Confidence, the clincher:
Controlling digital risks
so as to build up cyberresilience

Fabien Caparros,
Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

Abstract:
Thanks to confidence, which is laden with virtues for public and private organizations, leaders are able to devote adequate resources to performing their duties or creating value, and to calmly manage contingencies. Over the years, the risks stemming from digital technology have become strategic and systemic. Given this trend, how to trust an organization's digital operations? Understanding and controlling these risks can help bolster trust, but this requires a high level of organizational maturity. When this level is attained, the organization will not be immune to cyberattacks, but it will be ready to cope. Faced with cybermenaces, risk management can then enable the organization to build up confidence at three levels: confidence in its organization, in partners and in its ecosystem. This is hard to achieve, but it will be the clincher…

Confidence when active in cyberspace

Let us start by clarifying a few terms. For organizations, a strategic risk can be defined in terms of three characteristics: the risk cannot be eluded; it has a potentially mortal effect; and it cannot be fully transferred to others. Given that such risks are systemic, cybersecurity is as important for the organization as for its ecosystem.[1]

Given that cyberrisks are both strategic and systemic, their management is a responsibility for the organization's directors, a responsibility that can be neither delegated nor outsourced. To clearly understand cyberrisks in 2020, let us borrow an analogy from R. Knake and R. Clarke (2019).

● During the first decade of this new century, in a still "young" cyberspace, most threats came from computer viruses or worms; the risks were technical. The probability of an organization being infected was growing but remained bearable. As a consequence, this DECADE OF PROTECTION invented technical solutions, such as firewalls and antivirus software.

● During the 2010s, the importance of cyberspace grew, and new threats appeared that were capable of circumventing these protections and attacking strategic targets, such as an infrastructure. Given these "advanced persistent threats" (APT), the risks for organizations essential to a nation were evolving, and new capacities were needed to detect, and cope with, them — capacities with a slue of acronyms: security operation centers (SOC), security information and event management (SIEM), computer emergency response teams (CERT), etc. The 2010s was a DECADE OF DEFENSE.

[1] This article has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references. All websites were consulted in June 2021.

● In 2020, with the growth of both cyberspace and cybercriminality, as organizations have been forced to become part of deeply interconnected and interdependent (digital) ecosystems, all organizations are concerned, regardless of their size or sector of activity. Cyberrisks have become both strategic and systemic. No organization seems capable of wending its way through this decade without having been the victim, directly or indirectly, of at least one serious cyberattack. The 2020s will, therefore, be the DECADE OF RESILIENCE.

To cope with these new risks, managers will need risk analyses devoted to strategic decision-making, that will help to adapt governance and acquire new skills. To manage digital risks, decision-makers must be informed to help find the right match between the exposure to danger, operational costs and the hoped-for benefits. When this risk management was very technical, decision-making was delegated to experts who managed this complexity at their level. Since risks have become strategic however, this responsibility has fallen back on decision-makers themselves. The latter must improve their skills without, however, becoming engineers in cybersecurity. Whereas risk analysis used to enable engineers to see to an adequate level of system security, it must, nowadays, be a tool of assistance to those who make strategic decisions. Furthermore, the implementation of risk-reduction measures is no longer just a matter for end users. It now involves all resources in an organization, the three lines of defense well known to risk managers.[2] Within organizations, risk governance and expertise are, therefore, evolving to assist the multisectoral technical functions in charge of information technology, the operational functions at the core of various business processes, and managerial functions.

Given this, the National Cybersecurity Agency of France (Agence Nationale de la Sécurité des Systèmes d'Information, henceforth ANSSI) has, with its partners, started overhauling its doctrine of digital risk management. During the first phase, the motor has been redesigned. EBIOS, the method used to analyze cyberrisks, was developed at the turn of the century, like other methods in risk management. It regularly underwent improvements but was still beyond the reach of persons who were not experts. A new version, EBIOS Risk Manager, designed jointly with EBIOS Club (a nonprofit association of EBIOS users), has been designed for assisting strategic decision-making (ANSSI 2018). This new tool enables decision-makers and cyberprofessionals to have a shared view of the risks. In collaboration with AMRAE (an association for managing risks and insurance in firms, a benchmark for corporate risk managers), a handbook has been released that proposes a gradual approach for setting up a governance of cyberrisks within an organization (ANSSI & AMRAE 2019). Other publications have described drills in managing cybercrises (ANSSI & CCA 2020) and presented the jobs that are emerging in cybersecurity.

Confidence in having one's own means for managing risks is no longer sufficient during an age of cloud computing, digital services and attacks against information systems via the supply chain. It is just as important to have confidence in one's partners in cyberspace.

[2] AMRAE and IFACI, two French associations, have made the orientation of risk management around three lines of defense the benchmark in this field since 2013.

Confidence in partners in cyberspace

The question here is not about having confidence in the sincerity of partners but, instead, about how to know, reinforce and supervise the solidity of relations with partners while assessing the risks stemming from relations with them in cyberspace. I conducted my first risk analysis with EBIOS Risk Manager in 2018, a year before the method was released, in a medium-sized firm that ran an information platform for managing the logistics of a major French port. All public and private stakeholders at the port were interconnected. In response to questions about how much confidence could be placed in other stakeholders (against the backdrop of the attack against the port of Antwerp in 2011),[3] some shippers jokingly referred to their partners as “truants”. The vector of infection during the NotPetya attack in 2017 was a software program required by the Ukrainian administration.[4] During both these attack situations however, there was no question of severing relations via the Internet with private or public partners. So, It is time to assess risks, adopt suitable measures and manage residual risks. This is now the landscape of risk management.

It is not easy, however, for an organization to evaluate its digital ecosystem. Despite the launching of EBIOS Risk Manager two years ago, we still notice that organizations do not have a mature risk management. Let us take the example of an airport where, naturally, a terrorist attack was the top-ranking risk. When examining the airport’s relations with its partners, we soon noticed that its sales very much depended on parking. However outside firms (partners like Q-Park or Vinci, among others) ran the parking lots and garages. Were this service not available, business losses would soon climb. So, how much did the airport depend on digital relations with this partner? Would the partner cover eventual losses of earnings or the negative impact of a tarnished image? How interconnected were this partner’s services with the airport’s information system? Could an attack (like NotPetya) on these services penetrate this system? How mature was this partner’s cybersecurity? Was it worthy of the airport’s confidence? Using these questions, EBIOS Risk Manager evaluated, for each partner, the critical nature of the relationship so as to adjust the efforts for making this relationship “cybersecure”. It also proposed a “radar map” of the risks so that a strategy could be drafted for a global management of the airport’s partners. This visual representation helps both to orient security efforts there where they are needed and to widely diffuse security procedures throughout the whole organization. These questions might seem obvious, but as it turns out, organizations are seldom capable of answering them. The grounds for placing confidence are *a priori* flimsy. They take no account of the risks run. This partly explains the anxiety of decision-makers when faced with cyberrisks (Figure 1).

[3] The port of Antwerp fell victim to a very sophisticated attack in June 2011, when a “mafia” managed to take over the information system for managing containers in order to illegally import drugs.

[4] This especially destructive attack in 2017 paralyzed (for days or even weeks) the activities of several firms, including multinationals, doing business in Ukraine. American authorities estimated the damage from NotPetya at more than $10 billion.

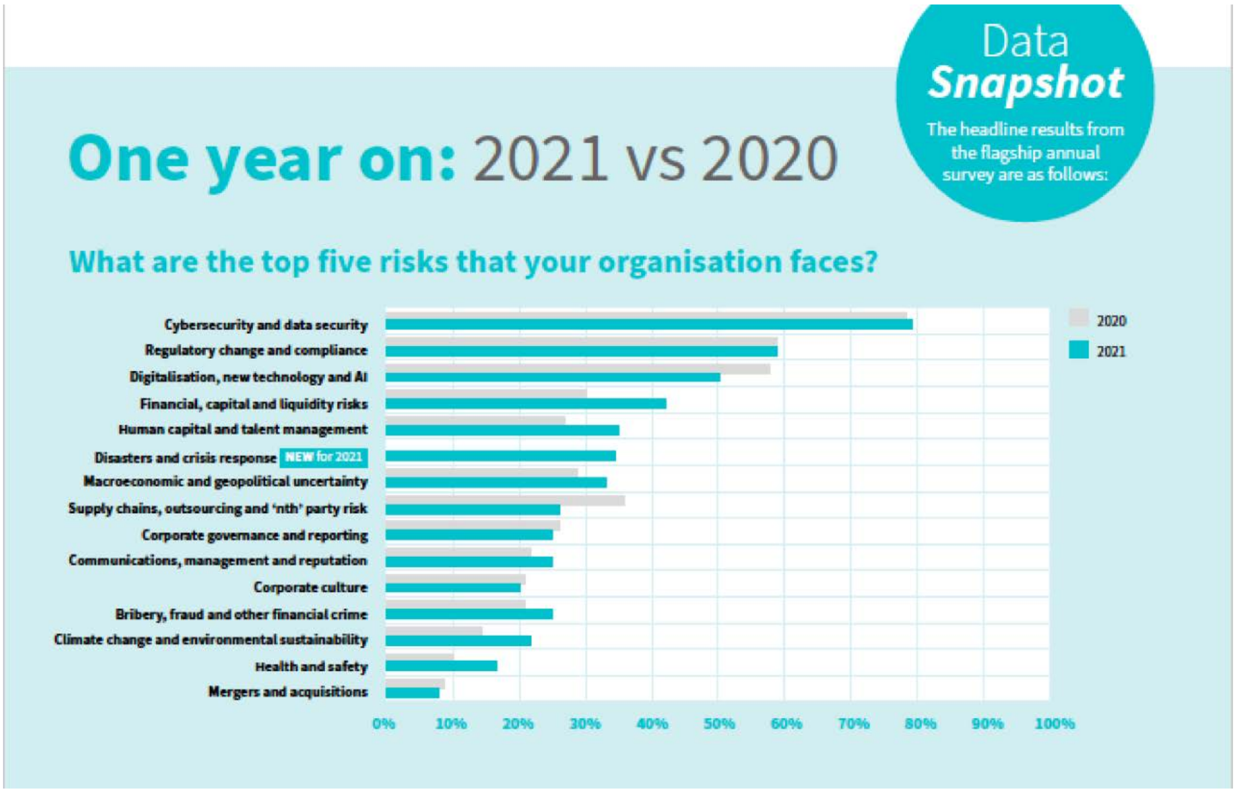

Figure 1:
Source: IFACI & ECCIA (2020)

In addition, organizations often poorly control how the responsibilities and costs stemming from cybersecurity are to be shared. It is worthwhile raising this issue with partners. For sure, security is now considered to be a cost. By simplifying somewhat, we can say that the head of information system security will tend to want to control as much as possible his own system's security and will, therefore, try to internalize operations so as have a system capable of interacting with an external environment in which confidence is initially lacking. On the other hand, clients will want to pass security efforts onto their partners and will even play the competition to thus transfer the largest share possible. While waiting for an eventual "zero trust network architecture", the solution will lie in between these two options.[5]

The question also crops up about responsibility in case of an attack. We need but read the clauses that restrict the liability of cloud providers to be convinced that the importance of this question is far from naught. Another problem is insurance coverage; and here too, the age of placing confidence without any control is over. Since regulatory authorities have forced insurance companies to review their so-called "silent coverage", the market has become tougher, as these companies have started paying close attention to their exposure to systemic risks.

[5] Underlying this architecture is the hypothesis that an organization's information system, even when well controlled, can be breached or might harbor a threat internally. The zero trust security model recommends taking under consideration the whole chain of connections with users, segmenting resources and establishing controls. It means no longer making the access to resources depend on whether or not an entity is present within the information system's bounds.

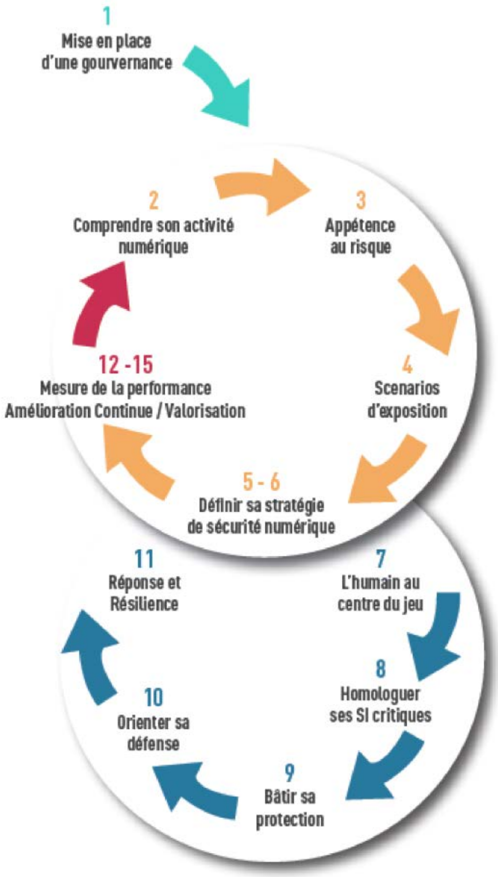

Figure 2: Gradual approach to building a cyberrisk management policy
Source: ANSSI & AMRAE (2019, p. 8)

Besides the questions of confidence on line and in relations with partners in cyberspace, another question has to do with the confidence that an organization can place in its environment. How to structurally set up virtuous mechanisms for reinforcing the digital resilience of an organization's ecosystem?

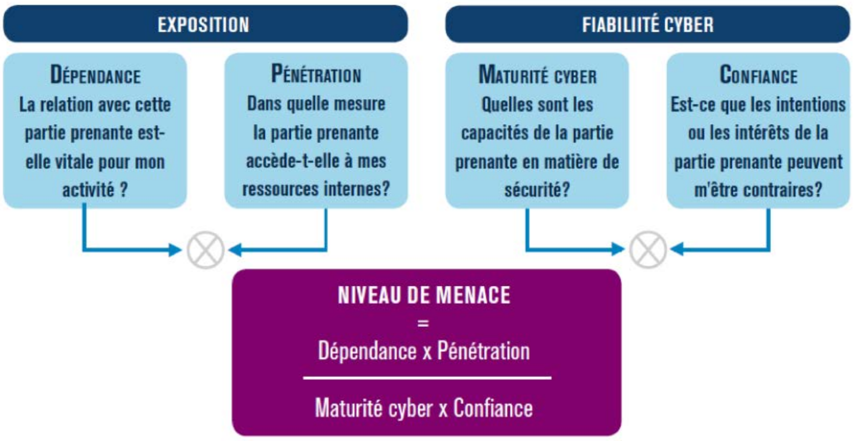
EXPOSITION
FIABILIITÉ CYBER
DÉPENDANCE
La relation avec cette partie prenante est-elle vitale pour mon activité ?
PÉNÉTRATION
Dans quelle mesure la partie prenante accède-t-elle à mes ressources internes?
MATURITÉ CYBER
Quelles sont les capacités de la partie prenante en matière de sécurité?
CONFIANCE
Est-ce que les intentions ou les intérêts de la partie prenante peuvent m'être contraires?
NIVEAU DE MENACE
=
Dépendance x Pénétration
Maturité cyber x Confiance

Figure 3: Assessing the risk stemming from relations with partners in cyberspace (EBIOS Risk Manager method)

Confidence in the digital environment

While digital ecosystems are being increasingly interconnected, embedded in each other and made interdependent, risk management can be used to improve the transparency of the supply chain so as to build up confidence. The current pandemic has shed new light on the question of confidence between buyers and sellers on the same value chain, and exposed the current model's inadequacy. When companies were to be chosen for supplying video conferencing services, a debate flared up about digital security. The current system for certifying security turned out to lack transparency. During the first months of the health crisis, Zoom's offer of video conferencing was sharply criticized for security reasons. The idea of making offers more transparent is now under study at the OECD. Through a pertinent risk analysis procedure adopted by both buyers and sellers, it would be possible for buyers to define the security measures necessary for them and for sellers to make competitive bids. As a complement to security certifications, this improved transparency of offers could serve to build up confidence in the digital ecosystem.

The stakeholders, in particular the customers of firms and users of public administrations, present in the same digital ecosystem are already demanding warranties of confidence. Rather than see these demands as a cost, private firms or public services could make offers that turn security into a source of value. This might seem obvious, but actually doing so is difficult. It is not evident how to bring security chiefs and the persons in charge of business processes to work together. ANSSI and AMRAE (2019) have thus proposed a "mixed governance" for bringing these persons into cyberrisk management committees. Strategies can then be devised for coupling digital security with the value of security efforts. A euro spent on security would become a euro that adds value to the offer made to the customer's or user's demand for a relationship of confidence.

Insurance is the driving force in a digital ecosystem's resilience. Insurance companies are not yet able to fill this role. To be efficient, an insurance system has to have a fairly stable state-of-the-art technology and be able to act to reduce both individual and systemic risks. Security measures for risk reduction are what EBIOS Risk Manager has called "baseline" security, which is probably the maturest field at present. These security measures must incorporate a system of inspection and evaluation. Stakeholders should be able to place confidence in this system, which might be sectoral or multisectoral (like the certification of merchant ships). Then comes the issue of knowledge about threats: knowing the current methods of action and the targets, and anticipating trends. This knowledge has to be statistical in order to build aggregate models for predicting the financial impact. Another question arises about the systemic nature of the risks. Means should be adapted so as to provide coverage (*e.g.*, reinsurance or state aid similar to what is provided to the victims of natural catastrophes). In all these fields, the state of the art has not yet been stabilized, but insurance companies are innovating and making progress under the attentive gaze of their regulatory authorities.

Conclusion

For public or private organizations, digital risk management provides a means for working on the issue of confidence in relation to their activities in cyberspace. Given the complexity of these risks (their strategic and systemic aspects), this risk management entails building confidence in organizations, their capabilities and relations with partners. It also requires constructing virtuous mechanisms for resilience that will bring confidence into the core of the digital ecosystem.

We might, rightly so, not share Clarke and Knake's excessive optimism, their pronouncement of the inevitable victory of security against cyberattacks. We do, however, agree with them that 2020 will be the decade of cyberresilience.

References

ANSSI (2018) *EBIOS Risk Manager — The Method* (Paris: Agence Nationale de la Sécurité des Systèmes d'Information) 96p., available via https://www.ssi.gouv.fr/uploads/2019/11/anssi-guide-ebios_risk_manager-en-v1.0.pdf.

ANSSI (2020) *Panorama des métiers de la cybersécurité, édition 2020* (Paris: ANSSI) 74p., available via https://www.ssi.gouv.fr/uploads/2015/07/anssi-panorama_metiers_cybersecurite-2020.pdf.

ANSSI & AMRAE (2019) *Controlling the Digital Risk: The Trust Advantage* (Paris: ANSSI/AMRAE) 60p., available via https://www.ssi.gouv.fr/uploads/2019/11/anssi_amrae-guide-controlling_digital_risk-trust_advantage.pdf.

ANSSI & CCA (2020) *Organiser un exercice de gestion de crise cyber* (Paris: ANSSI) 128p., available via https://www.ssi.gouv.fr/uploads/2020/10/anssi-guide-organiser-un-exercice-de-gestion-de-crise-cyber-v1.0.pdf.

CLARKE R. & KNAKE R. (2019) *The Fifth Domain: Defending Our Country, Our Children and Ourselves in the Age of Cyber Threats* (New York: Penguin Press).

IFACI & ECIIA (2020) "Risk in focus 2021: Practical guidance on climate change and environmental sustainability — How to tackle associated risks and harness opportunities?" (Paris: Institut Français des Auditeurs et Contrôleurs Internes) 8p., available via https://www.ifaci.com/wp-content/uploads/RISK-IN-FOCUS-CLIMATE_CHANGE.pdf.