FOCUS ON...

Délégation aux ENTREPRISES

SÉNAT

...CORPORATE CYBERSECURITY.

PREVENTION AND CURE: WHAT REMEDIES EXIST TO COMBAT COMPUTER VIRUSES?

1. A KEY ISSUE FOR BUSINESS SURVIVAL

Cybercrime targeting businesses is becoming commonplace for four reasons:

1. **The digitisation of the economy, accelerated by the lockdowns and the associated boom in remote working and fibre optics network rollout**;
2. **The professionalisation of cybercrime**, facilitated by **its "platformisation", its industrialisation, and the growth of cryptocurrencies**;
3. **The difficulty of prevention and crackdown**, which requires both awareness from everyone and effective international cooperation;
4. **The integration of cyberspace as a new theatre of geopolitical conflict**, where companies are either targets or collateral victims.

However, the digital economy, and especially e-commerce, can only grow if there is **trust between the company, its partners and its consumers**.
Companies of all sizes are being **encouraged to digitalise** their production processes, increase their use of e-commerce and allow their employees to work from home. The smallest companies think they are **safe** from cyberattacks. **This is an illusion, and sometimes fatal**: a company can fold after a cyberattack. Indirect costs sometimes emerge after a long latency period.

Every single user of a digital device or connected object is a **potential point of entry for an attack** which, if successful, could be fatal for their company, whatever its size. **Small and medium-sized enterprises** (**SMEs) and very small enterprises (VSEs), however, are more vulnerable to this scourge**. **The explosion in digital practices has been matched by an exponential increase in cyberattacks**. The following figures clearly illustrate this situation:

$6 trillion	***per year from 2021, against $3 trillion in 2015, all sectors combined: the cost of cybercrime worldwide***
3rd	***largest economy in the world if cyber risk was a country***
43%	***of SMEs experienced a cybersecurity incident in 2020***
16%	***of cyberattacks will threaten a company's survival by 2020***
155%	***increase in traffic on the cybermalveillance.gouv.fr website in 2020***
X 4	***ransomware attacks between 2020 and 2021 according to ANSSI***

The Chairman of the US Federal Reserve, Jerome Powell, believes that cyberattacks targeting companies are **the greatest current risk to the US economy, even more so than a financial crisis similar to that of 2008**. In response to this internationalisation of cybercrime, the President of the French Republic presented a **"Paris Appeal" for cyberspace security** at the Internet Governance Forum on 12 November 2020.

2. SLOW AND INADEQUATE REALISATION OF THE EXTENT OF CYBER THREATS

In 2018, cybersecurity was far from being considered as "everyone's business", as the French International Chamber of Commerce stated it should be. Too many companies, especially SMEs and VSEs, did not feel it applied to them. Cybersecurity seemed to be technical, could be outsourced, and was easily solved by purchasing a firewall!

However, there was a tipping point in the spring of 2020. Exposure to the risk of cyberattacks increased significantly when 8 million employees were suddenly working from home. At first, many companies encouraged their employees to use their own IT equipment. But this led to security breaches, as business continuity was more critical than digital security. Cybercriminals seized the opportunity, with **phishing attacks increasing by 667% between 1 and 23 March 2020**.

Business leaders have now started to take this risk into account, albeit to varying extents.

In response to the rise in security breaches, their IT departments are now trying to enforce the **Zero Trust concept**, a security model based on the principle that no user on a network is completely trustworthy.

Large corporations are beginning to recognise this need, especially as **rating agencies now include cyber risk in their financial ratings** and a market for cyber ratings has emerged. **ESG (environment, society, governance) ratings** now also mention **cybersecurity**. It is an **essential aspect of corporate governance** but also of **corporate social responsibility** when it comes to protecting against data theft. France Stratégie's *Plateforme RSE* (CSR Platform) even advocates the introduction of "corporate digital responsibility" (CDR).

Companies' cybersecurity capabilities must be **stepped up quickly and significantly before the boom in the Internet of Things** (IoT), which will dramatically increase exposure to cyber risk, **quantum computing**, which will expand the scope for intrusion, and **Artificial Intelligence**.

3. A GOVERNMENT-BACKED CYBER PROTECTION AGENCY WITH A FOCUS ON CRITICAL INFRASTRUCTURE COMPANIES

Companies classified as **critical infrastructure operators** are sufficiently protected at European and national levels by the French National Cybersecurity Agency (ANSSI). However, mid-sized companies, SMEs and VSEs that are **not** classified as being of **critical importance are not adequately protected** by this public system.

Public cybersecurity involves a **balance between the centralised nature of technical expertise and the need to be close to potential victims** to allow them to file a report at a local police station.

It provides a **unique way of allocating responsibilities, not according to the location of the offence (territorial criterion), but according to the type of ransomware involved (functional criterion)**. The size of the company is irrelevant when it comes to the legal treatment of the cyberattack.

This government scheme includes the **ability to deploy response teams on the ground to reassure a company director**, who usually has no idea of the digital skills that the French police services possess.

Corporate cybersecurity **relies on the smooth functioning of a four-pronged approach to cooperation** and sharing information for preventing, punishing and recovering from cyberattacks:

- between the judicial authorities and cybersecurity forces;
- between the national police and the gendarmerie, each of which has its own tools;
- between the public and private sectors;
- between France and its European and other international partners.

However, **the justice system remains helpless as cybercrime has become increasingly industrialised**.

4. CYBERSECURITY DIFFICULT TO ACHIEVE FOR SMEs

Large companies better protected, SMEs more vulnerable

Cybercriminals conduct market research on their targets. Once these targets have achieved a higher level of protection, the criminals redirect their sophisticated attacks to their original target's suppliers or subcontractors who are more vulnerable in terms of cybersecurity. In response to the proliferation of cyberattacks, **large corporations and mid-sized companies have taken defensive measures to make it more difficult for cybercriminals to attack them**. For example, developing effective strategies for backing up and restoring computer systems makes blocking access to those systems less attractive as a response to an unpaid ransom demand. **The downside of improved cyber defence at large corporations has been the shift of cybercrime to smaller, more vulnerable companies.** However, this transfer of risk to suppliers, subcontractors or customers continues to weaken large corporations' cybersecurity efforts through a feedback loop. This is because remote access to a company's information system increases its attack surface by opening new doors.

The "domino effect" can be catastrophic. Cybersecurity is therefore everyone's business, from one end of the value chain to the other.

Employees are often the weak link in cybersecurity, or even the Trojan horse.

Cybersecurity is still too often viewed as **an added burden** by employees themselves. The way in which management **operates in silos** in many companies does not always encourage teamwork. A minimum level of collaboration does not foster a shared culture in an effective way. A shared culture requires all levels of the company's hierarchy to be involved, including directors and the entire management team, as they have a major role to play in providing impetus.

The fight against cyber threats requires everyone to practice **digital hygiene** and take **protective measures at all times**. Simply increasing the budget allocated to tools is not the answer to the growing number of increasingly sophisticated threats. **Each employee holds the key to the company's cybersecurity.**

There is a worldwide shortage of people with expertise in cybersecurity. SMEs and VSEs are particularly affected by this situation as they are finding it difficult to afford trained staff. In addition to the shortage of cybersecurity skills, companies **rarely fully appreciate the value of securing information**.

Growing use of the cloud in an unbalanced business relationship

SMEs are in an uncomfortable position when it comes to **accessing cloud services**. They do not have a technical grasp of the issues and have to accept **an unbalanced commercial relationship**. Some providers even assume no responsibility for the availability or functionality of the service.

Despite the principle of free movement of data, reflected in Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018, and the guidelines of 29 May 2019, the **cloud market self-regulation process stalled** in November 2019 failing agreement on the drafting of codes of conduct.

There is a **systemic asymmetry between large global cloud service providers and their users**. For SMEs, accessing cloud services is sometimes like signing a membership agreement that contains unfair terms and conditions.

5. A WAKE-UP CALL OR CHAOS: THE PRESSING NEED TO STRENGTHEN THE FRENCH CYBERSECURITY ECOSYSTEM

An ambitious goal to be a leader in cybersecurity

As well as being a threat to companies, cybersecurity is an **opportunity to develop a buoyant market**. In France, cybersecurity generates **turnover of €13 billion**. It is a fast-growing sector, delivers €6.1 billion in added value, and employs 67,000 people. The global cybersecurity market is expected to be worth **$150 billion by 2023**.

France's cybersecurity industry is still **extremely fragmented** and **highly exposed to global competition**. Despite this, our country is home to some of the world's leading players. It has a number of key assets to maintain its **technological and economic lead**, especially in these three areas: **artificial intelligence** and machine learning, **cryptography** and **post-quantum technology**.

In the past, cybersecurity has been associated with constraints and spending, but today it must be seen as a competitive advantage and a profitable investment. Cybersecure behaviour is becoming a selection criterion for customers who are concerned about entrusting their personal or even sensitive data to a company.

The **government's strategy** is designed to encourage the development of a cybersecurity **ecosystem**. **Cybersecurity and the security of the Internet of Things** (IoT) is one of the five priorities of the "security industries" strategic contract of 29 January 2020, along with security at major events (including the Paris 2024 Olympic Games), digital identity, trusted territories and trusted digital experiences. The aim is to *"position French industry as a **world leader** in cybersecurity and IoT security"*. **It is an ambitious goal.**

A public policy of purchasing French cybersecurity solutions is the best way to develop the excellence of the French cybersecurity industry. Unfortunately, this is not happening. Buying unfamiliar foreign solutions is likely to threaten France's sovereignty. A culture that promotes buying French cybersecurity products is needed.

A **cybercampus** is due to be set up in the autumn of 2021 in La Défense, the main business district in Paris. Its aim is to **bring together the cybersecurity community**. This "cybersecurity flagship hub" is designed to attract the main public- and private-sector stakeholders in France and encourage them to develop **synergies**. It is crucial that it reflects France's determination to tackle the exponential rise in cyberattacks that threaten all organisations, both private and public. **If we fail to take action, we risk chaos in the short term!**

Regaining digital sovereignty in the cloud is nigh on impossible

The cloud market is expected to soar from €63 billion in 2021 to €560 billion in 2030. Controlling corporate data is a sovereignty issue. It will be difficult for France to **regain its sovereignty in the cloud**, now dominated by **three American players with a 70% market share**. However, the cloud is the **cornerstone of business development, including for SMEs**, just as it is for public entities, which are facing the same threats.

The desire to regain data sovereignty has been raised regularly in France since 2010. After the **failure of Andromeda**, the French government joined the German **Gaia-X** initiative in May 2020 and abandoned the idea of creating a new company from scratch, supported by public authorities and large corporations. The objective is now to create a European infrastructure based around a governance and coordination body responsible for issuing standards for security, interoperability and data portability.

The National Cloud Strategy of May 2021 acknowledges that the US private sector has an unassailable lead. We now need to **manage our dependence over the long term**. The government's gamble is based on the precedent set by the nuclear industry, where autonomy was achieved under licence from American technologies.

6. BRINGING CYBERSECURITY WITHIN REACH OF ALL BUSINESSES

The old adage *"prevention is better than cure"* applies particularly well to cybersecurity. The reality is that both aspects must be addressed. Add to this the need to punish cybercriminals.

The report puts forward <u>three areas for proposals</u> to develop the virtuous circle of cyber protection: test, alert, protect.

AREA 1: TEST AND STRENGTHEN COMPANIES' BUSINESS RESILIENCE AND CYBER RESILIENCE

The ***cybermalveillance.gouv.fr*** platform should be promoted more effectively to businesses, and an emergency service should be made available to businesses, drawing on **young people** in civic service with the appropriate digital skills (**proposal 1**).

An **anonymised collection of reports** should be made available to encourage companies to report cyberattacks while avoiding damage to their reputation and discouraging publicity about malicious software. This will also provide reliable statistics (**proposal 2**).

Computer Security Incident Response Teams (CSIRTs) should be rolled out **to the regions** to improve access to cyber protection for SMEs and **raise awareness among local authorities**. Along with public hospitals, local authorities are **new targets for cybercrime** (**proposal 3**).

To strengthen the resilience of the business fabric, the government should:

- draw up **national plans for preventing cyber risks**;
- **coordinate the response** of public authorities and private businesses **in the event of a systemic digital attack** affecting a significant proportion of companies, regardless of their size;
- organise regular **simulation exercises** (**proposal 5**).

AREA 2: ALERT, ADVISE, TRAIN ON THE CYBER THREAT

Employees and company directors must be made more aware of cybersecurity, digital hygiene and protective measures:

- Employees should be offered **cybersecurity awareness training as part of their professional training** (**proposal 9**).
- **Company directors**, who may be held personally liable in the event of a cyberattack on the value chain in which they are involved, should be made more aware of the risk of becoming a victim and being held liable. The matter should be addressed when defining the company's strategy (**proposal 15**).

Certification against a **cybersecurity framework** that is affordable for SMEs and VSEs should be encouraged (**proposal 14**).

To underscore the need to strengthen **security by design**, the "software warranty" on security updates should be extended to companies. A **corporate cybersecurity hackathon** could also be organised for World Cybersecurity Day on 30 November every year, supported by ANSSI and targeting new-to-market software (**proposal 13**).

To raise awareness of cybersecurity among the general public, a **cyberscore for digital platforms** should be introduced, as proposed recently by the Senate (**proposal 22**), and a **massive campaign to promote cybersecurity professions** should be launched (**proposal 10**).

AREA 3: PROTECT MID-SIZED COMPANIES, SMEs AND VSEs WITH APPROPRIATE TOOLS

The government cyber protection structure must be strengthened in terms of both human and financial resources

The creation of a **cybercampus** bringing together public- and private-sector cybersecurity players will be an asset in the fight against cybercrime.

To strengthen the criminal justice response to cybercrime, there is a need to: develop the initial and ongoing training in cybercrime for judges; increase the number of security force staff specialised in cybersecurity; provide cybersecurity forces with adequate funding; study the feasibility of creating a national public prosecutor's office to combat cybercrime; and create a specialised chamber to combat cybercrime at each level of the courts (**proposal 6**).

To respond to the industrialisation of cybercrime, **criminal proceedings must be adapted to speed up the judicial response and strengthen cooperation** with ANSSI over and above the fight against terrorism (**proposal 7**).

The French Presidency of the European Union in the first half of 2022 should be used to speed up negotiations on the **amendments to the Council of Europe's 2001 Budapest Convention on Cybercrime** and on the **European draft Regulation on e-Evidence**, and to **resume negotiations between the European Union and the United States** aimed at stepping up international cooperation against cybercrime (**proposal 8**).

To help strengthen the French cyber protection ecosystem, **public procurement law must be changed**:

- to make the provisions of the Decree of 24 December 2018 permanent, allowing local authorities to award a contract for "innovative services" without a competitive bidding process;
- to provide access to the cybersecurity solutions available outside wholesale markets;
- to consider the feasibility of allowing network operators to prioritise European or national purchases of cybersecurity solutions (**proposal 4**).

The role of insurance is key to strengthening corporate cybersecurity

Firstly, **insurance cover for both ransomware and administrative sanctions in the event of a breach of personal data protection regulations should be banned**, both at the European and national levels (**proposal 12**).

Secondly, **the insurance market needs to be strengthened** by:

- **gaining a better understanding of the risk** through knowing as much as possible about the claims;
- **using certified cybersecurity software and experts** to promote the ***Cyber Expert*** **label**;
- **creating a European cyber rating agency, using the standards** of the European Union Agency for Cybersecurity (ENISA), **or a French cyber rating agency**, using ANSSI standards (**proposal 16**).

Thirdly, **insurance claims for losses resulting from a cyberattack should only be paid out where the company has used a service provider with the *Cyber Expert* label** (**proposal 11**).

Simple and shared solutions for SMEs and VSEs

To **overcome the shortage** of expert staff, **SMEs need solutions that provide access to a pool of information system security managers** (ISSMs), such as setting up employer groups with "trusted third party" status (**proposal 17**).

To make life **easier** for companies, a **cybersecurity solution package** should be developed **for VSEs and SMEs** (**proposal 18**) and, in particular, the feasibility of a **quick-start solution that configures a company's cloud services to comply with the cybersecurity requirements defined by ANSSI** should be considered. **Furthermore, a joint Franco-German approach could make a stronger case for SMEs to be given greater consideration** in the common European strategy for cybersecurity in the cloud, defined by ENISA (**proposal 20**).

To **pay for** this upgrade in cyber protection, the French government should introduce **a tax credit for SMEs and VSEs**, as the Senate has recommended on several occasions. **This would cover part of the cost of the tools needed** (software or cloud subscription) and the **cybersecurity training for company directors and employees** (**proposal 21**).

To **restore a balanced business relationship** in the cloud, **SMEs and VSEs whose main activity is not related to digital technology must be granted protection against unfair terms under Article L.212-1 of the French Consumer Code** (**proposal 19**).

22 PROPOSALS TO BOOST CYBERSECURITY IN INTERMEDIATE-SIZED COMPANIES, SMEs AND VSEs

Proposal 1: Promote the *cybermalveillance.gouv.fr* platform more effectively to businesses and make an emergency service available to companies; young people with the appropriate digital skills could carry out their civic service in this area.

Proposal 2: Open an anonymised collection point for reporting cyberattacks on companies; this will provide reliable statistics.

Proposal 3: Establish Computer Security Incident Response Teams (CSIRTs) in the **regions** and include cybersecurity in regional economic development, internationalisation and innovation plans (SRDEIIs) to raise awareness among local authorities.

Proposal 4: Adapt public procurement law to support the cybersecurity ecosystem by:

- Making the provisions of the Decree of 24 December 2018 permanent, allowing local authorities to buy “innovative services” without a competitive bidding process;
- Providing access to the cybersecurity solutions available outside wholesale markets;
- Considering the feasibility of allowing network operators to prioritise European or national purchases of cybersecurity solutions.

Proposal 5: Develop national cyber risk prevention plans to coordinate the response of public authorities and private businesses in the event of a systemic digital attack affecting a significant proportion of companies, regardless of their size. Organise regular **simulation exercises**.

Proposal 6: Strengthen the criminal justice response to cybercrime:

- Develop the initial and ongoing training in cybercrime for judges;
- Increase the number of security force staff specialised in cybersecurity;
- Provide cybersecurity forces with adequate funding;
- Study the feasibility of creating a national public prosecutor’s office to combat cybercrime;
- Create a specialised chamber to combat cybercrime at each level of the courts.

Proposal 7: Adapt criminal proceedings to take account of cybercrime and strengthen cooperation between judicial institutions and ANSSI over and above the fight against terrorism.

Proposal 8: Speed up European negotiations on the draft Regulation on **e-Evidence** and **resume negotiations between the European Union and the United States** aimed at strengthening international cooperation on cybercrime.

Proposal 9: Require that employees be offered cybersecurity awareness training as part of their professional training in digital technology.

Proposal 10: Launch a massive campaign to promote cybersecurity professions, jointly funded by the government and the private sector.

Proposal 11: In the longer term, only pay out on insurance claims if companies have used a service provider with the *Cyber Expert* label.

Proposal 12: Ban insurance cover for both ransomware and administrative sanctions in the event of a breach of personal data protection regulations, through an amendment to the Council of Europe's Budapest Convention, an EU regulation and an express legislative provision in the French Insurance Code.

Proposal 13: To strengthen security by design:

- Consider extending the "software warranty" on security updates to businesses;
- Organise, with support from ANSSI, a "cybersecurity hackathon" for companies on World Cybersecurity Day, 30 November.

Proposal 14: Build a framework that can be used by SMEs and VSEs to strengthen cybersecurity **certification**.

Proposal 15: Raise awareness among SMEs of the personal liability incurred by company directors in the event of a cyberattack on the supply chain in which they are a stakeholder.

Proposal 16: Strengthen the cybersecurity insurance market by:

- Gaining a better understanding of the risk through knowing as much as possible about the claims;
- Using certified cybersecurity software and experts to promote the *Cyber Expert* label;
- Creating a European cyber rating agency, using the standards of the European Union Agency for Cybersecurity (ENISA), or a French cyber rating agency, using ANSSI standards.

Proposal 17: Provide SMEs with solutions that allow them access to a pool of information system security managers (ISSMs), such as employer groups with "trusted third party" status.

Proposal 18: Develop a simplified cybersecurity solution package for SMEs and VSEs.

Proposal 19: Grant SMEs and VSEs, whose main activity is not related to digital technology, protection against **unfair terms** under Article L.212-1 of the French Consumer Code, for cybersecurity-related contracts signed with providers.

Proposal 20: Consider the feasibility of a **quick-start solution that configures a company's cloud services to comply with the cybersecurity requirements defined by ANSSI** and of a joint Franco-German approach given greater consideration for SMEs in the common European strategy for cybersecurity in the cloud, defined by ENISA.

Proposal 21: Introduce a tax credit for company directors and employees of SMEs, covering part of the cost of tools needed and training in cybersecurity.

Proposal 22: Introduce a cyberscore for digital platforms aimed at the general public to raise awareness of cybersecurity.

Serge Babary
President
Senator for Indre-et-Loire (Les Républicains)

Rémy Cardon
Rapporteur
Senator for the Somme
(Socialiste, Écologiste et Républicain)

Sébastien Meurant
Rapporteur
Senator for Val d'Oise
(Les Républicains)

Senatorial Delegation for Enterprises

Telephone: +33 01 42 34 28 96
delegation-entreprises@senat.fr

Read the report:

http://www.senat.fr/rapports-classes/crentr.html