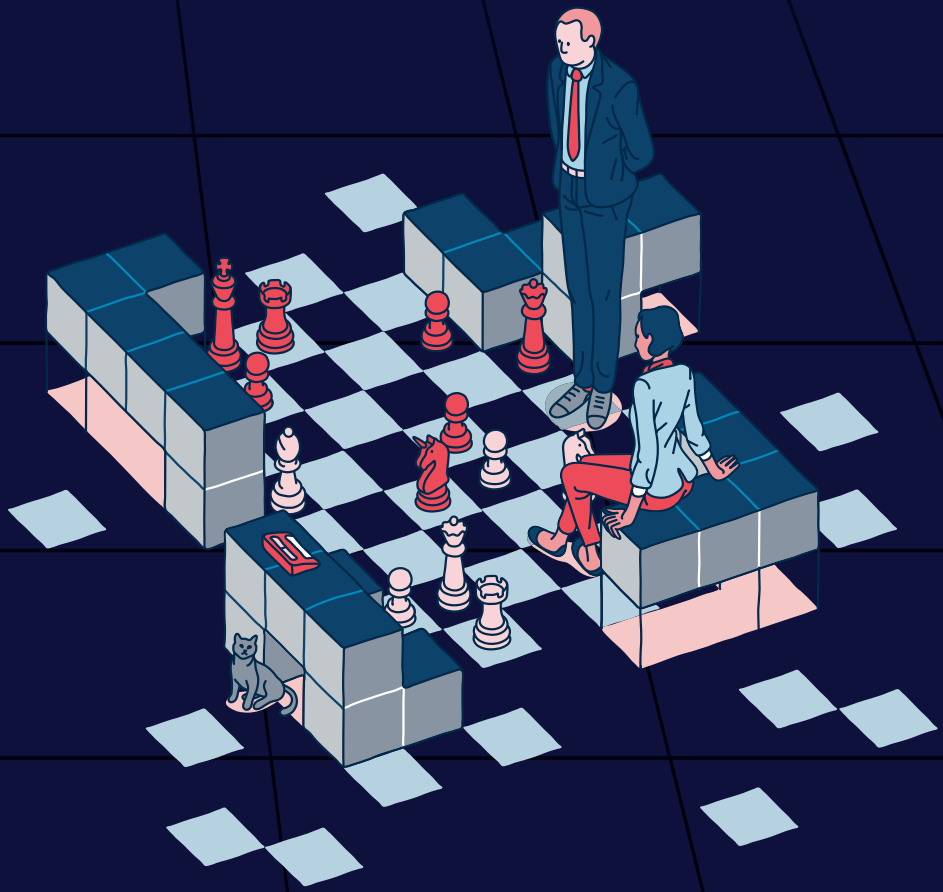
CONTROLLING THE DIGITAL RISK

THE TRUST ADVANTAGE



AMRAE

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION · ANSSI ·

CONTROLLING THE DIGITAL RISK

THE TRUST ADVANTAGE

CONTENTS

FOREWORD

Why did AMRAE and ANSSI decide to take up the pen together?

Brigitte Bouquot: We have been building a trusted relationship for several years now, and it is bearing fruit—our perspectives on risk are complementary: AMRAE focuses on economic objectives at the heart of corporate governance; ANSSI focuses deliver on technology at the heart of national security standards. And this is the key to deliver robust answers to the issues raised by the development of the digital economy in cyberspace. Only a joint and holistic approach enable us to make progress in mastering risk and setting standards for companies. This guide translates into deeds this shared will. It is often said that we have to transform ourselves in order not to disappear. That is particularly true in regard to digital risk! A company must take digital risks, but it must also deploy risk management strategies to master them. We need to address that without further delay. Tomorrow, the responsible and trusted company will be able to control this risk. Don't forget that it is above all a matter of competitiveness, not of constraint.

Guillaume Poupard: We have plenty of good reasons to work together! We share a common vision and our knowledge and experience are complementary. It allows us to mutually enrich each other. It is very helpful in matter of support and dialogue with our own beneficiaries. This is a reality: we speak different languages and we do not share the same experience with digital risk. This guide is the fruit of the sustained work carried out by our respective staff. To meet the expectations of leaders and risk managers, they were involved in the discussions to address the prospects of an investment in security.

Does digital risk still belong to the category of the "new threats" or has it become unavoidable?

Brigitte Bouquot: Digital risk has become truly unavoidable, but there is still some way to go before we master it! Leaders, informed by risk-managers, have taken full measure of digital risk and have gradually placed it at the center of overall risk management strategy. However, an entire ecosystem needs to be organized, industry by industry, to provide a complete answer to these challenges. I particularly have in mind insurance groups, whose offers are becoming clearer and larger. Risk transfer to insurance plays a significant role in a leader's commitment and in the resiliency of large or small companies. But if a compagny wants to be sustainable, it has to have a deeper knowledge of its digital risk.

Guillaume Poupard: Digital technologies have become daily partners at work and at home. They provide incredible opportunities as well as sophisticated and destructive threats. This encourages organisations to rethink themselves and to adopt a continuous improvement approach. Do I need to remind you that zero risk does not exist? Unfortunately, yes. Indeed, cyberattacks can jeopardize the survival of the organization or seriously compromise its image and its reliability. It is now impossible to ignore these issues and we do our best to guide each actor through this process, whatever their size, activity, maturity or resources.

Brigitte BOUQUOT, Chairperson of AMRAE
Guillaume POUPARD, Director General of ANSSI

INTRODUCTION

This guide owes its existence to the following observation: the digital risk that bears down increasingly every day on organisations can go as far as putting their very survival in peril and the one of their stakeholders. According to ANSSI (National Cybersecurity Agency of France) and AMRAE (French Association for Risk Management and Company Insurance), this must be considered as a risk to be treated at the highest level of the organisation, and no longer just as a risk of which the avoidance is the affair of technical experts.

This guide provides managers and risk managers with a progressive approach to build, Step by Step, a digital risk management policy within their organisation *(cf. Figure 1 – Progressive approach to build a digital risk management policy)*. In the event this policy already exists and needs to be consolidated or reoriented, the reader will find useful resources and advice in it.

The proposed approach makes it possible to:

- TAKING A READING OF THE DIGITAL RISK: this part allows the reader to position their organisation in its economic competition context while assessing the place that the digital risk holds in this equation. Today, the response that organisations give to the digital risk is among the most strategic issues. Like the other risks of this scale (business, legal, commercial, financial, etc.), digital risk management requires a holistic approach that involves many stakeholders within the organisation.

- UNDERSTANDING THE DIGITAL RISK AND GETTING ORGANISED (Steps 1 to 6): this part strives to describe the governance to be implemented in order to initiate the building of a digital security strategy. At each one of these Steps, managers and risk managers will have the concern of promoting the investments inherent to digital risk management.

- BUILDING YOUR SECURITY BASELINE (Steps 7 to 11): this part introduces the principles of protection, defence and resilience applied to the digital risk. Also addressed are the digital security processes and measures to be implemented in order to set down the previously-defined strategy.

- MANAGING ONE'S DIGITAL RISK AND ENHANCING ONE'S CYBERSECURITY (Steps 12 to 15): this part describes the continuous improvement mechanisms in terms of cyber risk management. This also includes the mechanisms for managing performance, essential for the organisation to remain competitive.

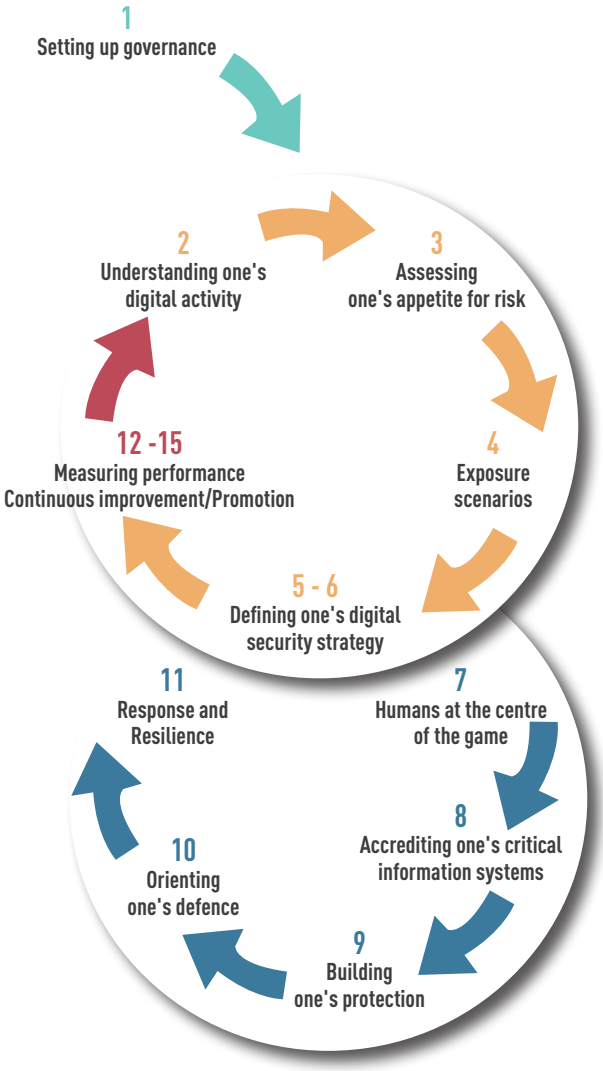


Figure 1 – Progressive approach to build a digital risk management policy

TAKING A READING

OF THE DIGITAL RISK

Digital risk management requires implementing a holistic approach that calls upon all the stakeholders in the organisation. AMRAE describes this approach using the concept of the "three lines of defence[1]".

To be effective, a digital risk management policy therefore requires being understood by and obtaining the support of all of the organisation's stakeholders, starting with its manager.

Economic globalisation and interconnection

The digital transformation is affecting all facets of society (companies, administrations, citizens, etc.) and has given rise to a new space for communicating and sharing information: cyberspace.

It has the characteristic of overcoming the traditional borders between States – whether they are territorial or political and upsets the notion of space-time.

A space for creating value but also for exchanging and confronting, cyberspace has become the theatre of social, technical, economic, operational and political interactions. In this new dimension, competition's rules are changing and attackers are Stepping up their ingenuity in order to achieve their goals. Whether involving isolated individuals or groups operating from a national territory or abroad, attackers are exploiting the new power relations stemming from globalisation, hypermediatisation and new digital uses.

Attacks stemming from these offensive strategies can take advantage of trusted relationships between stakeholders (for example, a company and its supplier) in order to unpredictably and swiftly affect organisations. In some cases, these attacks will be fatal for them.

[1] *Cf. Figure 2 – The three lines of defence, p13*

The digital risk, from a technical risk to a company risk

For many years, companies and public entities have implemented IT risk management only for the security of their information systems. This risk management was based on criteria such as confidentiality, integrity and availability, and was applied primarily to cross-organisational or support activities.

With the digital transformation of all of society's stakeholders and of their increasing interconnection, IT risk management has progressively moved within organisations towards a global management of digital risk. The latter, in light of the context described here in above, is bearing down more and more heavily on the activity of organisations.

A holistic view of risks

The changes in digital risk in the organisation now entail the criminal liability of the manager with respect to the management and processing thereof. This liability is accentuated by current regulations (GDPR[2], NIS[3], MPL[4], etc.).

With the increase of digital risk and its propensity to spread to all of the organisation's activities, managers must define with the boards and the business teams new risk acceptance thresholds (appetite for risk). These risks are not limited to the organization only, they also concern the stakeholders of the value chain with who they shall be shared.

The development and the transversality of this risk category now requires managers to reconsider their risk management model in such a way that the digital risk becomes part of the strategic, economic and legal concerns of organisations.

In order to acquire this holistic view of risks and ensure that they are clearly correlated with the organisation's objectives, whether public or private, a digital risk committee must be set up. Particular attention will be given to its ability to overcome the existing functional, business and operational silos.

[2] General Data Protection Regulation (GDPR)
[3] European directive Network and Information Security (NIS)
[4] French military planning law (MPL)

UNDERSTANDING

THE DIGITAL RISK AND GETTING ORGANISED

STEP 1. Defining a governance framework for the digital risk

A good risk governance entails setting up a committee that is devoted and adapted to the realities of the organisation.

Its role is to define the organisation's digital security strategy, to ensure its implementation, to manage the performance and to promote the investments made.

Defining a governance framework for the digital risk

Digital risk governance is part of a long-term approach and must be able to find its place in the normal operation of the organisation. It is managed by a digital security committee.[5]

The objective of the committee is to implement the digital security strategy by making use of up-to-date knowledge of the digital risks that bear down on the organisation's activities. It is chaired by the general management of the organisation and is comprised of at least one representative from each one of the three lines of defence as well as a member in charge of the development of the activities.

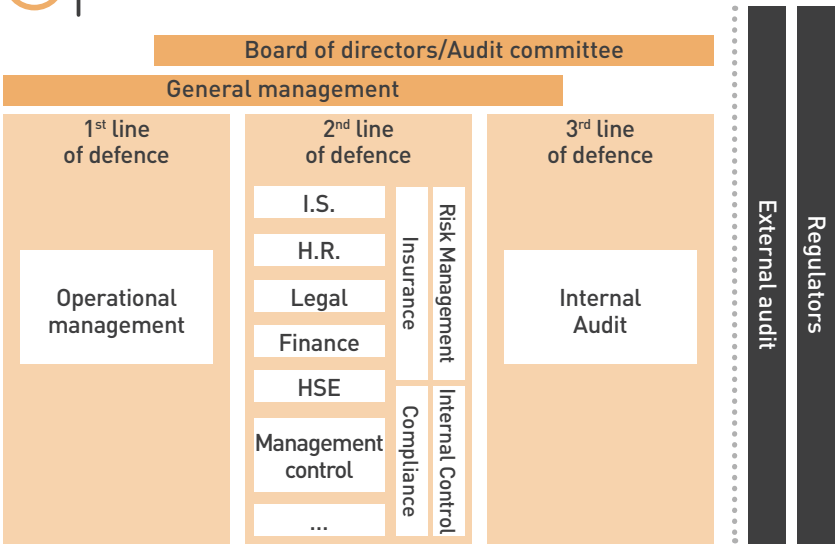
[5]The digital security committee is part of a global governance of the digital risk when the latter is planned by the organization.

The so-called concept of the "three lines of defence" has its roots in a partnership between the European Confederation of Institutes of Internal Auditing (ECIIA) and the Federation of European Risk Management Associations (FERMA).

The French Association for Risk Management and Company Insurance (AMRAE) and the French Institute of Internal Audit and Control (IFACI) offer a risk governance model based on "three lines of defence "[6].

1. The first line of defence groups together the operational functions and the business managers.
2. The second line of defence includes the risk specialists (including digital risks) able to assist the operational functions in identifying and evaluating main risks that concern their area of expertise.
3. The third line of defence ensures an independent audit function (internal or external according to the size of the organisation) that is linked to the organisation's highest level.

Model of the three lines of defence



Functions that participate in the global control system of risks

Figure 2 – The three lines of defence

[6]AMRAE and IFACI have adapted the concept in a work that meets the expectations of their targets: Three lines of defence for better performance: increasing the reliability of the strategy through organised risk management, AMRAE and IFACI, 2015.

The FERMA and ECIIA organisations have also published a recommendation guide of the internal organisation required for digital risk management: At the Junction of Governance and Cyber-security, FERMA and ECIIA, 2017, www.ferma.eu.

The missions of the digital risk committee are as follows:

1. Drafting and updating the Information Systems Security Policy (ISSP) that governs digital risk management.
2. Defining the organisation's digital security strategy and the investments required to implement it.
3. Giving priority to the security of the most critical digital services. These digital services or these information systems are the object of security accreditation[7].
4. Ensuring the management of the performance and continuous improvement in digital risk management.
5. Defining a strategy for promoting the investments made in the field of digital security.

[7] *Cf. Step 8 – Accrediting one's critical digital services*

STEP 2. Understanding one's digital activity

One's digital activity must be assessed and understood before any digital risk management approach.

An organisation's activity is based on processes and information that link it to its suppliers, its customers, its constituents, its partners, etc. These business assets[8], as ANSSI calls them, are themselves supported by services and information systems that need to be mapped very early.

Identifying one's business assets and critical supporting assets

Identifying the most critical business assets and supporting assets[9] is done starting with the organisation's missions that allow it to create value and then working progressively downward to the underlying digital services.

First, the objective is not to be exhaustive but to detect the main activities and digital services or information systems that are the most essential. This level of detail is enough to build one's worst risk scenarios[10] and to identify the digital services and the information systems that the committee will give special attention to through a Step of security accreditation[11].

For the least critical digital services, the security measures that apply systematically are based on an approach through conformity with standards and best practices and the building of a security baseline.

[8]Business asset: essential component in accomplishing the organisation's missions. This can be a service, a support function, a Step in a project and any related information or know-how. EBIOS Risk Manager, ANSSI, 2018, www.ssi.gouv.fr/ebios.
[9]Supporting asset: component of the information system on which one or several business assets are based. A supporting asset can be of a digital, physical or organisational nature. EBIOS Risk Manager, ANSSI, 2018, www.ssi.gouv.fr/ebios
[10]Cf. Step 4 – Building one's worst risk scenarios
[11]Cf. Step 8 – Accrediting one's critical digital services

Mapping one's ecosystem

Digital transformation plunges the organisation into a highly integrated ecosystem with its various stakeholders. This is referred to as the extended enterprise, including the organisation in a global production chain. The corollary is that the digital risk does not stop at the organisation's borders.

That is why it is essential to conduct mapping work of the organisation's ecosystem in order to get a view of its interactions and its flows. Likewise, because the ecosystem influences the organisation in its risk management, the manager has to include in the definition of the organisation's appetite for risk[12], its stakeholders, their threat levels and the principles of risk sharing.

Finally, as the stakeholders of the ecosystem develop along with the flow of economic opportunities, this mapping can be updated through an information watch activity[13].

In order to help the organisation to map its ecosystem and assess the digital threat that bears down on it, ANSSI proposes a simple and effective approach that can reveal the stakeholders that weaken the organisation the most (cf. workshop 3 of the EBIOS Risk Manager method).

Identifying the legal and regulatory framework that governs one's digital activities

The manager must know the legal and regulatory requirements that apply to their organisation and be able to appreciate their level of conformity in this respect. Although it is not always easy to identify the legal and regulatory framework that applies to one's organisation, initiating reflection according to the lines hereinbelow does however make it possible to draw up a rather complete situational analysis in order to identify the related obligations therefrom.

- The missions and activities of the organisation: security requirements included in the contracts concluded with its customers, suppliers or partners.
- The activity sector: particular protection requirements according to the organisation's activity sector (public, health, nuclear, transport, finance, etc.).

[12] *Cf. Step 3 – Defining the risk acceptance threshold*
[13] *Cf. Step 12 – Knowledge: from watch to analysis*

- The nature of the organisation: the State can for example grant the special statuses of Operator of Critical Infrastructure (OIC) or of Operator of Essential Services (OES) to the organisation.
- The nature of the information handled: requirements that apply to the handling of some sensitive information (for example, personal data).
- The national and international framework: national and international legal constraints that have for objective the protection of populations and the economy of nations.

In order to help it determine the legal and regulatory framework that applies to it and help it in its compliance approach, the organisation can have recourse to specialised external skills in terms of legal counsel.

STEP 3. Know your risk acceptance threshold

The appetite for risk is the level of risk that a manager accepts to take in order to support the activities and the development of their organisation. It supports the strategic decisions and orients operations.

How to know one's appetite for risk

The appetite for risk is strongly linked to the organisation's culture, its economic sector, its locations and its development strategy. It formalises the expectations of the managing bodies in terms of risk taking. The fruit of exchanges between the organisation's stakeholders (banks, insurance companies[14], partners, customers or suppliers[15], etc.), the appetite for risk defines the organisation's risk acceptance threshold.

To be effective, the appetite for risk must be reassessed on a regular basis using performance indicators[16] and in light of the developments[17] that exist in the environment (social, technical, economic, environmental and political).

A method for assistance in defining a risk appetite policy is proposed in the work "Management du risque : une approche stratégique", AFNOR edition, 2018.

[14] *Cf. Step 6 – Setting up suitable insurance policies*
[15] *Cf. Step 2 – Understanding one's digital activity*
[16] *Cf. Step 14 – Agility: continuous improvement and performance*
[17] *Cf. Step 12 – Knowledge: from watch to analysis*

STEP 4. Building one's worst risk scenario

Combined with an approach through conformity with best practices[18], identifying and financially quantifying the cyberattack scenarios that are the most critical for the organisation form the initial Step of the digital security strategy.

Adopting an approach through conformity for the most likely risks

Compliance with standards[19] and best practices in terms of information systems security makes it possible to anticipate the occurrence of the most likely cyberattacks. By thus becoming aware of the digital security measures that are essential for building the security baseline[20], the organisation becomes able to orient its risk analysis by focussing on the most critical scenarios for its activity.

Identifying the critical cyberattack scenarios[21]

The digital risk committee develops cyberattack scenarios that are likely to affect one or several activities that are vital for the organisation. These impacts can be digital, physical, financial, linked to the reputation or legal. The risk level is then defined according to the severity of these impacts and the likelihood of these scenarios. The likelihood of a scenario reflects the degree of feasibility or of the possibility that an attacker reaches their objective (cf. Figure 3).

[18] ANSSI's technical guides and basic best practices collections - https://www.ssi.gouv.fr/en/best-practices
[19] ISO/IEC 27000 family - Information security management systems, ISO - www.iso.org
[20] Cf. Steps 9, 10 and 11
[21] Workshops 2 and 3 of ANSSI's EBIOS Risk Manager risk analysis method can help in identifying the most critical digital risk scenarios. EBIOS Risk Manager, ANSSI, 2018 - www.ssi.gouv.fr/ebios

Regardless of the organisation's structure, the committee must base the development of its scenarios on the following questions.

- What are the feared events that can affect the organisation's business assets?
- Which attackers are able to infringe upon the organisation's activities and what are their target objectives?
- Are my information systems robust enough to withstand a targeted cyberattack?
- What are the other risks that can affect the organisation (negative image, non-compliance, sanitary, environmental, etc.)?

Developing cyberattack scenarios makes it possible to reveal the existence of information systems (internal or external) that, at first, were not identified as critical.

The critical digital services identified in Step 2 must be given special attention by the digital risk committee. This in particular results in implementing a Step of security accreditation[22].

Quantifying the impacts of critical cyberattack scenarios

Financially quantifying the impacts of the most critical cyberattack scenarios helps to make decisions as to the options for treating risks. In order to determine the cost of a successful cyberattack scenario, a financial analysis can be conducted, taking the following elements into account:

- the contractual commitments concluded with third parties or the non-compliance with applicable legal and regulatory constraints;
- operating and production losses;
- the loss or destruction of essential information;
- remediation of the information systems and resuming activity.

[22] *Cf. Step 8 – Accrediting one's critical digital services*

However, some costs are more difficult to estimate. This is in particular the case for those generated by a loss of trust or damage to the image. To estimate the cost of such impacts, setting up an information watch strategy[23] will allow the organisation to get information on cyberattacks targeting organisations of a similar size and with similar activities.

The precise description of a scenario's consequences can include different phases: crisis, remediation, improvement.

For each one of them, participants must specify which parties are impacted and at what level. This data will be interpreted in order to evaluate the hypothesis in financial amounts.

The credibility of financial estimations is capital in managers decision making regarding the digital security strategy.

[23] *Cf. Step 12 – Knowledge: from watch to analysis*

Activity	Feared event	Impact
Création / R&D	Copying of R&D data and manufacturing counterfeit products	**Financial impact** **Impact on the image and trust**
Manufacturing	Information leak on the manufacturing processes	**Legal impact** **Impact on the image and trust**
	Unavailability of the production chain	**Financial impact** **Impact on production goals**
Billing / Order	Theft of the customer/ supplier database	**Legal impact** **Competitive impact**
	Unavailability of the billing system	**Financial impact** **Impact on order goals**
	Leakage of commercial data	**Financial impact**
Delivery	Corruption of delivery slips	**Impact on the image and trust** **Impact on distribution goals**

Figure 3 – Example of the formalisation of digital risk scenarios

The risk manager has for mission to transcribe in an intelligible manner the various digital risk scenarios by describing their severity and their impacts, including financial impacts. This synthesis of scenarios that bears down on the activity of the organisation will be presented to the manager. This will orient the manager in making their decisions in terms of digital security strategy.

Estimated financial losses	Severity	Likelihood	Risk scenario
25% of the turnover	4 - Catastrophic	Likely	R1
25% of the turnover	3 - Major	Likely	R2
€80k/day	4 - Catastrophic	Very Likely	R3
4 % of the turnover	4 - Catastrophic	Likely	R4
€80k/day	3 - Major	Likely	R5
25% of the turnover	3 - Major	Very Likely	R6
€80k/day	4 - Catastrophic	Very Likely	R7

STEP 5. Defining one's digital security and promotion strategy

The manager must decide on the treatment of the digital risks identified according to their organisation's stakes and strategic objectives. Based on these choices, the digital risk committee draws up the digital security strategy and defines the priority objectives, the resources allocated and the Steps aimed at achieving the target level of cyber maturity.

Investing in digital security represents a cost but it is a response to the strong expectation of the organisation's customers and partners. It is therefore possible to turn this into a competitive advantage by adopting an approach of the *Cyber Business Partner* type: (cf. Step 15).

Analysing digital risks

The analysis phase of digital risks corresponds to the choices and decisions made by the manager concerning their organisation's stakes and objectives. These choices must be based on:

- the likelihood of the exploitation of attack paths and the impact of the worst scenarios on the organisation;
- the ability of the security measures in place to prevent the scenarios from occurring;
- the financial, human and technical resources available.

Taking account these criteria, the manager will be able to choose the risk treatment options to be selected such as implementing security measures, changing the business processes or transferring the risks through contracts to external third parties (subcontractors, insurances, etc.).

Digital security strategy

The risk treatment options are listed in the digital security strategy that will be managed by the digital risk committee. This strategy includes four lines:

- progressive implementation of the security baseline in order to have the latter converge with the Information System Security Policy (ISSP). Details on implementing the security baseline are provided in section "BUILDING YOUR SECURITY BASELINE".

- the implementing of a response to critical cyberattack scenarios. This response results in establishing of a Security Continuous Improvement Plan (SCIP) including a Step of accreditation[24].
- promoting digital security through communication so as to develop a competitive advantage[25].
- an effective risk transfer policy to the insurance market to supplement the risk management process. This policy must be elaborated in a global way but detailed by a specific team that includes the risk manager, the broker and the insurer (cf. Step 6).

Building a response to critical cyberattack scenarios

The response to critical cyberattack scenarios requires intervention from experts on information systems security. After having identified the attack paths that allow these critical scenarios to take place, they propose, for each one of them, mitigation measures. The latter aims to reduce the likelihood of the scenario and to increase the difficulty for the attacker to achieve their objective.

These measures can be based on technical solutions (digital or analogue), human (internal or external) or organisational (in particular through changing business processes). They will then be consolidated into an action plan, also called a Security Continuous Improvement Plan (SCIP) (cf. example Figure 4).

Security Continuous Improvement Plan (SCIP)

When the digital risk committee consolidates the mitigation measures in the SCIP, it has for objective to push forward the organisation in terms of digital security. Doing this, it is making a commitment on the digital security strategy in middle and long terms and must take into consideration the organisation's financial constraints, optimising of costs and the investments required for this increase in maturity.

During the building of the SCIP, the digital risk committee can for example indicate: the measures considered for each one of the critical cyberattack scenarios, the leader of the project, the required resources, an estimate of the cost for the implementation and the complexity thereof and the allotted time frame for implementation.

As with any management system, the committee has to reassess the worst scenarios in light of the progress with the SCIP. Through this review, it thus makes it possible to assess the effectiveness of the measures implemented and the return on investment for the latter.

[24] *Cf. Step 7 – Accrediting one's critical information systems*
[25] *Cf. Step 15 – Promotion: cybersecurity, a competitive advantage*

Security continuous improvement plan (PACS)

Security measures		Risk scenarios	Manager
Nature	Measure		
Human factor	Reinforced awareness of the methods of phishing	R4/R6	Security manager
Data protection	Reinforced protection of the creation, manufacturing and delivery data on the information system (solutions: encryption, partitioning)	R1/R2/ R4/R6	IT manager
Resilience	Business continuity plan with a partner/ subcontractor	R3/R5	Operational manager
Resilience	Cyber/civil liability insurance contract	R3/R5/R7	Financial manager

Figure 4 – Example of a Security Continuous Improvement Plan (SCIP)

Complexity	Estimated cost	Time frame	Priority
+	€5k	3 months	P2
++	€15k	3 months	P1
+++	€30k	1 month	P2
++	€5k/year	1 month	P1

Promoting one's investment in digital security

The security strategy on the one hand and the promotion strategy on the other hand can be conducted simultaneously and this, right from the start. Thus, to transform the investment effort into a competitive advantage, the digital risk committee can consider the security investments in light of their impact on the risks and on the promotion that can be made of them[26].

[26] *Cf. Step 15 – Promotion: cybersecurity, a competitive advantage*

STEP 6. Setting up suitable insurance policies

Among the measures that make it possible to improve the organisation's resilience, setting up a suitable cyber insurance policy is essential. Indeed, insurance can allow the organisation to take on the financial impact of a crisis and, in particular, the losses of income linked to a stoppage of the activity during the crisis.

Thanks to all the work already done to control one's digital risk, the organisation must have a clearer idea of its residual risk and of the potential impacts of a crisis not only on its activity, but also on its stakeholders.

Taking an inventory of the existing coverage

Before starting to look for specific insurance, the organisation must first analyse its insurance policies in the event one of them would cover digital incidents. Indeed, it is entirely possible for the digital risk to be partially covered in terms of damage or in terms of civil liability or product liability.

Today however, conventional coverage covers the digital risk only very partially. Although it is sometimes possible to interpret some clauses in favour of coverage for this type of risk, insurers are generally reluctant to cover them. Thus, the trend is increasingly an explicit exclusion of the digital risk from conventional insurance policies, moving towards more specific insurance policies.

Key pillars of a cyber insurance policy

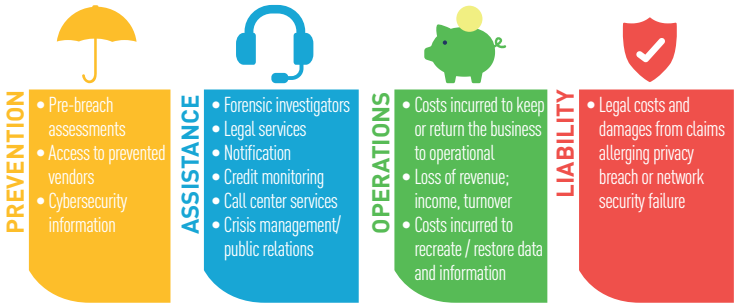


Figure 5 – The four pillars of a cyber insurance policy - © Ferma

Identifying the best coverage

Once its insurance assessment is complete, the organisation can begin the search for specific coverage. Contrary to conventional policies that separate the consequences for the organisation (damage insurance) from those on third parties (liability insurance), cyber insurance can offer coverage for direct and indirect risks. Generally, these various aspects are broken down into four pillars:

- prevention: the insurer will assist the organisation in setting up or in improving the management of its digital risk, by providing it with support in applying the approaches described in this document. Thus, the setting up of a policy can allow the organisation to improve its digital risk management thanks, in particular, to the diagnosis and recommendations issued by the insurer;
- assistance: in case of an event, the insurer will come into play to provide its expertise and thus make it possible to come out of the crisis faster. By helping to quickly restart the activity, they can make it possible to reduce the amount of the losses;
- coverage of operations: the insurer covers the financial losses directly incurred by the organisation: operating and revenue losses and expenses incurred to handle the crisis;
- liability coverage: the insurer will cover the cost of recourse and damages that may be incurred by third parties.

In light of its various intervention levers, cyber insurance is a complex tool that requires genuine expertise. It may be judicious to have recourse to the services of an insurance broker who is familiar with the stakes regarding digital security and the context in which the organisation in question operates.

As cyber insurance is a relatively recent product, there is still no real market standard.

Test the selected solution

Setting up cyber insurance is not just a box to be ticked. The subscribed policy must meet the organisation's needs and interests. A good way to ensure the relevance of one's choice is, before committing, to test the policies in light of the risk scenarios identified by the organisation.

The organisation can thus evaluate the relevance of its coverage and, possibly, activate certain variables (prices and amounts, scope of coverage, etc.).

Four recommendations to find the best cyber insurance

- Get advice from a broker who knows the cyber subject but also the sector in which the organisation operates. They will lend support in reflecting on the required level of insurance coverage.
- Carefully prepare the documentation to be given to the insurer to assess the risk.
- Compare the offers. There can be substantial differences between the offers proposed, especially if the coverage involves specifics concerning the activity of the organisation (aviation, maritime, construction, etc.).
- Take the time to conduct each Step correctly in order to have detailed knowledge of the stakes involved before turning to the insurance market. The objective is not to take out a policy in order to reassure oneself, but to commit to a contract that is genuinely adapted to the needs of the organisation.

In the document Preparing for Cyber Insurance, published in October 2018, the Federation of European Risk Management Associations (Ferma), Insurance Europe (representing insurers) and the European Federation of Insurance Intermediaries (BIPAR) provide a large amount of advice for dialoguing with the market, accurately checking the conditions of a possible cyber insurance contract and comparing the offers.

www.ferma.eu

BUILDING

YOUR SECURITY BASELINE

STEP 7. Humans at the centre of the game

Humans are the origin and at the core of the system.

Because they are at the centre of the game, humans are often a privileged target of attackers.

By fully including the human factor into the Information System Security Policy (ISSP), it is possible to obtain active participation in digital security for the organisation from employees, followed by significant and quick results at a reasonable cost.

Awareness raising and exercises

The human factor is one of the attackers' privileged action levers. It is therefore essential to include it in the organisation's digital security strategy. To achieve this, efforts to increase awareness can be made or realistic exercises[27] can be organised. The challenge is to develop a genuine culture for digital security in such a way that the members of the organisation, with the help of security procedures, are able to thwart the most common traps set by attackers.

The actions carried out at each level (awareness, exercises) have to be renewed at regular intervals in order to really be effective because teams transform, best practices evaporate and the threat never stops changing.

Acquiring and maintaining skills

For teams whose speciality concerns the security of information or IT systems, acquiring and maintaining skills at the state of the art is to be included in the annual training plan. This training can take the form of online programmes (MOOC[28]), training sessions or continuing education programmes[29].

[27]Crisis scenarios or role playing (serious game). Serious games for security and cybersecurity for the general public and professionals, CCI, www.cci.fr/web/presse/actualite-fiche/-/asset_publisher/9FDf/content/actu-:-serious-games-pr-pro (French only)

[28]Improve your knowledge and skills in terms of digital security with the ANSSI's SecNumAcadémie MOOC. www.secnumacademie.gouv.fr/ (French only)

[29]ANSSI has developed the SecNumedu-FC training label. It lists the establishments that offer continuing education programmes in the area of digital security. www.ssi.gouv.fr/particulier/formations/secnumedu-fc-labellisation-de-formations-continues-en-cybersecurite/formations-continues-labellisees-secnumedu/ (French only)

STEP 8. Accrediting one's critical digital services

This Step is prior to instilling trust in the organisation's digital services. Thanks to an iterative and sustainable approach, it provides risk control concerning the most critical digital services and participates in promoting the investments in digital security.

The Step of accreditation[30] is a commitment made by the top managers in terms of the most critical digital risks for which they are held accountable that bear down on their organisation. It guarantees that they are aware of the risks and that the latter are controlled by their teams.

This Step makes it possible to form a genuine security dossier for digital services and critical information systems. It also involves the teams and resources required for the unfolding thereof in the framework of an iterative approach. The latter aspect provides a periodic review of the security dossier and of the residual risks in the life cycle of information systems.

It is conducted by the business managers, assisted by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO) and includes going through an accreditation commission, chaired by the top manager. On this occasion, the digital risks, the responses to the worst scenarios and the strategy for treating risks are presented to them.

The Step towards accreditation can be initiated by the top manager in parallel with the building of the organisation's security baseline.

In some cases, the Step towards accreditation can be mandatory. In France, mention can be made for example of Interministerial General Instruction no. 1300[31], the General Security Baseline (RGS)[32], the State Information Systems Security Policy (SISSP)[33] and the Military planning law[34] (MPL).

[30] *Security accreditation in nine simple Steps, ANSSI, 2017, www.ssi.gouv.fr/guide-homologation-securite (French only)*
[31] *Interministerial General Instruction no. 1300, SGDSN, 2011, www.ssi.gouv.fr/igi1300 (French only)*
[32] *The General Security Baseline (RGS), ANSSI, 2014, www.ssi.gouv.fr/rgs (French only)*
[33] *The State Information Systems Security Policy (SISSP), ANSSI, 2014, www.ssi.gouv.fr/pssie (French only)*
[34] *The Military planning law 2014 to 2019, www.legifrance.gouv.fr*

STEP 9. Building one's protection

Protecting the organisation's business activities and its supporting assets entails setting up security measures. These measures are at the crossroads of organisational, digital and physical considerations.

They are selected based on an approach through conformity with respect to the various security reference standards (legal, regulatory, etc.) that apply to the organisation.

Legal elements of protection

An active contractual prevention policy must be deployed in order to avoid exposure to proceedings that are sometimes criminal, initiated by customers and partners, regardless of their nationality. The liability of the manager and the reputation of the organisation depend on it. As such, it is essential to observe a few legal points of attention:

- the legal and regulatory obligations that the organisation is subjected to;
- the contracts established with third parties and with subcontractors in particular (the applicable jurisdiction of the contractual elements, the professional civil liability, the security annexes);
- a "security assurance plan" supplied by[35] third parties.

The implementation of legal protection measures able to protect the organisation in a constantly changing environment requires special skills in terms of legal council.

Business project management

Any business change must take into account the digital security aspects and this, as early as possible. So as to avoid limiting the businesses by excessively restrictive measures with regards to security needs, it is recommended to integrate security in an agile manner[36] into the projects.

[35] The security annexes are security requirements that are imposed by contract on partners, subcontractors and suppliers.

Being attentive to the level of digital security of components right from the design stage of the IT architectures – security by design – makes it possible to limit application vulnerabilities.

Finally, conducting a technical or organisational security audit[37] by a third-party and independent company[38] is a good way to close out the project and the related security Step.

Controlling digital uses

The professional and personal use of IT resources (computers and mobile telephones, tablets, removable media, etc.), and travel and access to wireless networks inside and outside of the organisation, are all sources of threats for the organisation's information systems. These situations should be anticipated in order to reduce one's exposure to such threats.

The uses proper to each organisation must be controlled and listed in the organisation's ISSP. In addition, each use or resource has to be accompanied by a security operating procedure.

The same applies for handling and access to the organisation's most sensitive information. It is indispensable to control the distribution thereof and their exposure, in particular with regards to people or spaces that this data does not concern (for example, R&D data that can be accessed by a trainee or from a professional trade fair).

To assist managers in preventing the digital risks generated by the current uses in the organisation, ANSSI publishes best practices guides applied to certain audiences and/or situations[39].

[36]ANSSI makes available to organisations a methodological guide to support them in the secure development of projects and the management of the digital risk in agile mode. Agility & digital security, ANSSI, 2018 - www.ssi.gouv.fr/uploads/2018/11/guide-securite-numerique-agile-anssi-pa-v1.pdf
[37]Cf. Step 14 – Agility: continuous improvement and performance
[38]PASSI (cybersecurity audit service providers) are ANSSI-qualified service providers specialised in digital security audit activities - www.ssi.gouv.fr/passi (French only)
[39]Recommendations on digital mobility, ANSSI, 2018 - www.ssi.gouv.fr/nomadisme-numerique (French only)
Digital security – Good practices for the use of travelling professionals, ANSSI, 2019 www.ssi.gouv.fr/en/guide/the-travel-advice-booklet

Digital protective barriers

Protecting one's business activities and one's supporting assets is also implementing application, system and network protective measures. This arsenal of technical measures is aimed at limiting the conducting of malicious actions on digital components and business information so as to preserve their availability, their confidentiality and their integrity.

Adding digital protective measures can generate the opposite effect if they contain vulnerabilities. For attackers, they become additional entry points to the information systems. It is therefore important to carefully choose one's digital security products and services and to maintain a relationship of trust with the manufacturer or the publisher of the latter.

In some cases, organisations can be subjected to specific regulations in terms of digital protection. Operators of Critical Infrastructure (OIC)[40] and Operators of Essential Services[41] (OES) must thus refer to the regulatory texts that concern them in order to direct their choices in terms of solutions and services[42] for digital security.

Physical protective barriers

Controlling the digital risk also entails controlling one's physical environment and one's premises. Physical access control to the most critical information systems must be implemented and associated with a video protection system. To supplement the physical means of protection, it is highly recommended to provide means of alert, and even protection, against environmental incidents (fire, flood, overheating, etc.).

However, the aforementioned means of protection remain information systems as a whole. As such, they can be exposed to cyber-threats and must be taken into account in the risk scenarios.

Some organisations in the research sectors, defence or industry are subjected to specific regulations in terms of physical protection.

In France, the General secretariat for defence and national security should be contacted to get information on the regulations specific to the security of sectors of critical importance, to the protection of the Nation's scientific and technical potential or to the protection of national defence secrecy.

[40] Military planning law (MPL)
www.ssi.gouv.fr/entreprise/protection-des-oiv/protection-des-oiv-en-france (French only)
[41] European directive Network and Information Security (NIS)
www.ssi.gouv.fr/entreprise/reglementation/directive-nis (French only)
[42] Security certification and qualification delivered by ANSSI, ANSSI's security Visas, www.ssi.gouv.fr/en/security-visa

STEP 10. Orienting one's defence and anticipating the reaction thereof

Defending one's organisation and its business activities against cyber-threats is orienting one's defence according to the worst risk scenarios identified. Implementing suitable means of detection, logging and correlation will participate in detecting cyberattacks. While the processes for identifying and managing a cyberattack will make it possible to contain and control its impacts on the organisation's activities.

Detecting cyberattacks

Detecting cyberattacks consists first and foremost in directing one's detection methods towards the paths and methods used by the attackers[43]. Systems for detecting cyberattacks aimed at the supporting assets and business activities identified as the most critical must be implemented as decided by the CISOs and IT management. These systems can be placed on the office networks but also on the production networks as well as on the user stations, mobile devices and Internet access points.

Logging and correlation

In addition to detection devices, it is recommended to implement a logging system that records the events concerning access to the information systems and to sensitive data. These events and logs are then correlated and analysed to effectively contribute to detecting cyberattacks.

In France, according to the organisation's legal and regulatory framework, the latter may have the obligation to make use of ANSSI-qualified service providers specialised in the activities of detecting cyberattacks[44].

[43] *Cf. Step 6 – Humans at the centre of the game*
[44] *Security incident detection service providers - www.ssi.gouv.fr/pdis (French only)*

Qualifying and managing a cyberattack

Qualifying a cyberattack consists in identifying the activities and the supporting assets affected by the attack, and especially the severity of these impacts. This then entails reacting, treating and classifying the incidents. To do this, it should be answered the following questions:

- what to do when an incident is detected?
- who to alert?
- which first measures to apply?
- what is the impact of the cyberattack on the operation of my organisation?

An escalation procedure has to be defined to manage the incidents at the correct level of responsibility (businesses, internal IS services, CISO) and decide whether or not to trigger the crisis unit for the largest organisations or those subjected to specific obligations. Finally, the management of a cyberattack must integrate a post-incident analysis phase that makes it possible to improve the effectiveness of the security measures that were initially deployed.

The Government watch, alert and response centre against IT attacks, CERT-FR in France, produces and makes available a certain number of informative notes, news bulletins and alerts[45].

In France, in case of an act of or suspected cybercrime, the cybermalveillance.gouv.fr platform can lend support to companies:

- by putting them in contact with competent proximity service providers to identify the nature of the incident and get the systems back into operating condition;
- by redirecting them to other platforms (PHAROS, Perceval, signal spam, etc.);
- by making substantial contents and practical advices available to them.

[45] *Good reflexes in case one's information system is infiltrated, CERT-FR, 2002, www.cert.ssi.gouv.fr/information/CERTA-2002-INF-002 (French only)*

STEP 11. Showing resilience in the event of a cyberattack

An organisation's resilience after a cyberattack depends on its ability to maintain its activity despite the occurrence of a malicious action against it.

Activating the crisis unit

If the operation of the organisation is strongly affected by the cyberattack, the digital risk committee must be convened and the crisis unit has to be formed. The members of the unit define and launch the actions to be implemented in order to limit the impacts of the cyberattack in progress and prevent the propagation of the crisis and its edge effects (financial, legal, operational, professional or image). If the impact of the attack is close to the risk appetite thresholds , then the business continuity plan (BCP) has to be activated.

Crisis communication

Crisis communication is an integral part of the crisis management system. Being transversal, it pursues two objectives:

- reducing the direct impacts of the cyberattack (alerting stakeholders, instructions and operation coordination);
- and preserving the organisation's reputation (media, financial, legal, etc.).

To successfully carry out these two objectives, it is necessary to conduct anticipatory work, from an organisational standpoint (defining a crisis communication system, training communicators, etc.) as well as from an operational standpoint (identifying typical scenarios, defining dedicated communication plans, preparing turnkey response elements, etc.).

[46] *Cf. Step 3 – Defining the risk acceptance threshold*

Relations with the authorities

In case of a cyberattack, it is necessary to contact the police in order to inform them of the situation. You can solicit the territorial police services in the vicinity. In the event a complaint is filed, it is recommended that you obtain the assistance of a specialised lawyer in order to determine the criminal infractions that you or your organisation are a victim of.

According to the legal and regulatory framework in which the organisation operates (OCI, OES, etc.), the latter may have the obligation of informing its national security agency.
In France: www.ssi.gouv.fr/en-cas-dincident (French only)

The Business continuity plan (BCP)

The Business continuity plan (BCP) aims to guarantee the organisation's survival after a cyberattack. It organises the restarting of the activities as quickly as possible with a minimum loss of information, with or without the assistance of a service provider. To be relevant, a BCP is based on a study of the worst scenarios. It forms an essential chapter of the organisation's security policy and must be reviewed, tested and enhanced on a regular basis in order to remain effective.

To assist you in forming your BCP, you can make use of the following resources:

- ISO 22301: 2012 Business continuity management systems - www.iso.org
- Guide pour réaliser un plan de continuité d'activité, SGDSN, 2015 - www.sgdsn.gouv.fr/uploads/2016/10/guide-pca-sgdsn-110613-normal.pdf (French only)
- Plan de continuité d'activité à l'usage du chef d'entreprise en cas de crise majeure, DGE, 2015 - www.entreprises.gouv.fr/files/files/directions_services/politique-et-enjeux/entrepreneuriat/Guide-PCA-en-cas-de-crise-majeure.pdf (French only)

The Disaster recovery plan (DRP)

The objective of the Disaster recovery plan (DRP) is to rebuild the information systems and data in order to restart the applications and business processes as quickly as possible in case of a critical cyberattack. The DRP is formed from a set of technical, organisational and security procedures and can rely on partners and external service providers.

Just like the BCP, the DRP is based on a study of the worst scenarios. Integrated into the organisation's security policy, it must be reviewed, tested and enhanced on a regular basis in order to remain effective.

Relations with your insurer

During crisis management, activating the insurance policy taken out in Step 6 may be required. This can in particular allow the organisation to benefit from specific additional resources to assist with managing the crisis and returning to a normal situation as quickly as possible. According to the selected insurance coverage and the severity of the incident, the following resources can intervene:

- cyber experts, to manage the incident and conduct the investigations required in order to qualify and control it;
- system experts, to assist in rebuilding information and restoring data;
- legal advisers for protecting civil and criminal liabilities of the organisation and of its manager;
- crisis communication advisers in order to assist the manager in managing the crisis, limiting the impacts of it and preserving the organisation's image.

Cyber insurance can also lessen the financial impact, especially losses of revenue linked to the stoppage of the activity.

Finally, insurance can make it possible to handle the potential costs incurred to offset the damages caused to third parties because of the incident that occurred. Taking this aspect into account is essential in order to preserve the organisation's reputation and credibility with regard to its stakeholders.

MANAGING ONE'S

DIGITAL RISK AND PROMOTING ONE'S CYBERSECURITY

STEP 12. Knowledge: from watch to analysis

Faced with digital transformation, the organisation has no other choice than to be aware of the world in which it operates. It is vital for it to understand its environment and its momentum in order to anticipate the threats and the impacts thereof.

Targeting and structuring one's watch approach

As specified in Step 2, the digital risk committee has to include in the framework of the organisation's digital risk management the setting up of a continuous and iterative information watch approach. The watch strategy adopted has for purpose to keep the organisation's knowledge up to date in terms of its activities, its ecosystem (competition, e-reputation, legal aspects, technological capacity, digital development, etc.), the threat sources and attack methods.

Repositioning the organisation in its environment

Keeping the sector, business and transversal knowledge of the organisation up to date helps the digital risk committee when making decisions when faced with new threats, vulnerabilities or legal and regulatory constraints.

STEP 13. Commitment: from adhesion to action

Obtaining the commitment from one's employees and the organisation's stakeholders to the digital security strategy makes it possible to increase agility when faced with a threat.

Thus, the exploitation of the human factor as an attack vector is reduced, while the acuity of the employees faced with the traps that have been set by attackers is reinforced.

Federating one's employees and stakeholders

It is through implementing a real commitment plan, stemming from the digital security strategy, that the organisation's various stakeholders (internal and external) will feel fully involved in the process of managing the risk[47]. It will thus be possible to consider humans as a defensive factor rather than as an attack vector.

The commitment plan is based on three lines:

- Authority. The manager must communicate with their employees and stakeholders the contextual information (economic, political, etc.), the impacts of the digital risks on the organisation (financial losses, partial unemployment, etc.), the stakes of digital security (protection of data and of know-how, fraud and corruption, maintaining production, etc.), and the missions and objectives of every individual;
- The skills. Employees have to be drilled and trained, as such their skills will be maintained over time;
- The resources. The IT resources provided to the employees and stakeholders must allow them to fulfil their activities in compliance with the Information System Security Policy (ISSP) and digital security procedures.

[47] *Cf. Step 7 – Humans at the centre of the game*

Commitment as a performance indicator

Measuring employee and stakeholder commitment as actors in the defence of the organisation must be carried out on a regular basis through internal surveys and questionnaires.

This indicator in particular makes it possible to detect the weak signals of demotivation or of a lack of understanding of the stakes regarding digital security from the various stakeholders (internal and external) of the organisation.

STEP 14. Agility: continuous improvement and performance

By including its digital risk management strategy in an iterative approach of continuous improvement, the organisation adapts to new threats, reinforces its security baseline and controls its investments.

Audit and control strategy

Setting up of an effective audit and control strategy makes it possible to ensure the maintaining of the organisation's level of security. The audits and controls concern the compliance with organisational, digital or physical measures. They highlight "the points of vigilance" and the points of non-compliance with regards to standards and the implementation of the Security Continuous Improvement Plan.

The audit and control strategy must be reviewed on a regular basis in order to incorporate the changes in the organisation and its environment.

In France, according to the organisation's legal and regulatory framework, the latter may have the obligation to make use of ANSSI-qualified service providers specialised in the activities of auditing digital security. www.ssi.gouv.fr/passi

Constantly adapting to the threat

The Step of continuous improvement carried out by the digital risk committee must be based on:

- the information watch strategy;
- the tools for measuring performance (indicators and dashboard);
- the results of the control and audit actions.

By integrating the knowledge of new threats, the objectives of the digital security strategy and the correcting of audit non-conformities, the organisation is able to dynamically adapt its risk management strategy.

It thus becomes capable of changing its Security Continuous Improvement Plan (SCIP) in an agile manner and of anticipating the digital risk and its impacts: (cf. Figure 6).

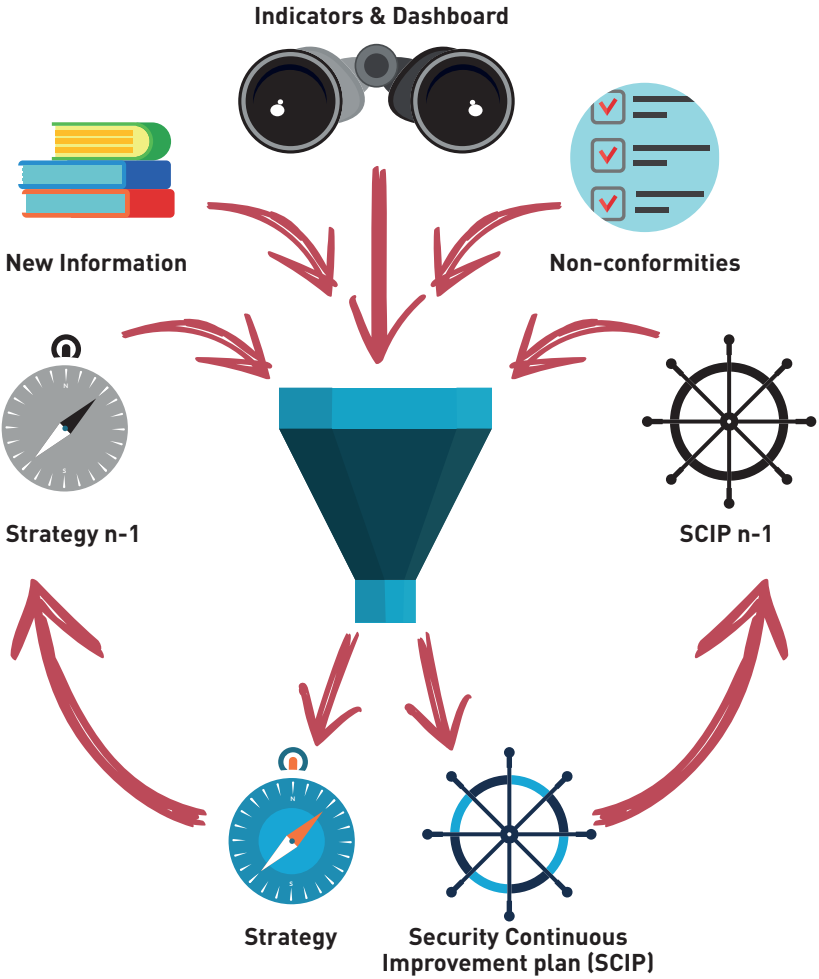


Figure 6 – Cycle of continuous improvement

Performance management

In order to enable the digital risk committee to correctly steer the management of the digital risk, the latter must be provided with measuring tools in the form of indicators (strategic, steering, operational, organisational or technical).

In order to be fully usable, this data can afterwards become part of dynamic dashboards in order to obtain a visual representation of the achievement of the objectives and thus bring out trends or deviations.

Examples of indicators		
Strategic	**Steering**	**Operational**
State of the governance of the digital risk	- Frequency of the digital risk committees - Frequency of the compliance audits - Frequency of the review of the risk treatment strategy - Number of ISSP exemptions - Frequency of the review of regulations - Frequency of the reassessment of the cyberattack scenarios	-
State of the digital risk	- Rate of coverage of the risks - Rate of critical stakeholders - Rate of analysis of the risks on new projects - Rate of critical IS covered by an accreditation - Number of open non-conformities - Rate of progress of the SCIP - Frequency of the BCP tests	- Number of losses or thefts of equipment and terminals - Percentage of systems identified as vulnerable - Update rate for anti-virus and patches on stations and servers - Number of operational components (hardware and application) that are obsolete or not maintained
State of the management of security incidents	- Number of controlled security incidents - Number of non-controlled security incidents - Activity interruption time	- Number of cyberattacks detected - Rate of availability of the critical business applications - Percentage of security incidents according to the environments (email, intranet, extranet, etc.)

Examples of indicators		
Strategic	**Steering**	**Operational**
State of the security documentation	- Frequency of the review of the security policy - Frequency of the review of the business security processes	- Number of new security procedures drafted
State of the awareness, training and drilling actions	- Rate of awareness - Rate of competency of the teams - Number of crisis exercises conducted	- Awareness certificates - Training certificates for administrators

Figure 7 – Example of indicators

STEP 15. Promotion: cybersecurity, a competitive advantage

Assessing the return on investment of the efforts devoted to digital security remains difficult, as well as quantifying the benefits thereof.

By promoting these investments and by adopting a Cyber Business Partner approach, the organisation can develop its competitive advantage, tackle new markets, generate growth and change its image positively and strategically.

Developing Cyber Business Partner approach

A structured management of the digital risk based on a sustainable approach[48] induces human and financial investments, of which it is difficult to assess the profitability.

On the contrary, the stakeholders that are affected by digital transformation expect that the organisation goes beyond the simple management of the digital risk and that it positions itself truly as a third party of digital trust.

By adopting a Cyber Business Partner approach with the stakeholders in its ecosystem (customers, partners, suppliers and investors), the organisation provides the guarantee of a cyber maturity that is compatible with the risk acceptance threshold of its stakeholders.

Promotes the investments of its digital security strategy in order to transform them into competitive advantages. The organisation provides its entire ecosystem with values other than the cost, such as trust, proactiveness or investment optimisation[49].

[48] *Cf. Step 8 – Accrediting one's critical digital services*
[49] *Cf. Step 5 – Defining one's digital security and promotion strategy*

The organisation can then make use of this promotion as a token of trust for:

- generating growth and seizing development opportunities with its investors and partners;
- rationalising and optimising its cyber insurance policy with its insurer;
- accessing new markets (especially sensitive ones) by positioning itself as a trusted operator that controls the entire production and supply chain.

Finally, by associating this approach with a communication strategy, the organisation will influence the level of cyber maturity of its ecosystem and will make its brand image change in a positive way.

Today, this aspect is starting to be taken into account by some organisations such as scoring agencies. Some organisations have seen the quality assessment of their credit sanctioned due to a cyber event.

Organisations have to be able to anticipate as of now the future expectations of customers, regulators and investors in terms of their ability to handle the digital risk and to provide them with guarantees.

Bibliography

Step 1

FERMA and ECIIA, *At the Junction of Governance and Cyber-security,* FERMA and ECIIA, 2017, www.ferma.eu

IFACI et AMRAE, *Trois lignes de maîtrise pour une meilleure performance,* 2015, www.amrae.fr (French only)

Step 2

ANSSI, *EBIOS Risk Manager*, 2018, https://www.ssi.gouv.fr/ebios/

Step 3

SUTRA G., *Management du risque : une approche stratégique*, Afnor éditions, 2018 (French only)

Step 4

ANSSI, *Technical and good practices guides*, www.ssi.gouv.fr/en/publications

International Organization for Standardization, *Famille ISO/IEC 27000 - Information security management systems,* ISO, www.iso.org

Step 6

FERMA, BIPAR and Insurance Europe *Preparing for Cyber Insurance*, 2018, www.ferma.eu

Step 8

ANSSI, *L'homologation de sécurité en neuf étapes simples*, 2017, http://www.ssi.gouv.fr/guide-homologation-securite (French only)

SGDSN, *Instruction générale interministérielle n° 1300*, 2011, www.ssi.gouv.fr/igi1300 (French only)

ANSSI, *Le Référentiel général de sécurité (RGS*), 2014, www.ssi.gouv.fr/rgs (French only)

ANSSI, *La Politique de sécurité des systèmes d'information de l'État, (PSSIE)*, 2014, http://www.ssi.gouv.fr/pssie (French only)

Step 9

ANSSI, *Agilité & sécurité numérique – Méthode et outils à l'usage des équipes projet,* 2018, https://www.ssi.gouv.fr/administration/guide/agilite-et-securite-numeriques-methode-et-outils-a-lusage-des-equipes-projet (French only)

ANSSI, *Recommandations sur le nomadisme numérique*, 2018, www.ssi.gouv.fr/nomadisme-numerique (French only)

ANSSI, *Digital security - Best practices for business travelers*, 2019 - www.ssi.gouv.fr/en/guide/the-travel-advice-booklet

Step 10

CERT-FR, *Les bons réflexes en cas d'intrusion de son système d'information :* CERTA-2002-INF-002, 2002, www.cert.ssi.gouv.fr (French only)

Step 11

International Organization for Standardization, *ISO 22301: 2012 Business continuity management systems,* 2012, www.iso.org

SGDSN, *Guide pour réaliser un plan de continuité d'activité*, 2015 - www.sgdsn.gouv.fr (French only)

DGE, *Plan de continuité d'activité à l'usage du chef d'entreprise en cas de crise majeure*, 2015, www.entreprises.gouv.fr (French only)

Additional helpful resources

AMRAE et CESIN, *Cyber risques - Outil d'aide à l'analyse et au traitement assurantiel*, 2015, www.amrae.fr (French only)

Institut Français de l'audit et du contrôle internes, *Cyber-risques : Enjeux, approches et gouvernance*, 2018, https://docs.ifaci.com (French only)

Fédération Française de l'Assurance, *Anticiper et minimiser l'impact d'un cyber risque sur votre entreprise*, 2017, www.ffa-assurance.fr (French only)

ANSSI, *Mapping the information system,* 2018, www.ssi.gouv.fr/guide/mapping-the-information-system

AMRAE, *La Cartographie: un outil de gestion des risques*, Collection Maîtrise des Risques, 2010, www.amrae.fr (French only)

AMRAE, *La Communication sur les Risques,* Collection Maîtrise des risques, 2016, www.amrae.fr (French only)

AMRAE, PME et ETI ; *La gestion des risques est aussi pour vous !*, Collection Maîtrise des risques, 2018, www.amrae.fr (French only)

IFIE, *Le Risk Manager & l'Intelligence Economique*, Collection Maîtrise des risques, 2010, www.amrae.fr (French only)

AMRAE, *Les Plans de Continuité d'Activité,* Collection Maîtrise des risques, 2015, www.amrae.fr (French only)

CLUSIF et AMRAE, *Risk Manager et Responsable sécurité du système d'information : deux métiers s'unissent pour la gestion des risques liés au Systèmes d'Information,* Collection Maîtrise des risques, 2008, www.amrae.fr (French only)

AMRAE, *Trajectoire vers un Enterprise Risk Management*, Collection Maîtrise des risques, 2012, www.amrae.fr (French only)

IRT System X, *La maîtrise du risque cyber sur l'ensemble de la chaîne de sa valeur et son transfert vers l'assurance*, www.irt-systemx.fr (French only)

DARSA J.-D. et DUFOUR N., *Le coût du risque - Un enjeu majeur pour l'entreprise,* GERESO édition, 2018, 2e édition (French only)

Revue de la Gendarmerie nationale, *Sécurité et vie privée by design,* décembre 2018 (French only)

Lcl TORRISI C., *kit de sensibilisation des atteintes à la sécurité économique, édité par l'INHESJ et la DGGN,* 2019, https://inhesj.fr https://www.gendarmerie.interieur.gouv.fr (French only)

Association pour le Management des Risques et des Assurances de l'Entreprise
AMRAE • 80 boulevard Haussmann 75008 Paris
www.amrae.fr • amrae@amrae.fr

Agence nationale de la sécurité des systèmes d'information
ANSSI • 51, boulevard de la Tour-Maubourg • 75 700 PARIS 07 SP
www.ssi.gouv.fr • communication@ssi.gouv.fr

The approach described in this guide has been developed by ANSSI and AMRAE. It builds on the experience of the principal actors involved in digital risk control.
In 15 steps, this reference work supports public or private organisations of all sizes through a process that drains strategic, economic and reputation issues.
Tomorrow, the responsible and trusted organisation will be able to control the digital risk. That said, leaders have to understand it, implement the appropriate actions and learn to value this investment.

www.amrae.fr
www.ssi.gouv.fr

ISBN: 979-10-97351-02-1