The CREOGN Research Notes

French Gendarmerie Officers Academy Research Centre

Issue 62 – October 2021

Florence ESSELIN

EBIOS RISK MANAGER : ACCESSIBLE METHODOLOGY TO SECURE DIGITAL TRANSFORMATION

Under the combined effect of competitive market and public policies, organisations and people become more and more addicted to "digital" – technologies, systems and services enabling dematerialisation of goods and persons, to compute and broadcast huge volume of information in a borderless world: cyberspace.
Within cyberspace, worldwide and constant competition can suddenly worsen into confrontation: cyber criminality is rife.
This situation exposes everyone – all the more so every gendarme in his personal life or professional duty – to risks that must be understood for their own security.
Proceeding to risk analysis prior to implementing a digital transformation project, and frequent cyber threats assessment are not only recommendations: in many cases, this is a legal obligation.
This document shows a method developed and recommended by the French National Cybersecurity Agency (ANSSI): EBIOS Risk Manager[1]. Although this method is relatively new, its usage increases rapidly: it shares common features with the tactical reasoning method (MRT) taught to Army and Gendarmerie commissioned officers, which can ease adoption by gendarmes in their cyber threat prevention and cyber space protection mission.

I) Information security risk analysis: recommendation or legal obligation?

Reserving a book at the local library via your town's webpage, managing your bank account from a personal computer, declaring taxes on line, consulting a doctor remotely, booking and paying a car park from your cell phone, filling out an online complaint form, making an appointment with your local Gendarmerie station, etc., all these online services share a common obligation: early risk analysis dedicated to information security.
Three approaches are now mandatory for specific sectors or due to the nature of the data, and rely on risk analysis:

- Security approval: it aims at "ensuring that all risks have been identified, dealt with appropriately, and that the remaining risks are acceptable, on the basis of a global risk assessment which takes into account all components, including environmental and those indispensable for the proper working and security of the information system under consideration",". A formal approval validates this approach and engages the responsibility of the private individual known as approval authority. It is mandatory for classified[2] information systems, administrative[3] on line services, any State[4] information system, vital[5] information systems, as well as for the networks and information systems of essential services operators[6];

1 EBIOS Risk Manager : https://www.ssi.gouv.fr/en/guide/ebios-risk-manager-the-method/
2 Cf Instruction générale interministérielle n°1300.
3 Cf Le référentiel général de sécurité, pris en application du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives.
4 Cf la politique de sécurité des systèmes d'information de l'État, portée par la circulaire du Premier ministre n° 5725/SG du 17 juillet 2014.
5 Arrêté du 17 juin 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au secteur d'activités d'importance vitale « Gestion de l'eau » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du Code de la défense.
6 Cf. Art. 10 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique, transposant la directive européenne Network and Information System Security (NIS) du 6 juillet 2016.

- Impact assessment[7]: required by the regulation relating to data protection and European directive 2016/680 about “penal sphere[8]” data, it includes personal data risk assessment;

- Information system certification for health data hosts[9].

II) Risk is a combination of a threat and its ensuing losses

Risk has been a part of our lives since childhood: which kid has never tried to defy parental rules, running the risk of having to face some consequences, maybe punishment, in the unlikely hope that it will pay off ? ISO 31000 (risk management) and ISO/IEC 27000 (information security management) standards provide a general definition and add some clarifications. Risk can be defined as the combination of a threat and its ensuing losses, concealing potential positive consequences which usually inspire risk-taking. Defining more precisely a risk linked to information systems security (cyber risk) enables us to start thinking about how to deal with it, by working on its components. Thus, “cyber” risk can be defined as the fact that a source of risks[10] may take advantage of IT tools’ vulnerabilities (hardware, software, etc.) targeting an objective and impacting the “business values” (information and processes needing protection) of the target. A path of attack can be set up on the vulnerabilities intrinsic to the information system (IS) of the entity and on those introduced by its interconnection with the IS of multiple stakeholders (partner, host, etc.).

How can such a method be useful to fight cyber crime?
Just as the tactical reasoning method prompts officers to analyse the situation before designing a manoeuvre subject to the commander's decision, the EBIOS method (expression of needs and identification of security objectives) makes it possible to assess the risks that weigh on a digital project so as to be able to tackle them, that is to say to determine and validate the actions to be taken and the means to be implemented to strengthen its security and prepare to deal with the consequences of residual risks.
It is a tool for reflection, prevention and protection, which can be used both for preparing the security certification of an IT project and for the implementation of an internal cyber risk management process for the whole IS. It is also a communication tool between the stakeholders of digital transformation. Finally, mastering EBIOS Risk Manager can also be an asset in anticipating the evolution scenarios of the cyber component of a crisis, because this version of the EBIOS method makes it possible to quickly define risk scenarios at strategic and operational levels.

25 years of EBIOS evolution
The EBIOS method was created in 1995 within the central information systems security department of the general secretariat for national defence, whose heirs are respectively ANSSI and the general secretariat for defense and national security. This method has been adopted by the armies and the Gendarmerie as a security certification tool for classified and sensitive information systems. It has evolved taking into account both standardization in the field of cyber risk management (ISO 27005 standard) and feedback from ANSSI as well as the EBIOS club which gathers method experts, trainers and software editors for the EBIOS Risk Manager (RM) version.
The first versions of EBIOS aimed at identifying in an exhaustive manner the various components of a risk in order, on the one hand, to eliminate all unlikely combinations or combinations of negligible impacts and, on the other hand, to determine which elements to work on to reduce each risk.
With the EBIOS RM version presented in October 2018, ANSSI bet on a method more oriented towards the study of the annoyance capacities of the actors of the "ecosystem" - friends and enemies - and the identification of the most significant scenarios of attacks. EBIOS RM abandons the exhaustive and often laborious inventory of vulnerabilities specific to the IS that it aims to protect and unsophisticated current threats, considering that they can be compensated for by applying "computer hygiene" measures constituting the "security baseline".
This approach is supported by two phenomena :

- many organizations have generally established a foundation of security measures out of necessity, to comply with various laws and regulations; these measures must be taken into account in the new IS, without justifying them by a risk analysis ;

- correcting all the known breaches of an IS is a very difficult task and of limited effectiveness, because in addition to the vulnerabilities and their possible correctives published every day by the editors and the CSIRT (Computer Security Incident

7 Privacy Impact Assessment (PIA) https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf
8 EVANS, Mark. Les fichiers de sécurité : une exigence d’efficacité et une obligation de conformité [en ligne]. Revue de la gendarmerie nationale, décembre 2018, n° 263, p. 93-97. Available on : https://www.gendarmerie.interieur.gouv.fr/crgn/publications/revue-de-la-gendarmerie-nationale/revue-n-263 . French version.
9 Code de la santé publique, art. L.1111-8 modifié par la loi n° 2016-41 du 26 janvier 2016.
10 The source of a risk can be natural, animal, involuntary human or malicious with various profiles such as an opportunistic fraudster, an unfair competitor, a vindictive relative, a recidivist cyberdelinquent, a cybermercenary working for a back room, a group of cyberterrorists, etc.. EBIOS RM essentially studies malicious human risk sources.

Response Teams), new vulnerabilities that are not yet made public but may be known to cybercriminals (called "zero day" vulnerabilities) will arise. The priority should be to patch the vulnerabilities that can be exploited in credible attack scenarios that would have the most impact.

III) EBIOS Risk Manager method: a 5-step iterative approach

EBIOS RM aims for efficiency but not exhaustiveness; used with common sense and agility, depending on the objective of the study and its calendar constraints, it requires the involvement in its various "workshops" of a representative panel of parties concerned with the IS to be secured.
The method, illustrated by the study of the fictitious case of a biotechnology company manufacturing vaccines, is presented in detail in a guide and its supplement available on the ANSSI website (www.ssi.gouv.fr/ebios) .

Workshop 1 – Scope and Security Baseline
In the first workshop, EBIOS RM invites you to set out the framework of the study, its scope, the trades and entities concerned and any other useful contextual element. From this stage, it is important to state the “feared events”, i.e. situations or events that you want to avoid because of their potentially significant negative impact.
This workshop is also an opportunity to identify all the things that constitute the security baseline (for example the information systems security policy or the security rules imposed on the sector of activity in question).
The main questions to ask yourself are:

- what are the missions of the organization?
- what are the critical processes and information that need protection ("business values")?
- who are the stakeholders of the IS?
- which situations and damage do you want to avoid first and foremost?
- what are the various constraints (operational, legal, etc.)?
- what are the existing security measures ?

Workshop 2 – Risk Origins
EBIOS RM then invites you to identify the "sources of threats" and the "objectives targeted" by them. The sources considered in EBIOS RM are exclusively human and malicious. The postulate is that the other sources (animal, natural, involuntary human) generate risks already covered by the security baseline or carried by the stakeholders studied in workshop 3.
In this workshop, the knowledge that the gendarmes have of cybercrime is particularly valuable. The BEPA-Cyber[11] [12] scale developed by cyber reservists from the gendarmerie can also help to quickly diagnose the sources of threats and their capabilities.

Workshop 3 – Strategic Scenarios
EBIOS RM also strives to identify all the partners who interact with the IS to be protected but who are beyond the control of the organization responsible for the IS, in order to assess the level of threat they bring, to then counter them. This analysis has become a necessity with the evolution of cyber threats against large companies or the state; indeed, since they generally have implemented substantial security measures allowing only identified partners to enter their IS, the tactic of cybercriminals is often to attack the smaller and more accessible partners, to finally reach the targeted entities.
With the results of the previous workshops, it is then possible to draw up a list of likely attack scenarios, which could cause significant damage if they reached "business values".

Workshop 4 – Operational Scenarios
Next, you must refine each strategic scenario and turn them into operational scenarios, through your knowledge of the operating methods of cybercriminals. It allows you to anticipate the progress of an attacker in the IS according to their ability to exploit flaws of various kinds (technical, procedural, human). The vulnerabilities of the technical components of the IS under consideration (harware and software, etc.) give a likelihood to each of the operational scenarios.

Workshop 5 – Addressing risk
Thanks to this analysis, we are able to define measures capable of stopping, or at the very least delaying, an attacker’s progression and discouraging him.
You can also specifically record and monitor required "passing points" to detect abnormal behavior. The reasoning in this dematerialized space is very similar to that used for the protection of goods and people in the real world.

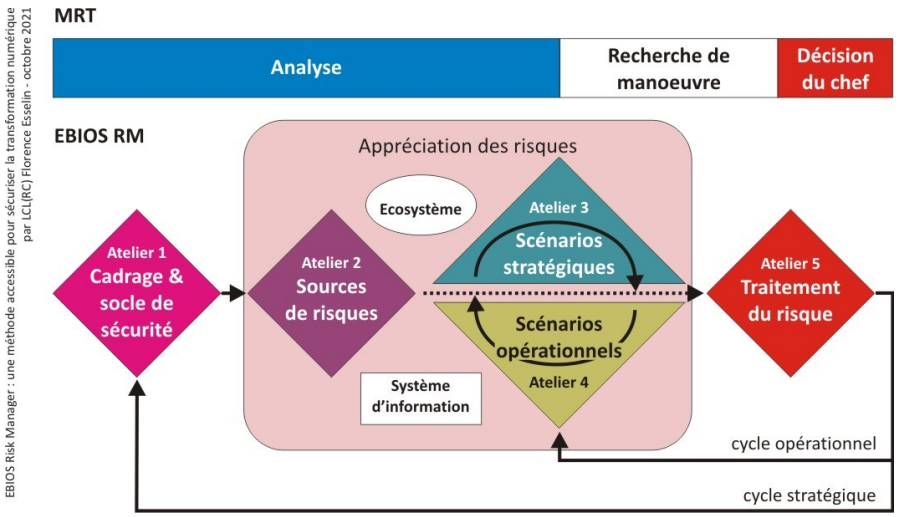
11 ESSELIN, Florence, AUTRET, Thierry. BEPA-CYBER, la base d’estimation des potentiels d’attaques cyber [en ligne]. Revue de la gendarmerie nationale, décembre 2013, n° 248, p. 112-125. Available on : https://www.gendarmerie.interieur.gouv.fr/notre-communication/publications-documentations/la-revue/revue-248 French version.

12 ESSELIN, Florence. De la résilience humaine à la résilience collective face aux cybercrises avec la BEPA-Cyber [en ligne]. Revue de la gendarmerie nationale, décembre 2019, n° 266, p. 65-74. Available on : https://www.gendarmerie.interieur.gouv.fr/crgn/publications/revue-de-la-gendarmerie-nationale/revue-n-266 French version.

Addressing identified risks is a matter of strategic decisions:

- accepting risk and its consequences ;
- reducing each risk by acting on one or more of its components to reduce its likelihood ;
- transfering part of the risk to a trusted third party ;
- abandonning all or part of a digital transformation project to avoid unacceptable risks that cannot be addressed otherwise.

IV) Similitude with Tactical Reasoning Methodology (MRT)



EBIOS RM and the MRT have many similarities. Indeed, workshop 1 is part of the analysis stage of the MRT, through the study of the general framework of the action and the definition of roles and missions. Workshops 2 and 3 (identifying critical stakeholders) contribute to the quantitative and qualitative assessments of enemies and friends (as identified through the MRT analysis).
The major effect sought is then defined by the knowledge of the security needs of the "business values", of the feared events and of the objectives targeted by the sources of risk.
As for the design of maneuvers, it is based on the strategic and operational scenarios determined in workshops 3 and 4.
Finally, when addressing a risk, the decision of the leader intervenes in workshop 5; it requires validation of the risk tackling strategy and informs the leader of residual risks, by suggesting a security improvement plan within a formal risk monitoring framework.

V) A Winning Method

The use of EBIOS RM extends in France within public and private entities thanks to the certification system supported by the EBIOS Club. The method is also promoted at European level; the evolution of the regulations regarding the protection of economic interests in the cyberspace of the European Union's member countries should develop risk analysis in the digital transformation.
If the EBIOS RM method is mainly used to prevent sophisticated cyberattacks, its scenario-based approach and the similarities it has with the MRT, used to structure operational action within a constrained time frame, make it possible to consider developing its use to anticipate actions in crisis situations.
There is little doubt that EBIOS Risk Manager will interest, not only IS security officers, but also officer cadets captivated by digital technology, unit commanders promoting innovation with an IT component, points of contact advising companies and communities, digital transformation project managers and even any gendarme keen to know what risks they and their family take in their current use of the Internet and social networks.

Florence ESSELIN *is an engineer, inspector at ANSSI, former expert adviser in digital and cybersecurity in the office of the Director General of the French gendarmerie (July 2018 - June 2021), lieutenant-colonel of the French citizen reserve of the national gendarmerie.*

Translated by Karl COULON, gendarme in the gendarmerie operational reserve