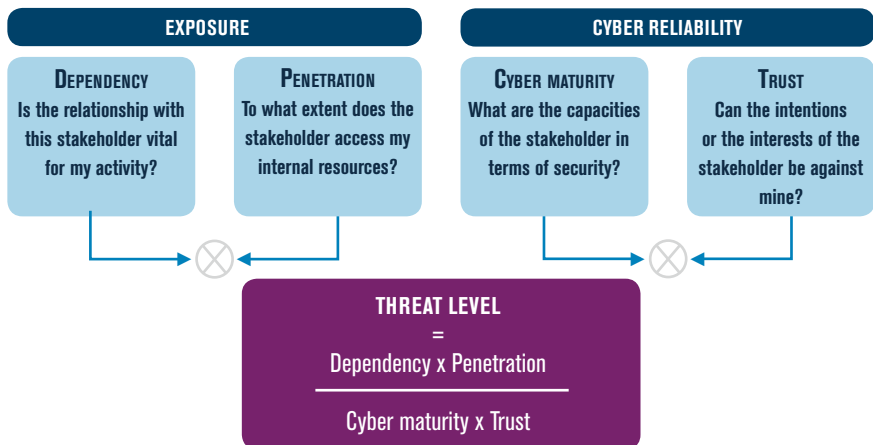**EXAMPLE** : **operations, maintenance.**

**NOTE**: the risk origins identified in workshop 2 are not to be taken into account as such when carrying out this step. The stakeholders that can also be considered as risk origins are here studied solely as stakeholders.

**EXAMPLE** : **partner company in the context studied but a competitor elsewhere.**

◆

# 2 / How to assess the threat level that the stakeholders represent with respect to the object studied?

We suggest the assessment criteria hereinafter. The exposure criteria tend to increase the threat while those concerning cyber reliability attenuate it.



| EXPOSURE | | CYBER RELIABILITY | |
|---|---|---|---|
| **DEPENDENCY** Is the relationship with this stakeholder vital for my activity? | **PENETRATION** To what extent does the stakeholder access my internal resources? | **CYBER MATURITY** What are the capacities of the stakeholder in terms of security? | **TRUST** Can the intentions or the interests of the stakeholder be against mine? |

THREAT LEVEL
=

$$\frac{\text{Dependency x Penetration}}{\text{Cyber maturity x Trust}}$$

**NOTE:** the calculation formula hereinabove is generic and will enable you to carry out a preliminary assessment. If you wish to refine it according to the context, you can calibrate it in order to enhance some criteria that seem preponderant in comparison with others. For example, in order to express greater sensitivity at the cyber maturity level, you can weigh the maturity criterion in the previous expression. In the same way, if you feel that a stakeholder will be used to its own detriment as a simple intermediary by an attacker, then the trust criterion will not be preponderant and could be taken out of the formula.

A metric for scoring each criterion is suggested hereinafter. Here again, do not hesitate to adapt it to the context of your activity and to the object studied.

| | DEPENDENCY | PENETRATION | CYBER MATURITY | TRUST |
|---|---|---|---|---|
| 1 | Relationship not required for strategic functions | No access or access with user privileges to user terminals (work station, mobile phone, etc.). | IT rules are applied on a one-off basis and are not formalised. The capacity to react to an incident is uncertain. | The intentions of the stakeholder cannot be assessed. |
| 2 | Relationship useful for strategic functions | Access with administrator privileges to user terminals (computer equipments, set of mobile terminals, etc.) or physical access to the sites of the organisation. | The IT and regulatory rules are taken into account, without integration into a global policy. Digital security is conducted according to a reactive mode. | The intentions of the stakeholder are considered to be neutral. |
| 3 | Relationship is essential but not exclusive. | Access with administrator privileges to "business" servers (file server, database, web server, application server, etc.). | A global policy is applied in terms of digital security. The latter is provided according to a reactive mode, seeking to centralise and anticipate some risks. | The intentions of the stakeholder are known and are probably positive. |
| 4 | Relationship is essential and unique (no possible substitution in the short term) | Access with administrator privileges to infrastructure equipment (directories, DNS, DHCP, switches, firewall, hypervisors, storage arrays, etc.) or physical access to the server rooms of the organisation. | The stakeholder implements a risk management policy. The policy is integrated and is carried out proactively. | The intentions of the stakeholder are perfectly known and fully compatible with those of the studied organisation. |

The stakeholders of the ecosystem have been assessed according to the aforementioned metric:

| CATEGORY | STAKEHOLDER | DEPENDENCY | PENETRATION | MATURITY | TRUST | THREAT LEVEL |
|---|---|---|---|---|---|---|
| CLIENTS | C1 – Healthcare institutions | 1 | 1 | 1 | 3 | 0.3 |
| | C2 – Pharmacies | 1 | 1 | 2 | 3 | 0.2 |
| | C3 – Depositories and whole-sale distributors | 1 | 2 | 2 | 3 | 0.3 |
| PARTNERS | P1 – Universities | 2 | 1 | 1 | 2 | 1 |
| | P2 – Regulators | 2 | 1 | 2 | 4 | 0.3 |
| | P3 – Laboratories | 3 | 3 | 2 | 2 | 2.25 |
| SERVICE PROVIDERS | F1 – Industrial chemical suppliers | 4 | 2 | 2 | 3 | 1.3 |
| | F2 – Manufacturing equipment suppliers | 4 | 3 | 2 | 3 | 2 |
| | F3 – IT service provider | 3 | 4 | 2 | 2 | 3 |

# 3 / Which representation should be adopted?

The following radar representation is suggested. The radial distance corresponds to the threat level according to the assessment scale used. The more a stakeholder poses a substantial digital threat for the object studied, the closer it will be to the centre.
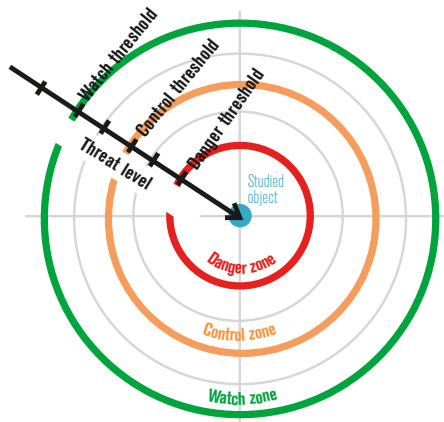
Stakeholders that are located in the danger and control zones must be included in the risk assessment scope because they risk being exploited by an attacker. Concretely, these so-called critical stakeholders must be taken into account when developing strategic scenarios.

**DANGER ZONE:** zone for which the threat level is considered to be very high and difficult to accept. Consequently, no stakeholder should be located in this zone. The security measures that are subsequently taken must remove the stakeholder from this zone.

**CONTROL ZONE:** zone for which the threat level is considered to be high but tolerable under control. The stakeholders in this zone must be subject to special vigilance and are intended, in the middle term, to move to a less threatening position through measures to reduce the risk.
**EXAMPLE : enlistment in the risk management organisation.**

**WATCH ZONE:** zone for which the threat level is considered to be low and acceptable as is. The stakeholders in this zone can be watched without being taken into account in the development of strategic scenarios.

**OUT-OF-SCOPE:** the stakeholders located outside the watch zone represent a threat level that is deemed as negligible. They are not subjected to any risk treatment.

# 4 / How to set the values that define the threat zones?

Choosing the threshold values – watch, control, danger – is the responsibility of the project governance according to the feedback available, the risk appetite and the target ambitions. The project manager or the CISO should provide their expertise in defining relevant values. In practice, these values are often defined after assessment of all of the stakeholders, so as to obtain a fair balance in the acceptance of the risk linked to the ecosystem. It is in general easier to adjust the values via a difference with regards to thresholds that are set more or less approximately. Two methods are as such proposed.

**DANGER THRESHOLD:** it can be set in reference to a stakeholder considered as being at the limit of admissibility, either to exclude it, or to include it. Determining this threshold will result in substantial consequences on the security policy: the latter will have to make it possible to reduce the associated risk below the danger threshold or refuse to establish or maintain the corresponding interaction.

**CONTROL THRESHOLD:** it can be set by using prior attacks as a reference that occurred in a comparable context. The value of this threshold is decisive for the rest of the analysis because it results in taking the stakeholders into account in developing strategic scenarios.

**WATCH THRESHOLD:** it is less decisive but defines the sensitivity relative to the taking or not taking account of the stakeholders in the following of residual risks.

If you feel you are lacking in feedback and in the absence of decision from the project governance, you can set your threshold values as follows, once the assessment of all of the stakeholders has been conducted:

■ Danger scope: 10% of the stakeholders with the highest threat levels.
■ Control scope: 40% of the next stakeholders.
■ Watch scope: 40% of the next stakeholders.
■ Out-of-scope: the remaining 10%.

◆

# 5 / Which degree of depth to choose?

As an initial approach and without any other analysis, you can begin by establishing your threat map by considering only the stakeholders that directly interact with the studied object (rank 1 stakeholder).

To refine this analysis, then iteratively consider the rank 2 and rank 3 stakeholders, in particular if they are linked to a rank 1 stakeholder deemed as critical. The following rules can assist you in adjusting this degree of depth:

■ stakeholder located within the danger scope: assessment of the related stakeholders to rank 3;
■ stakeholder located within the control scope: assessment of the related stakeholder to rank 2;
■ non-critical stakeholder (outside the control scope): no further in-depth analysis of the related stakeholders.
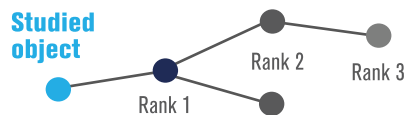
■ In order to guarantee readability, rank 1 stakeholders will be represented first and foremost on the radar map. Rank 2 and 3 stakeholders may also appear according to their threat level.

METHODOLOGICAL SHEET

# 6

◆

**Defining security measures
for the ecosystem (Workshop 3)**
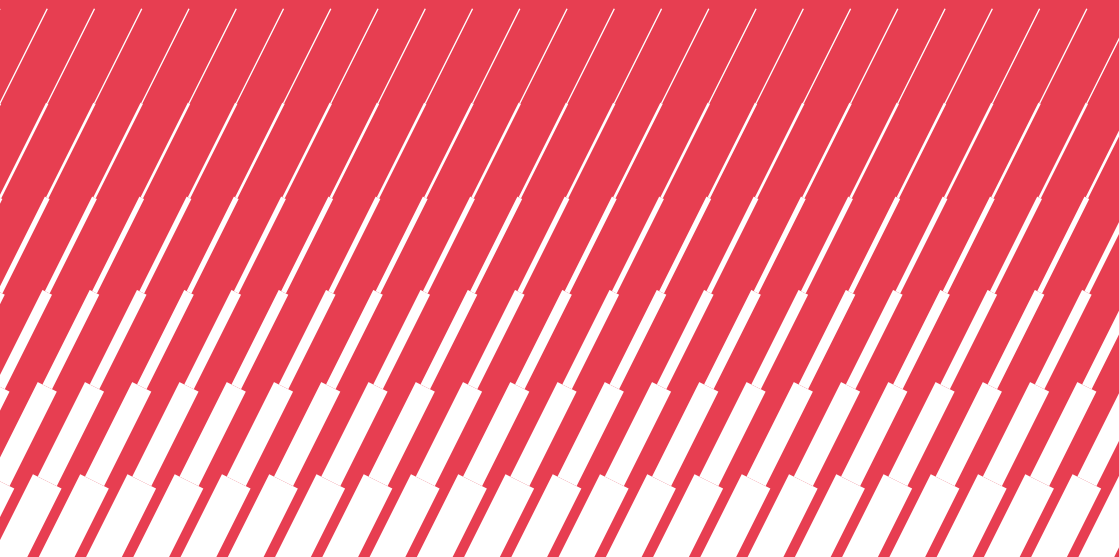
According to the threat level of a stakeholder with regards to the studied object, security measures can be set up. The following set of rules can as such be adopted, with the entry criterion being the threat level assessed for the stakeholder:

| THREAT LEVEL | ACCEPTABILITY | RECOMMENDATIONS OF ACTIONS |
|---|---|---|
| VERY HIGH – DANGER ZONE | Unacceptable | No stakeholder in this zone: reduction of the risk, or refusal to establish interaction. |
| HIGH – CONTROL ZONE | Tolerable under control | Enlistment of the stakeholder in the risk management process:<br>- specific monitoring, and even increased, in terms of cyber defence;<br>- technical and organisational security audit;<br>- reduction/transfer of the risk in a security continuous improvement plan. |
| LOW – WATCH ZONE | Acceptable as is | Not applicable (residual threat). |

You can define an initial orientation by proposing a criterion to focus on first (for example: increasing the trust or maturity, decreasing penetration or dependency). These orientations are guided in particular by the following considerations:

■ choosing the most detrimental criterion in the initial situation;
■ choosing the criterion for which an improvement will be obtained at least cost;
■ choosing the criterion that is *a priori* the most effective in light of the strategic scenarios identified.

You can qualify the set of rules hereinabove for stakeholders that are in the danger zone, especially if it appears to be very difficult to get them out of this zone in light of operational constraints.

**EXAMPLE**: **a stakeholder may be tolerated in the danger zone only if its level of maturity and trust are at least 3.**

# 7

# Developing attack graphs (Workshop 4)

An operational scenario can be represented in the form of an attack graph that makes it possible to view the methods of attack planned by the attacker in order to achieve their objective. The attack graph has the form of a **chain of elementary actions on supporting assets**. Several methods of attack can be carried out by the risk origin in order to achieve its target objective: they are represented by different sequential chains before reaching the final step. An example of an operational scenario is provided hereinafter.
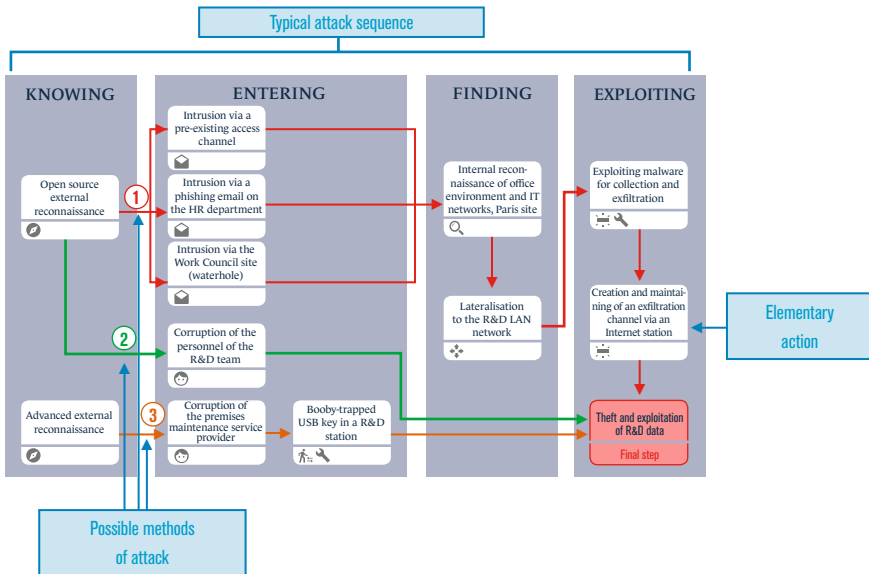
# 1 / Attack sequence model

Operational scenarios can be structured according to a typical attack sequence. The model proposed revolves around 4 phases:

**KNOWING:** all of the activities of external targeting, reconnaissance and discovery conducted by the attacker in order to prepare their attack and increase their chances of success (map of the ecosystem, searching for information on the key persons and systems, searching for and assessing vulnerabilities, etc.). This information is collected by any means possible according to the determination and the resources of the attacker: intelligence, economic intelligence, use of socio-professional networks, direct approaches, specialised outfits for obtaining information that cannot be accessed as an open source, etc.

**ENTERING:** all of the activities conducted by the attacker to digitally or physically enter, either directly and head on into the information system of the target, or into its ecosystem for the purposes of a bouncing attack. The intrusion is generally carried out via "border" supporting assets that are used as entry points due to their exposure.
**EXAMPLE** : user station connected to Internet, a service provider's maintenance tablet, remotely-maintained printer, etc.

**FINDING:** all of the internal reconnaissance activities of networks and systems, lateralisation, raising of privileges and persistence that allow the attacker to locate the sought data and supporting assets. During this phase, the attacker generally seeks to remain discreet and not leave any trails.

**EXPLOITING:** all of the activities of exploiting the data and supporting assets found in the preceding step. For example, in the case of a sabotage operation, this phase includes the triggering of the active load, in the case of a spying operation aiming to exfiltrate emails, this can be setting up and maintaining the discreet capacity of collecting and exfiltrating data.
**EXAMPLE** : ransomware.

You can adopt more sophisticated models of attack sequences and break them down into variants according to the attack technique of the risk origin in order to achieve its objective (data exfiltration, passive listening, denial of service, ransomware, etc.).
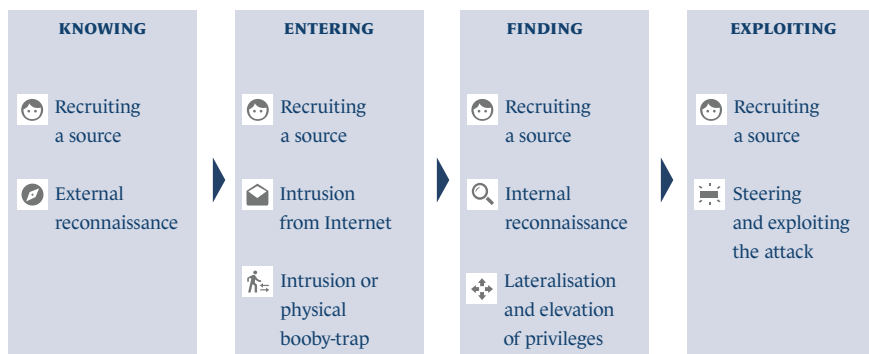
**NOTE:** for the "Entering" phase, we recommend that you distinguish in the sequencing the elementary actions for entering into the information systems of the ecosystem, and those concerning the supporting assets of the studied object. Regarding the ecosystem, you will not always be able to accurately describe what the target supporting assets are for the stakeholder involved. In this case, remain at a macroscopic and functional level (example: office environment IS, production line).

# 2 / Categories of elementary actions and means implemented

◆

The illustration hereinafter proposes a categorisation of elementary actions in liaison with the attack sequence model proposed hereinabove. The means and techniques that are commonly observed are stated for each category of elementary actions (bullet point ◆). Do not hesitate to adapt this base to your context and to enrich it with any information stemming from your watch activities.

**EXAMPLE: usage of bulletins from CERT-FR and cyber-attack watch bulletins.**

| KNOWING | ENTERING | FINDING | EXPLOITING |
|---------|----------|---------|------------|
| Recruiting a source | Recruiting a source | Recruiting a source | Recruiting a source |
| External reconnaissance | Intrusion from Internet | Internal reconnaissance | Steering and exploiting the attack |
| | Intrusion or physical booby-trap | Lateralisation and elevation of privileges | |

**NOTE**: in some cases, when an exfiltration channel is required and is different from the infiltration channel, an intrusion from Internet or via a physical booby-trap can be conducted in the "Exploiting" phase. The initial intrusion can for example be conducted via Internet, but the exfiltration via an ad hoc physical channel set up (the case with isolated systems).

## RECRUITING A SOURCE, CORRUPTION OF PERSONNEL

A "recruiting" operation of a source inside the organisation or that has access to it can be long and complex, but very useful for setting up a hardware booby-trap or obtaining information on the targeted system. The reasons that push a target to betray their entity of origin – potentially unknown to them – are covered by four major categories, referred to as "MICE" (Money, Ideology, Compromise, Ego). Outfits that are specialised in recruiting sources exist.

## EXTERNAL RECONNAISSANCE OF THE TARGET

During the reconnaissance phase, the risk origin will search all of its available databases for the information required to plan its attack. The data collected can be of a technical nature or concern the organisation of the target and of its ecosystem. The means used can vary greatly:

♦ social networks (social engineering);
♦ Internet (digital trash bins, sites);
♦ discussion forums on Internet;
♦ professional forums and events;
♦ fake client, fake journalist, etc.;
♦ direct contact (former employees, etc.);
♦ specialised outfits or agencies (non-open sources);
♦ electromagnetic intelligence (interceptions).

## INTRUSION FROM INTERNET OR THIRD-PARTY IT NETWORKS

The purpose of the initial intrusion is to introduce a malicious tool into the targeted information system or into another that belongs to the ecosystem (for example the supply chain), generally at the level of an entry supporting asset that is more particularly exposed. Ideally for the attacker, the initial intrusion of the malicious tool is carried out from Internet. The most commonly used intrusion vectors and techniques are:

♦ direct attacks against services exposed on Internet;
♦ phishing or spearfishing emails;
♦ attacks via servers that are specifically administered for this purpose or compromised (so-called waterhole attacks);
♦ the booby-trap of an apparently legitimate update.

## INTRUSION OR PHYSICAL BOOBY-TRAP

This method of intrusion is used to physically access resources of the information system in order to compromise it. It can be carried out by an external person or simplified through the recruiting of a source internal to the targeted organisation. Physical intrusion is in particular useful for the attacker who wants to access a system that is isolated from Internet, which requires crossing one or more air gaps. Commonly used physical intrusion techniques are provided below:

♦   knowledge of connection identifiers;
♦   compromise of the machine (e.g.: booby-trapped USB key);
♦   connecting to the network of a piece of hardware that is external to the information system;
♦   intrusion via a poorly-secured wireless network;
♦   booby-trapping of a piece of hardware upstream of the supply chain (so-called supply chain attack);
♦   abusive use of legitimate means of access to the information system.

**EXAMPLE : theft and use of a professional mobile phone of an employee.**

## INTERNAL RECONNAISSANCE

Generally, after the initial intrusion, the attacker is in an environment of the local network type of which the access can be controlled by directory mechanisms (Active Directory, OpenLDAP, etc.). In fact, they must conduct internal reconnaissance activities that allow them to map the network architecture, identify the protection and defence mechanisms in place, list the vulnerabilities that can be exploited, etc. During this step, the attacker attempts to locate the services, information and supporting assets, objects of the attack. The internal reconnaissance techniques hereinafter are widely used:

- mapping networks and systems in order to conduct propagation (network scan);
- advanced mapping (example: memory dump);
- search for vulnerabilities (for example to facilitate propagation);
- access to critical system data (address plans, safes, passwords, etc.);
- mapping of services, databases and supporting assets of interest for the attacker;
- dissimulation of trails;
- use of generic or customised malware that makes it possible to automate internal reconnaissance.

### LATERALISATION AND ELEVATION OF PRIVILEGES

Starting from their initial point of access, the attackers will implement techniques of lateralisation and elevation of privileges in order to progress and maintain themself in the information system. For them, this generally entails exploiting the internal structural vulnerabilities of the system (lack of network partitioning, insufficient access control, no robust authentication policy, negligence concerning the administration and the maintenance of the information system, absence of supervision, etc.).

- Exploitation of software or protocol vulnerabilities (in particular identified during the reconnaissance);
- Modification or abuse of rights on key user accounts, administrator, machines;
- Other specific techniques: brute force attack, memory dump, "pass-the-hash" attack.

**NOTE**: the internal reconnaissance and lateralisation / elevation of privileges phases are in practice iterative and occur as the attacker progresses through the information system.

### STEERING AND EXPLOITING THE ATTACK

This final step corresponds to the carrying out of the objective that the risk origin is aiming for. According to this objective, this can be for example triggering the destructive malicious load, exfiltering or modifying information. The attack can be one-off (for example in the case of a sabotage operation) or long-lasting and takes place with total discretion (for example in the case of a spying operation aimed at exfiltering information on a regular basis). The means and techniques for exploiting an attack will depend on the target objective. In the case where the latter is sustained over time and needs to be oriented, the attacker will have to set up of steering channel, whether synchronous or asynchronous, and even a physical channel in the case of an air gap.

Hereinafter are a few examples of exploitation techniques used according to the target objective:

#### SPYING

♦   Data exfiltration;

♦   Observation or remote passive listening (drone, listening hardware, etc.);

♦   Interception and exploitation of compromising parasite signals (TEMPEST threat)[4].

---

4 The TEMPEST threat can also be exploited actively by booby-trapping, beforehand, for example via the supply chain, a peripheral device (cable, keyboard, mouse, video projector). It then becomes a source of compromising parasite signals that can be remotely activated and deactivated as long as sufficiently powerful transmitters are available to create a leakage channel.

## OBSTACLE TO FUNCTIONING (SABOTAGE, NEUTRALISATION)

♦ Attack via distributed denial of service (DDoS);
♦ Breach of the integrity of a supporting asset or of data (deletion, encryption, alteration);
♦ Scrambling of a supporting asset (to make it blind or neutralise it);
♦ Lure of a supporting asset (for deceiving or falsifying)[5];
♦ Industrial systems: sending of commands that are at risk for operating security[6];
♦ Intentional electromagnetic interference (IEMI).

## LUCRATIVE (FRAUD, FUNCTION CREEP, FORGERY)

♦ Modification of a database (for example in order to dissimulate fraudulent activity);
♦ Alteration or function creep of a business or support application;
♦ Identity theft (in a logic of abusing rights);
♦ Extortion or embezzlement.

**EXAMPLE** : ransomware, crypto currency miner.

## INFLUENCE (AGITATION, PROPAGANDA, DESTABILISATION)

♦ Defacement of Internet sites;
♦ Diffusion of ideological messages via the taking over of an information channel;
♦ Identity theft (in a logic of undermining the reputation);

---

5 Includes cognitive lure techniques with the purpose of misleading or dissimulating an activity in the eyes of a user (example: illegitimate authentication request, concealed alert message).

6 For example to provoke premature wear of a piece of equipment or modify the alert thresholds on key operating parameters. The fine assessment of the modes for exploiting an attack on an industrial system is indissociable from the operating security analyses.

METHODOLOGICAL SHEET

# 8

◆

# Assessing the likelihood of operational scenarios (Workshop 4)

The likelihood of an operational scenario reflects the degree of feasibility or of the possibility that one of the attacker's methods of attack reaches the target objective. The likelihood is a decision-making indicator. Combined with the severity, it makes it possible to estimate the risk level and to deduce the treatment strategy for the risk.

# 1 / Which likelihood scale should be used?

A scale of levels of likelihood must be understood and able to be used by the persons in charge of assessing the possibility that a risk manifests itself. Developing it can be usefully carried out in collaboration with the persons who will be estimating these levels: as such the values will have a concrete meaning and be coherent.

If you do not have a likelihood scale, draw one up at the beginning of **workshop 4**. For this, you can **use and adapt the generic scale** hereinafter.

| LIKELIHOOD SCALE OF AN OPERATIONAL SCENARIO | |
|---|---|
| **LEVEL OF THE SCALE** | **DESCRIPTION** |
| **V4 – NEARLY CERTAIN** | The risk origin will most certainly reach its objective by following one of the considered methods of attack. The likelihood of the risk scenario is very high. |
| **V3 – VERY LIKELY** | The risk origin will probably reach its objective by following one of the considered methods of attack. The likelihood of the risk scenario is high. |
| **V2 – LIKELY** | The risk origin is able to reach its objective by following one of the considered methods of attack. The likelihood of the risk scenario is significant. |
| **V1 – RATHER UNLIKELY** | The risk origin has relatively little chance of reaching its objective by following one of the considered methods of attack. The likelihood of the risk scenario is low. |
| **V0 – UNLIKELY** | The risk origin has very little chance of reaching its objective by following one of the considered methods of attack. The likelihood of the risk scenario is very low. |

> **NOTE:** the purpose of estimating the likelihood of an operational scenario is not to be predictive (it does not reveal the probability of the risk origin carrying out its attack according to this scenario[7]). However, if the attacker decides to conduct their attack via the method of attack concerned, then its likelihood of succeeding will be that which is estimated.

Use a scale with 4 or 5 levels is guided by the following considerations:

■ the coherency of the number of levels between the severity and likelihood scales (if you use a severity scale with 4 levels, use a likelihood scale with 4 levels);

■ the need to more or less finely estimate these likelihoods.

◆

# 2 / Which approach to choose for scoring the likelihood of the operational scenario?

You can consider three approaches for scoring the likelihood of the operational scenario:

■ express method: direct scoring of the likelihood of the scenario;

■ standard method: scoring of the "probability of success" of each elementary action of the scenario, from the point of view of the attacker.

■ advanced method: in addition to the scoring of the "probability of success", scoring of the "technical difficulty" of each elementary action of the scenario, from the point of view of the attacker.

> **NOTE:** here, the "probability" must not be understood in the mathematical meaning of the term.

---

7 On the contrary, if this scenario was selected after workshops 2 and 3, it is because it is considered to be pertinent.

## a EXPRESS METHOD: DIRECT SCORING OF THE OVERALL LIKELIHOOD OF THE SCENARIO

In the methods presented hereinafter (standard and advanced), the global likelihood of the scenario is assessed using the score of the elementary actions. The express method consists in directly assessing the overall likelihood of the scenario, based on general considerations relating to the risk origin (motivations, resources) and the security of the targeting supporting assets in the scenario (exposure, vulnerabilities). The section "How to score elementary actions?" will provide precious assistance for the assessment. It is possible to assess the methods of attack under consideration on the operational scenario separately and to identify the one that seems to be the most likely.

In this approach, you can:

■ directly estimate the level of likelihood of the scenario;

■ or score its likelihood of success and its technical difficulty for the purpose of deducing via crossing the likelihood of the scenario according to the typical matrix presented hereinbelow.

| | | TECHNICAL DIFFICULTY OF THE OPERATIONAL SCENARIO | | | | |
|---|---|---|---|---|---|---|
| | | 0 – NEGLIGIBLE | 1 – LOW | 2 – MODERATE | 3 – HIGH | 4 – VERY HIGH |
| PROBABILITY OF SUCCESS OF THE OPERATIONAL SCENARIO | 4 – NEARLY CERTAIN | 4 | 4 | 3 | 2 | 1 |
| | 3 – VERY HIGH | 4 | 3 | 3 | 2 | 1 |
| | 2 – SIGNIFICANT | 3 | 3 | 2 | 2 | 1 |
| | 1 – LOW | 2 | 2 | 2 | 1 | 0 |
| | 0 – VERY LOW | 1 | 1 | 1 | 0 | 0 |

## b STANDARD METHOD: PROBABILITY OF SUCCESS OF THE ELEMENTARY ACTIONS

In the standard method, you will score each elementary action according to an index of the probability of success as seen by the attacker. The following scale can be adopted, the percentage chances are mentioned for the purposes of information in order to facilitate the scoring:

| SCALE OF PROBABILITY OF THE SUCCESS OF AN ELEMENTARY ACTION | |
|---|---|
| **LEVEL OF THE SCALE** | **DESCRIPTION** |
| **4 – NEARLY CERTAIN** | Probability of success is nearly certain > 90% |
| **3 – VERY HIGH** | Probability of success is very high > 60% |
| **2 – SIGNIFICANT** | Probability of success is significant > 20% |
| **1 – LOW** | Probability of success is low < 20% |
| **0 – VERY LOW** | Probability of success is very low < 3% |

For example, an index of "3 – Very high" for an elementary action of intrusion via booby-trapped email (spearfishing) will mean that you feel that the attacker has very good chances of succeeding in their action, i.e. that one of the users targeted by the spearfishing campaign will click on the booby-trapped attachment.

> **NOTE:** the scales for scoring elementary actions must have as many levels as the likelihood scale.

# C ADVANCED METHOD: PROBABILITY OF SUCCESS AND TECHNICAL DIFFICULTY OF THE ELEMENTARY ACTIONS

**In the advanced method,** you will also score the technical difficulty of carrying out the elementary action, from the point of view of the attacker. It makes it possible to estimate the resources that the attacker will have to implement in order to carry out their action and increase their chances of success. The following scale can be adopted:

| SCALE OF TECHNICAL DIFFICULTY OF AN ELEMENTARY ACTION | |
|---|---|
| LEVEL OF THE SCALE | DESCRIPTION |
| 4 – VERY HIGH | Very high difficulty: the attacker will implement very substantial resources in order to carry out their action. |
| 3 – HIGH | High difficulty: the attacker will implement substantial resources in order to carry out their action. |
| 2 – MODERATE | Moderate difficulty: the attacker will implement significant resources in order to carry out their action. |
| 1 – LOW | Low difficulty: the resources implemented by the attacker will be low. |
| 0 – NEGLIGIBLE | Negligible difficulty, or even zero: the resources implemented by the attacker will be negligible or already available. |

**NOTES:**

■ The advanced method allows for a finer appreciation of the likelihood: it takes into account the level of expertise and the resources that the attacker will need to carry out their attack, in light of the security of the targeted system. In fact, this method makes it possible to consider the return on investment for the attacker and therefore to build a risk treatment strategy that is driven by a logic of discouragement.

■ The "technical difficulty" and "probability of success" scoring criteria are not rigorously independent. However, the "technical difficulty" is more particularly linked to the level of protection of the target (its exposure and its vulnerabilities), while the "probability of success" is further influences by its level of defence and resilience (capabilities of supervision, of reaction in case of an incident and continuity of activity).

# 3 / Standard and advanced methods: how to score elementary actions?

Scoring elementary actions is not necessarily easy. Indeed, it must take account of and confront:

■ on the one hand the motivation / determination and the resources / capacities of the risk origin;

■ on the other hand the security of the targeted system within its ecosystem.

The scoring can be carried out via the judgement of an expert, which entails having available in the working group expertise that is sufficient in cyber-attacks and fine knowledge of the level of security of the studied object within its ecosystem. In order to assist you in the work of scoring and in order to make it more objective and reproducible, you will find at the end of the sheet the main criteria for determining the probability of success or the technical difficulty of an elementary action.

# 4 / Standard and advanced methods: how to calculate the likelihood of the operational scenario?

## a STANDARD METHOD

In the preceding step, you scored each elementary action according to an index of the probability of success. You can assess the global index of the probability of success of the scenario by applying the following rule. The principle is to progress in a method of attack by assessing step-by-step at each elementary action "AEn" of a node "n", an intermediate cumulative probability index of "AEn" and of the intermediate cumulative index of the preceding node "n-1":

$$\text{Indice\_Pr}(AE_n) = \text{Min}\left\{\text{Indice\_Pr}(AE_n), \text{Max}(\text{Indices\_Pr}(AE_n\_1))\right\}$$

*intermediate cumulation*           *intermediate cumulations*

The global index of the probability of success (final step) is obtained by taking the highest intermediate cumulative probability index from among the methods of attack that reach the final step. It corresponds to the method(s) of attack of which the chance of success appears to be the highest.

**NOTE:** the calculation rule hereinabove allows for a relative simply and fast assessment of the global index of the probability of success. It does however reach its limits when a sequence of a method of attack comprises a long chain of steps in series (**about ten or so as an indication**)[8]. The assessment will then tend to overestimate the probability of success of the corresponding method of attack, resulting in an overestimated likelihood of the operational scenario. For the sequences of the method of attack concerned, you can compensate this limit by decreasing the intermediate cumulative probability index obtained at the end of the sequence by one level.

---

8   Especially if the corresponding elementary actions have identical index of the probability of success.

The **likelihood of the operational scenario** obtained at the end of these operations corresponds to the global probability index of success.

---

**EXAMPLE** : biotechnology company manufacturing vaccines.

The assessment of the likelihood was carried out with 4-level scales:

■  For the probability of success: "Pr 1" – low probability to "Pr 4" – nearly certain.

■  For the likelihood: "V1" – rather unlikely to "V4" – nearly certain.

The intermediate cumulative probability index are indicated in parentheses and *in italics*.
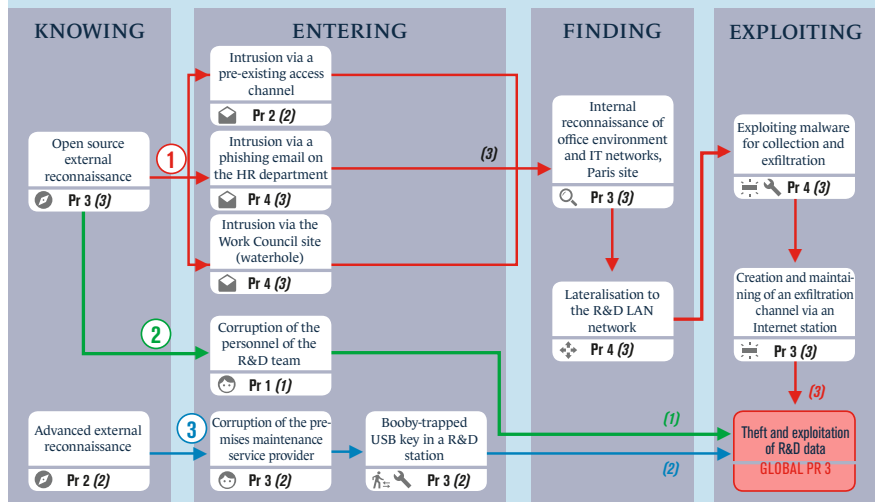


The global probability index of success of the scenario is estimated at "3 – Very high": reaching the target objective by the risk origin according to one or the other of the methods of attack of the operational scenario is considered as **very likely (V3)**. The easiest or most feasible method of attack is the red one numbered ①.

## b ADVANCED METHOD

Begin by calculating the global probability index of success of each method of attack of the operational scenario according to the approach explained hereinabove.

Then calculate the technical difficulty index of each method of attack according to the particulars hereinafter. The principle is to progress in a sequence of a method of attack by assessing step-by-step at each elementary action "AEn" of a node "n", an intermediate cumulative difficulty index using the elementary difficulty of "AEn" and of the intermediate cumulative difficulties of the preceding node "n-1":

$$(AE_n) = \text{Max} \left\{ \text{Indice\_Diff}(AE_n), \text{Min (Indices\_Diff}(AE_n\_1)) \right\}$$
$$\text{\textit{intermediate cumulations}}$$

**NOTE:** the calculation rule hereinabove allows for a relative simply and fast assessment of the global index of technical difficulty. It does however reach its limit when a sequence of a method of attack comprises a long chain of steps in series (about ten)[9]. The assessment will then tend to underestimate the difficulty of the corresponding method of attack, resulting in an underestimated likelihood of the operational scenario. For the sequences of the method of attack concerned, you can compensate this limit by increasing the intermediate cumulative difficulty index obtained at the end of the sequence by one level.

Finally, deduce the global likelihood of the operational scenario by proceeding as follows[10]:

---

9 Especially if the corresponding elementary actions have identical difficulty index.

10 You can also retain for the likelihood the one obtained by crossing the global probability index of success and the global index of technical difficulty obtained. But your result may be skewed in case of crossing probability and difficulty index that relate to different methods of attack. In this case the likelihood of the operational scenario would be overestimated.

- evaluate the level of likelihood of each method of attack that reaches the final step, by using the crossed chart hereinafter (which may be adapted);
- the level of likelihood can then be weighted for the operational scenario and that of the most likely method of attack;
- this level of likelihood can then be weighted according to the nature of the risk origin (motivation and resources). If you feel that the latter is particularly determined to achieve its objectives – and therefore is ready to engage substantial means and persevere in case of successive failures –, then you may decide to increase the level of likelihood obtained by one level.
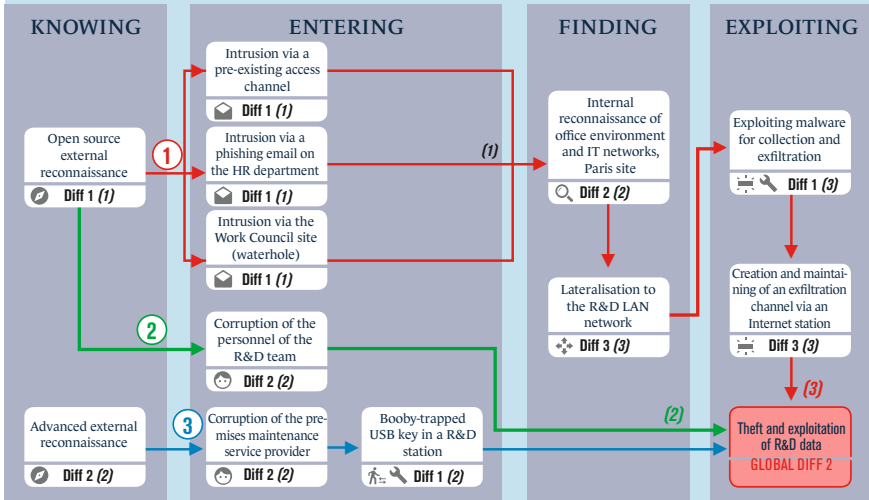
| | | TECHNICAL DIFFICULTY OF THE METHOD OF ATTACK | | | | |
|---|---|---|---|---|---|---|
| | | 0 – NEGLIGIBLE | 1 – LOW | 2 – MODERATE | 3 – HIGH | 4 – VERY HIGH |
| PROBABILITY OF SUCCESS OF THE METHOD OF ATTACK | 4 – NEARLY CERTAIN | 4 | 4 | 3 | 2 | 1 |
| | 3 – VERY HIGH | 4 | 3 | 3 | 2 | 1 |
| | 2 – SIGNIFICANT | 3 | 3 | 2 | 2 | 1 |
| | 1 – LOW | 2 | 2 | 2 | 1 | 0 |
| | 0 – VERY LOW | 1 | 1 | 1 | 0 | 0 |

**NOTES:**

■ The model assumes that the probabilities of success are independent from one another, which is not necessarily true. The same remark applies for the technical difficulties. On the other hand, for certain categories of actions (such as the corruption of a member of the personnel), the probability of success can depend on the difficulty, which is not captured by default in the model.

■ Using a software for building and scoring attack graphs is strongly recommended.

**EXAMPLE** : biotechnology company manufacturing vaccines.

The intermediate cumulative difficulty index are indicated in parentheses and in *italics*.



The technical difficulty of the scenario is estimated globally at "2 – Moderate", the least technically difficult methods of attack are those numbered ② and ③. In light of the probabilities of success assessed hereinabove, it is possible to establish the following summary:

|  | Probability of success | Technical difficulty | Likelihood |
|---|---|---|---|
| Path ① | 3 – Very high | 3 – High | V2 – Likely |
| Path ② | 1 – Low | 2 – Moderate | V2 – Likely |
| Path ③ | 2 – Significant | 2 – Moderate | V2 – Likely |
| | | Global scenario | V2 – Likely |

The three methods of attack considered in the attack graph have the same level of likelihood. A likelihood of **"V2 – Likely"** is the result for the scenario. With respect to the assessment carried out with the standard method (V3), the estimated likelihood is lower. Taking the technical difficulty criterion into account contributes a weighting on the estimation of the level of likelihood. Indeed, if the method of attack ① appears to have the highest probability of success, it also has a relatively high technical difficulty.

# 5 / Elements for assistance in scoring elementary actions

This section presents for each category of elementary action (**refer to methodological sheet n°7**) the major elements that determine its probability of success or technical difficulty.

## RECRUITING A SOURCE

- Many potential targets having access to the targeted information, to the critical supporting assets or to their physical environment **(Note 1)**.
- Personnel, service providers, suppliers able to be driven by a spirit of vengeance.
  **EXAMPLE : discontented recently dismissed employee.**
- Personnel having undergone a process of security authorisation and/or an investigation, which provide a certain level of assurance on their integrity.
- Satisfaction of the targets regarding their wages or how they are considered within the organisation.
- Adhesion of the potential targets to the values of the company **(Note 2)**.

**Note 1 :** the more numerous the potential targets are, the easier it will be for the attacker to find a target that can be corrupted.
**Note 2 :** persons who are poorly considered and poorly paid will naturally be easier to corrupt. These levers must not be underestimated.

## EXTERNAL RECONNAISSANCE

- Information on the entity and on its ecosystem that are easy to access over the Internet (websites, on-line chat forums, socio-professional networks, etc.).
- Regular participation of the entity, of its partners (suppliers, subcontractors, clients) or of former employees in professional events or on-line forums **(Note 3)**.
- Use of encryption in the entity's relationships with the outside, in the services offered by the entity to the outside **(Note 4)**.
- Special skills required to search for information, in light of the entity's field of activity **(Note 5)**.

**Note 3 :** a lot of information is easily obtained through informal approaches in professional contexts. During commercial approaches in particular, many sensitive information is often exchanged
**EXAMPLE**: fake client, response to a call for tender.
**Note 4 :** encryption protocols make it possible to limit the impact of data leakage, in particular with respect to interceptions or diverting of traffic.
**Note 5 :** attacks that require strong skills in one or more fields of expertise in liaison with the activity of the target
**EXAMPLE**: air traffic control, nuclear, radiological, bacteriological and chemical risks, railway signalling, are naturally more expensive and difficult to identify and treat than attacks that implement methods that are primarily technical.

# INTRUSION FROM INTERNET

*The criteria differ according to the intrusion technique used by the attacker.*

## HEAD-ON ATTACK OF SERVICES

- Number of services and/or applications exposed on the Internet.
- Exposed services that have been approved or that been subjected to a development process that integrates security.
- The filtering technology in place
  **EXAMPLE** : **REVERSE PROXY, WAF, ETC.** **(Note 6)**.
- Use of "border" supporting assets that are certified or qualified **(Note 7)**.

**Note 6** : these tools operate based on signatures and are rather effective in detecting the roughest attacks.

**Note 7** : a qualified or certified technology is more robust with regards to exploits, as it is subject to increased development quality, with substantial attention given to security, and has undergone intrusion tests

**EXAMPLE** : first level security certification, common criteria, accreditation, general security mechanism.

## PHISHING / WATERHOLE

Number of users likely to be targeted **(Note 8)**.

- Users who are regularly made aware and trained in reacting to phishing and waterhole attacks.
- Effective anti-spam filter in place **(Note 9)**.
- Filtering capacity of Internet browsing for users in place
  **EXAMPLE** : PROXY, IPS **(Note 10)**.
- Filtering of Internet sites based on a white list (list of authorised sites) **(Note 11)**.

**Note 8** : the more users there are, the easier it is to test several targets until one of them performs the expected operation.

**Note 9 :** this type of tool is rather effective in detecting the roughest attacks (mass phishing, for example the sending of a booby-trapped email containing non-targeted ransomware).

**Note 10 :** solutions for filtering browsing make it possible to both filter what is known to host malicious activity and to log the traffic for the purposes of in-depth investigation in the framework of security supervision.

**Note 11 :** the browsing authorised by white lists are relatively complex to get around for an attacker who wants to conduct a waterhole attack.

## INTRUSION VIA A WIRELESS NETWORK

- Existence of wireless (Wi-Fi) networks in the entity's office or industrial environment.
- Secure Wi-Fi access, for example according to ANSSI's technical guide[11].

---

11 Note technique – Recommandations de sécurité relatives aux réseaux Wi-Fi, ANSSI, 2013.

## INTRUSION VIA SOFTWARE OR A LEGITIMATE PATCH

- Existence of a security policy relating to software updates, business applications and firmware **(Note 12)**.
- Sources and channels of trust (even certified or qualified), verification of the identity of the signatories for the updates.

**Note 12** : setting up measures for securing software and firmware updates can make it much more difficult for an attack of the Trojan horse type.

Examples of measures: antivirus sandbox (certified) before applying updates, procedures for controlling the integrity of patches and hot fixes.

## INTRUSION OR PHYSICAL BOOBY-TRAP

- Control of interventions by service providers: access management for the premises, supervision, logging, etc.**(Note 13)**.
- Security authorisation process or preliminary investigation conducted for the service providers that intervene on site.
- Use of IT hardware managed by the organisation so that the service providers carry out the interventions on the supporting assets of the entity

`EXAMPLE`: maintenance tool case, firmware USB key **(Note 14).**

- Number and facility of access to physical and logical connection points of the entity's IT networks.
- Existence of remote-maintenance links or connections with secure third-party networks.
- Existence of a security policy for the industrial supply chain

`EXAMPLE`: contractual requirements, supplier security audits, etc.

- Existence of security measures for the maintenance of support assets **(Note 15)**.
- Existence of physical security measures and type of technology used: access control

`EXAMPLE`: gantry, badge, entry code, biometrics, video protection, etc.

- Supervision of the physical security and reactivity of the intervention teams in the event an intrusion is detected(on site, remotely, 24/7, only during business hours).
- Number of barriers to cross to physically access the critical supporting assets **(Note 16)**.

- Security personnel trained on the risk of the physical introduction of listening hardware.
- Users who are made aware, and even trained, on vigilance with respect to physical intrusions.
- Mutual knowledge of the persons who can have legitimate access.
- Existence of a security policy for professional travel, awareness of the employees as to the risks during their missions.

**Note 13 :** interventions conducted outside business hours or in the absence of any vigilance/human presence facilitate fraudulent or illegitimate activity. The same is true if a service provider has an access badge that allows it to circulate freely in all of the zones.

**Note 14 :** the fact that a service provider uses its own means of intervention to, for example, perform maintenance on an automatic machine or the updating of an IT network, increases the risk of introducing malicious code whether or not targeted, possibly without the service provider even being aware.

**Note 15 :** examples of measures: removal of non-volatile memory storage media, physical sealing, application of ANSSI's reference standards concerning the integration and the maintenance of industrial systems.

**Note 16 :** it is recommended that there are at least three physical barriers to access the critical supporting assets.

# INTERNAL RECONNAISSANCE

# LATERALISATION, ELEVATION OF PRIVILEGES

The major elements that affect the probability of success or the technical difficulty of internal reconnaissance, a lateralisation or of an elevation of privileges; are relatively similar and are grouped together.

- Users that have administrator rights on their workstation **(Note 17)**.
- Existence of a policy for managing user profiles and their access rights, of the least privilege principle.
- Remote connections to the systems limited to machines dedicated for administration, with no access to the Internet.
- Existence of a security operating centre (SOC).
- Existence of an authentication policy on the networks **(Note 18)**.
- Partitioning of the entity's IT networks by trust domains or data sensitivity (for example according to ANSSI's recommendation guides).
- Secured administration of networks and services (for example according to ANSSI's recommendation guides).
- Level of heterogeneity of the IT base **(Note 19)**.
- Number and specificity of the services offered by the information system **(Note 20)**.
- Facility of access to critical data **(Note 21)**.

**Note 17 :** the fact that a user has administrator rights on their workstation greatly facilitates the operations of internal reconnaissance, lateralisation and the elevation of privileges.

**Note 18 :** examples of means of authentication from the most secure to the least secure: strong authentication, password with a restrictive policy, password without a policy, no authentication.

**EXAMPLE : smart card**.

**Note 19 :** the higher the degree of heterogeneity is, the greater the attack surface is and the easier it is to find a vulnerability that can be exploited. For the purposes of information: high heterogeneity (external changes, BYOD, disparate services, etc.), average heterogeneity (progressive rationalisation, application convergence, etc.), low and controlled heterogeneity(standard applications, etc.).

**Note 20 :** the more the business services offered by the information system are numerous and specific, the greater the attack surface is and the easier it is to identify a vulnerability that can be exploited.

**Note 21 :** searching for technical information (address plans, passwords, etc.) or business information can be made very complicated for the attacker. Examples in increasing order of difficulty: data stored as clear text in a centralised zone and that can be identified easily (by the naming thereof, etc.), data stored in multiple locations, encrypted data (for the attacker, it will then be necessary to obtain the decryption key).

### STEERING, EXPLOITING THE ATTACK

*The elements to be considered can depend on the objective targeted by the attacker and on the method of attack used.*

- Type of channel that would have to be set up in order to steer or exploit an attack on the targeted supporting assets **(Note 22)**.
- Assumed time constraints for the exploitation of the attack **(Note 23)**.
- Existence of a security operating centre (SOC).
- Existence of an anti-DDOS system.
- Taking account of the TEMPEST threat, linked to the interception of compromising parasite signals, especially if the entity's premises are located in a densely-populated urban area.

**Note 22 :** examples of command & control channels: pre-existing channel already in place (backdoor), synchronous channel set up for the attack
**EXAMPLES :** **direct, reverse tcp/http, asynchronous channel (examples: email, social networks), physical channel (example: air gap via removable storage media).**

**Note 23 :** the exploitation time will depend on the target objective. It can be very short (a few minutes to a few hours), for example in the case of sabotage or a non-persistent denial of service attack, or relatively long (several months, even years) for a spying operation. On the other hand, certain time constraints can make the attacker's task more difficult. For the purposes of information, in increasing order of difficulty: no constraint, the attack can be launched at any time; the timing has to be precise, but the forewarning is substantial; the timing has to be precise and the attacker will have little forewarning; the attack has to be coordinated on several machines, without an Internet connection.

### MALICIOUS TOOLS

*Most of the attacks require the installation of malware in the targeted systems, sometimes in several steps. This section, which supplements the preceding sections, groups together the major elements that determine the success and the cost of a malicious project (method of attack, tool(s), etc.). It can assist you in refining the estimation of the likelihood of an elementary action that would require the installation of malware.*

- Type of technology of the supporting assets targeted by the malicious tool **(Note 24)**.
- Delay for applying security patches after the publication thereof. Implementation of ANSSI's recommendations concerning the maintaining in security conditions **(Note 25)**.
- Extent of the age of the technology of the targeted supporting assets.

**Note 24 :** it is rare that a piece of software is developed specifically to malicious purposes and used solely for the purposes of an attack.

However, according to the technology of the target supporting assets, the attacker may need to adapt or redevelop a piece of malware. In certain cases, if the target technology is very specific, they must even acquire the supporting asset.

**EXAMPLE**: **aeronautical calculator, industrial programmable logic controller**
The target type of technology therefore greatly influences the technical difficulty.

**Note 25 :** a support asset that is up to date in terms of security patches obliges the attacker to develop an exploit referred to as "0-Day", therefore unknown to the public. Otherwise, the attacker only has to exploit a public vulnerability (zero difficulty and likelihood of success is nearly certain). The longer the delay for applying a security patch for a known vulnerability is, the greater the window of opportunity is to obtain an exploit without difficulty.

# 9

# Structuring the risk treatment measures (Workshop 5)
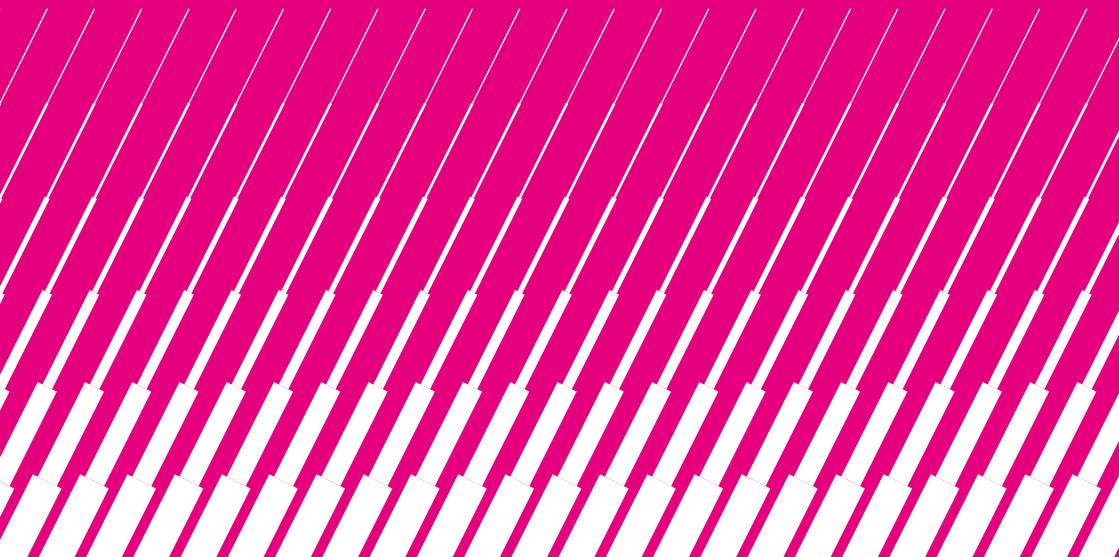
Risk treatment measures can be structured according to the in-depth security principles hereinafter:

■ governance and anticipation;

■ protection;

■ defence;

■ resilience.

**They can be organised as follows:**

| GOVERNANCE AND ANTICIPATION | **Governance**<br>♦Organisation of the management of the risk and continuous improvement;<br>♦Accreditation process;<br>♦Control of the ecosystem;<br>♦Management of the human factor (awareness, training);<br>♦Digital performance steering indicators.<br><br>**Knowledge of vulnerabilities:**<br>♦Security audits, watch.<br><br>**Knowledge of the threat:**<br>♦Watch (intelligence, economic intelligence). |
|---|---|
| PROTECTION | ♦Partitioning of supporting assets by trust domains.<br>♦Management of authentication and access control.<br>♦Administration/supervision management.<br>♦Management of data inputs / outputs and removable media.<br>♦Data protection (integrity, confidentiality, management of encryption keys).<br>♦Security of interconnection gateways and of "border" supporting assets.<br>♦Physical and organisational security<br>♦Maintaining in conditions of security and obsolescence management.<br>♦Security of the processes of development, procurement (supply chain) and of maintaining in operating condition.<br>♦Security with regards to compromising parasite signals. |
| DEFENCE | ♦Event monitoring.<br>♦Incident detection and classification.<br>♦Response to a cyber incident. |
| RESILIENCE | ♦Continuity of activity (back-up and restoring, management of degraded modes).<br>♦Resuming activity.<br>♦Management of a cyber crisis. |

# Terms and definitions

### 0-DAY

Exploit aiming for a vulnerability for which the patch has not yet been released by the publisher either because the latter is not aware of this vulnerability, or because the publisher is continuing the analysis.

◆

### ACCESS OR INTRUSION MODE OF ATTACK

Any method, technique or means that allow an attacker to get his foot in the door and compromise an information system, or to access the information that it contains.

◆

### AIR GAP

Security measure consisting in physically isolating a system from any IT network. The various ways of getting around this are transfers via removable media, setting up a hacked connection, etc.

◆

### BACKDOOR

Functionality unknown to the legitimate user that provides secret access to the system and that allows the attacker to take control of it.

◆

### BRUTE FORCE ATTACK

Method consisting in attempting to try all possible combinations in order to gain access to the resource.

## EXPLOIT

Program element that allows an malicious individual or piece of software to exploit a vulnerability in a piece of software, a firmware, a protocol, whether remotely or on the machine on which this exploit is executed. The objective can be to take over a computer or a network, to increase the privilege of a piece of software or of a user, etc.

◆

## EXPLOITATION MODE OF ATTACK

Any method, technique or means that allow the attacker to carry out his objective on the targeted system.

◆

## MALWARE

Program developed for the purpose of harming an IT system, without the consent of the user of whom the computer is infected. It can be classified into three categories: "exploits", required to obtain the rights on the machines that the attacker does not have before the attack, backdoors, which are used to add functionalities for the purpose of facilitating an exploit and rootkits, used to dissimulate the activity.

◆

## PHISHING

Phishing consists in extorting confidential information (access codes, banking coordinates, etc.) by subterfuge. By passing for a trusted person or third party (bank, Tax Administration, Internet service provider, etc.), the attacker attempts to glean information from their victims by having recourse to various methods: email bearing incongruous and indiscreet requests, downloading of booby-trapped attachments, following links that redirect to fraudulent sites, etc.

## RANSOMWARE

Contraction of the words "ransom" and "software", ransomware is by definition a malicious program of which the purpose is to obtain the payment of a ransom from the victim. To achieve this, the ransomware will prevent the user from accessing their data, for example by encrypting it, then provide the user with instructions on how to pay the ransom in exchange for restoring their data.

◆

## ROOTKIT

All of the techniques implemented by one or several pieces of malicious code to dissimulate the trail of their activity, on the systems or the network.

◆

## SERVICE PROVIDER

The qualification of a service provider certifies its compliance with the requirements of ANSSI. Mention can be made of:

- PASSI: Audit service provider for information system security (Prestataire d'audit de la sécurité des systèmes d'information)
- PDIS: Security incident detection service provider (Prestataire de détection des incidents de sécurité)
- PRIS: Security incident response service provider (Prestataire de Réponse aux Incidents de Sécurité)
- PSCE: Electronic certificate service provider (Prestataire de service de certification électronique)
- PSHE Electronic timestamp service provider (Prestataire de service d'horodatage électronique)
- SecNumCloud: Cloud IT service provider)

## SPEARFISHING

A variant of phishing to which is added social engineering techniques. Contrary to conventional phishing that is based on sending a generic message to a large number of recipients, spearfishing focuses on a limited number of users to whom are sent a highly personalised message.

# NOTES