EBOOK

VICTANIS
Market review of Cybersecurity in France

MAY 2021

victanis

Table of contents

1 Introduction

Context

Due to the strong digital transformation of every sector in today's societies, cybersecurity represents a **major strategic issue**: firms and administrations digitalise their processes and interconnect their data networks, and the Internet of things (IoT) is expanding by the day, hence **the need to secure the digital systems through cybersecurity.**

Besides, the Covid-19 crisis has demonstrated the fundamental role of cybersecurity for a nation's resilience, digital tools being the major means of maintaining business and social ties during the lockdowns.

Cybercriminals' targets include natural and legal persons, private individuals, companies and states alike, with goals as diverse as spying, stealing, undermining and sabotaging.

Facing these increasing and evolving threats, **the cybersecurity market offers a variety of answers**: security awareness and training; cybersecurity tools such as anti-malware, identity management or access control; expert assessments and audits; vulnerability management and threat intelligence; emergency intervention and maintenance services; etc.

1 Introduction

What is Cybersecurity?

Cybersecurity includes two types of activities, often combined in practice and both entailing highly qualified human labour, hence a **very high added value** for cybersecurity companies:

- **Services**
  - → Consulting & Advisory;
  - → Risk Management;
  - → Architecture & Design (*governance, implementation*), Audit/Assurance/Compliance (*e.g. with "ethical hacking"*);
  - → Technical Services;
  - → Managed Services (*secure data storage, incident response, threat anticipation and analysis, etc*).

- **Products**
  - → Hardware (*computers, electronic chips, servers, terminals, etc*);
  - → Software (*firewalls, antivirus, detection and surveillance systems, etc*);
  - → Other solutions (*cloud, encrypted communications, etc*).

2 The Global Cybersecurity Market

Each year, **global economy loses around $600 billion to cybercrime** (almost 1% of the global GDP), and there has been a 667% increase in spear-phishing e-mail attacks related to Covid-19 since the end of February 2020.

As a result, **the global cybersecurity market was worth $152.2 billion in 2020**, against $149 billion in 2019. The market is now expected to recover from the Covid-19 outbreak and reach $208 billion in 2023, with a forecasted annual growth rate of 11%.

Besides, **global spending on cyber-protection reached $37 billion in 2019** (up 9% from 2018), and $42 billion in 2020 (up 13%).

Sources:

Joint MacAfee and Centre for Strategic and International Studies (CSIS) report

Capgemini

Research and Markets

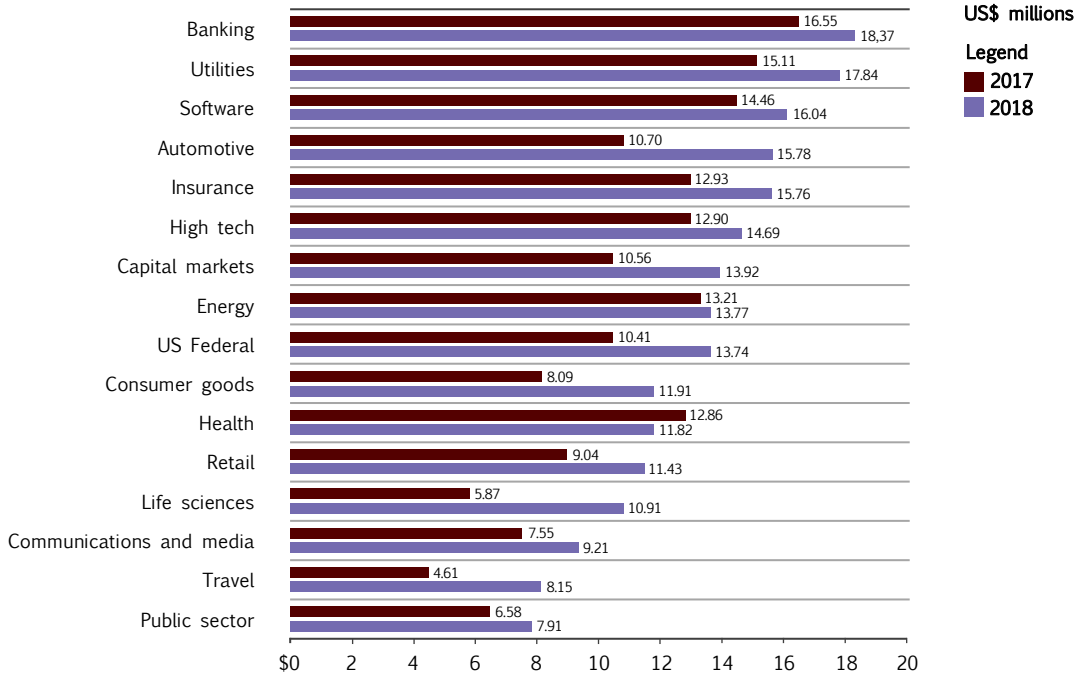
Canalys, quoted in: Guillaume Farde, „Le continuum de sécurité nationale“

2019 Accenture Annual Cost of Cybercrime study

The Cost of Cybercrime

Likewise, the **cost of cybercrime is rising**, with substantial impact to organisations and industries: the total cost of cyber-crime for each company (globally) increased from $11.7 million in 2017 to a new high of $13 million (a 12% increase).

As shown on the graph below, **Banking and Utilities industries have the highest cost of cybercrime**, with an increase of 11% and 16% respectively between 2017 and 2018.



Average annual cost of cybercrime by industry – Accenture

2 The Global Cybersecurity Market

The Cost of Cybercrime

Source:

2019 Accenture Annual Cost of Cybercrime study

External cybercrime costs can be broken down into **four major consequences of attacks**: business disruption, information loss, revenue loss and equipment damage. Adding together the individual cost for each consequence in 2018 gives the total cost of cybercrime to an organisation for that year.

The table below shows **how different types of cyberattacks contribute to each of these main consequences**. The heatmap indicates the largest contribution from each type of attack: malware, web-based attacks and denial-of-service attacks are the main contributing factors to revenue loss.

Besides, although one of the smaller costs of cybercrime overall, **the financial consequences of ransomware have increased by 21% in 2018 alone**.

	Business disruption	Information loss	Revenue loss	Equipment damage	**Total cost by attack type**
Malware (+11%)	$ 0.5	$ 1.4	$ 0.6	$ 0.1	$ 2.6
Web-based attacks (+17%)	$ 0.3	$ 1.4	$ 0.6	$ —	$ 2.3
Denial-of-service (+10%)	$ 1.1	$ 0.2	$ 0.4	$ 0.1	$ 1.7
Malicious insiders (+15%)	$ 0.6	$ 0.6	$ 0.3	$ 0.1	$ 1.6
Phishing and social engineering (+8%)	$ 0.4	$ 0.7	$ 0.3	$ —	$ 1.4
Malicious code (+9%)	$ 0.2	$ 0.9	$ 0.2	$ —	$ 1.4
Stolen devices (+12%)	$ 0.4	$ 0.4	$ 0.1	$ 0.1	$ 1.0
Ransomware (+21%)	$ 0.2	$ 0.3	$ 0.1	$ 0.1	$ 0.7
Botnets (+12%)	$ 0.1	$ 0.2	$ 0.1	$ —	$ 0.4
Total cost by consequence	$ 4.0	$ 5.9	$ 2.6	$ 0.5	**$ 13.0**

Consequences of different types of cyberattacks (average annual cost; figures in US$ million) – Accenture

2 The Global Cybersecurity Market

The Cost of Cybercrime

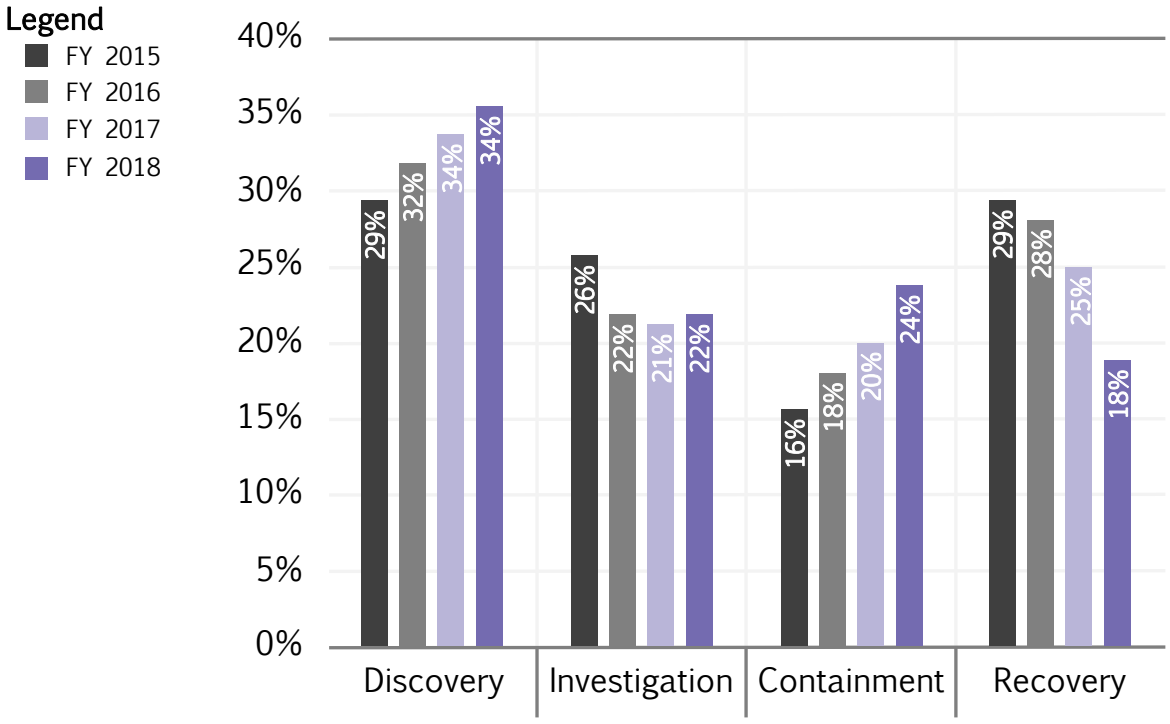
With the understanding of the main consequences of cyberattacks, **organisations can improve their cybersecurity protection**: below is a chart where cybersecurity is broken down into **four major categories of internal activity** (discovery, investigation, containment, recovery).

Source:

2019 Accenture Annual Cost of Cybercrime study

The columns illustrate the evolving **global trend for each activity from 2015 to 2018:** for example, the overall proportion of spending on recovery is reducing annually, and was the lowest component of expenditure in 2018, whereas the proportion of spend on discovery activities has increased steadily since 2015.

This can be explained by the fact that companies **invest more and more in security technologies**, especially security intelligence and threat sharing applications, and **in expert personnel**. Moreover, the expanded use of automation (*machine learning, orchestration, etc*) has allowed recovery costs to decrease.



Percentage of expenditure by internal activity – Accenture

3 The French Cybersecurity Market

Key Figures

Source:

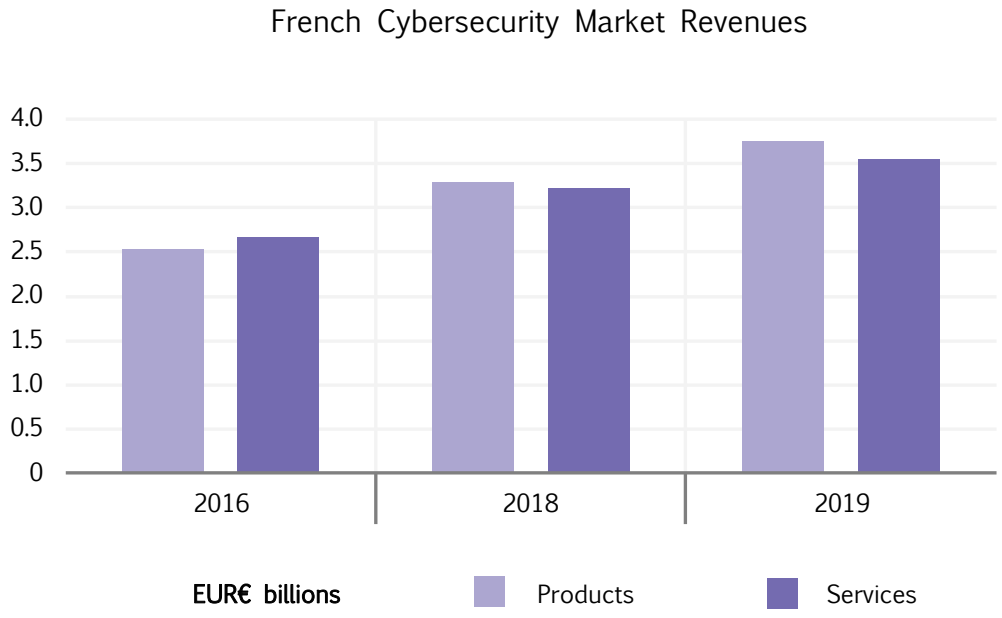
DECISION Etudes & Conseil

CAGR = Compound annual growth rate

In France, state action on the cybersecurity market is essentially of a regulatory and normative nature, leaving the field of cybersecurity services and products open to the emergence of a cybersecurity market.

In 2019, **the French cybersecurity market was worth €7.3 billion**, against €5.2 billion in 2016 with a 11.8% CAGR over this period. Its offer is supported by nearly **600 companies** and dominated by consultancy services.

- Cybersecurity services were worth €3.55 billion in 2019, with a 9.8% CAGR (2016-2019);
- Cybersecurity products were worth €3.75 billion in 2019, with a 13.9% CAGR (2016-2019).

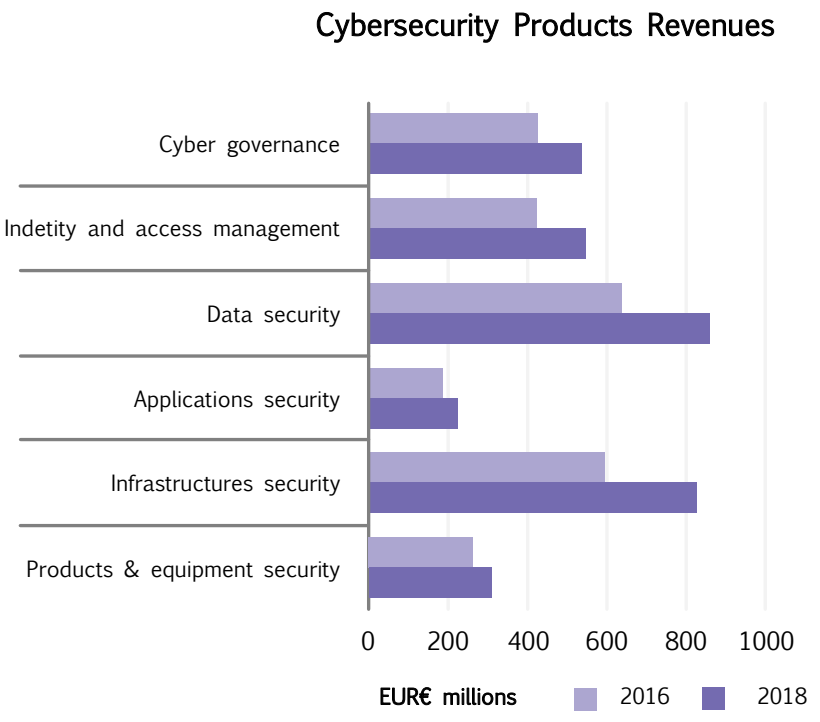


With its new National Cybersecurity Strategy announced in February 2021, the French government is aiming at a **market worth €25 billion in 2025**, thanks to a €1 billion investment in the sector, of which €720 million public funding.

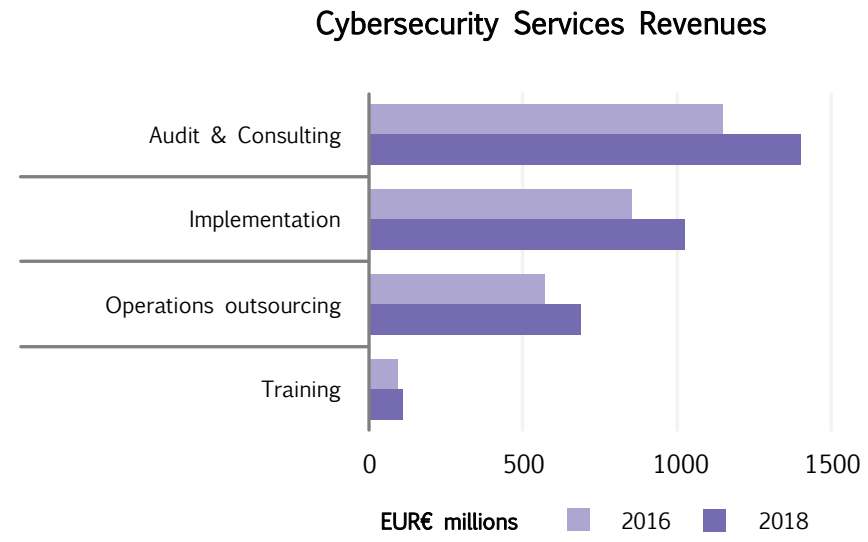
3 The French Cybersecurity Market

Key Figures

Below are the segmentations of the main cybersecurity products and services in France.



Products segmentation	Revenues (€M) 2016	Revenues (€M) 2018	2016-2018 CAGR
Global products market	2540	3300	14%
Cyber governance	427	537	12.1%
Identity and access management	423	546	13.6%
Data security	637	855	15.8%
Applications security	190	225	8.7%
Infrastructures security	594	821	17.5%
Products & equipment security	264	311	8.6%



Services segmentation	Revenues (€M) 2016	Revenues (€M) 2018	2016-2018 CAGR
Global services market	2680	3220	9.6%
Audit & Consulting	1152	1400	10.2%
Implementation	858	1028	9,4%
Operations outsourcing	571	685	9.4%
Training	95	104	4.6%

Source: DECISION Etudes & Conseil

3 The French Cybersecurity Market

The Legal Framework

The European and French legal frameworks related to cybersecurity activities are growing exponentially, becoming increasingly specific and binding.

EU

Topic	Regulation	Adoption	Object
1st EU-wide legislation on cybersecurity	**NIS Directive**	6 July 2016	Establishes a framework for cooperation among EU Member States, through the CSIRTs Network; and ensures a culture of security for critical infrastructures and essential services operators.
Data protection	**GDPR**	4 May 2016	Unifies the data protection framework in the EU, with, among others, the implementation of the concept of "privacy by design".
General	**Cybersecurity Act**	7 June 2019	Strengthens ENISA and establishes an EU-wide cyber-security certification framework for digital products, services and processes.
IoT / Critical infrastructures	**EU 5G Tool-box**	26 March 2019	Comprehensive and objective risk-based approach for the security of 5G and future generations of networks.
Cybersecurity Strategy	**NIS 2.0** → revised NIS Directive)	Proposals, presented on 16 December 2020	Modernises the existing legal framework taking account of the increased digitisation of the internal market and an evolving cybersecurity threat landscape: – Adds new sectors[1] and a clear size cap (all medium/large companies in these sectors will be included); – Imposes a risk management approach for companies, with a minimum list of basic security elements that have to be applied[2]; – Strengthens critical supply chain cybersecurity for key information and communication technologies.
	CER Directive		Member States would adopt a national strategy for ensuring the resilience of critical entities and carry out regular risk assessments.
	SOC Network		Powered by artificial intelligence, it will constitute a real "cybersecurity shield" for the EU.
Addition of cybersecurity requirements	The European Commission is looking at **including cybersecurity requirements into existing directives and regulations**, to make the products more resistant against cyberattacks, following the deployment of the IoT. The first directive being considered is the Radio Equipment Directive (RED); others considered include low voltage equipments, machines and medical devices.		

1. **Essential sectors:** Energy, Transport, Banking, Financial market infrastructures, Health, Drinking/Waste Water, Digital infrastructure, Public administration, Space.
Important sectors: Postal and courier services, Waste management, Manufacture/production/distribution of chemicals, Food production/processing/distribution, Manufacturing, Digital providers.
2. At least: risk analysis and information system security policies, incident handling, business continuity and crisis management, supply chain security, security in network and information systems, policies/procedures (testing and auditing) to assess the effectiveness of the cybersecurity risk management measures, and use of cryptography and encryption.

3 The French Cybersecurity Market

The Legal Framework

FRANCE

Topic	Regulation	Adoption	Object
Data protection	**Data Protection Act** (LIL – *loi informatique et libertés*)	6 January 1978	Sets out responsibilities and clear limits for entities responsible for the collection and processing of personal data, and creates the CNIL (*Commission nationale informatique et libertés*), the French supervisory authority which enforces data protection laws. This act has then been modified by several laws to comply with the EU GDPR.
Criminalisation of malicious acts	**Law on Computer Fraud** (*Loi Godfrain*)	5 January 1988	Acknowledges the importance of data processing systems and represses cybercrime. The legal framework was then expanded to, for instance, extend the criminal liability of cybercriminals to their accomplices (2004 law for confidence in the digital economy), and increase the sentences for passive fraudulent intrusions such as espionage (2015 Intelligence Act).
Critical infrastructures (OIV[1])	**Military Planning Act 2014-2019** (LPM – *loi de programmation militaire*)	18 December 2013	Article 22 establishes a common minimum level of cybersecurity for all critical operators and reinforces the ANSSI to support them in the event of a cyberattack; applies to both public and private operators.
	Military Planning Act 2019-2025	13 July 2018	Enhances detection capabilities: article 34 authorises electronic communications operators (ECAs) to implement detection systems in their networks to detect computer attacks against their customers, which contributes to better secure the OIV's networks.

1. **OIV** (*opérateur d'importance vitale* — critical operators) : Civil, military, judicial activities of the state, space & research, water management, public health, food supply, energy, electronic communications/audio-visual & information, transports, finances, industry.

4 Main Drivers & Restraints

Although cyber awareness is increasing among companies, the majority are **struggling to fully integrate cybersecurity within their organisations**. As a result, the responsibility for network and information systems protection is often split between several roles that do not cooperate well: too few have a dedicated person such as a chief information security officer (CISO, in French: *responsable de la sécurité des systèmes d'information* – RSSI).

Source:

Canalys study, quoted in: Guillaume Farde, "Le continuum de sécurité nationale"

Besides, despite an increase in global spending on cyber-protection, the budget actually allocated by companies to their cyber-protection remains **generally very low**: cyber-protection spending only represent 2% of companies' IT spending.

However, the rising cyberattacks and the central role of the ANSSI (*autorité nationale de sécurité des systèmes d'information* – the French National Cybersecurity Agency) both contribute to drive entities to acquire cybersecurity services to protect their organisations – the only restraint to the market is the lack of specialised manpower.

Market Drivers — Cyberattacks

The increasing complexity of information systems constitutes a **vulnerability**. Indeed, the scope of information systems is constantly expanding, **increasing the organisations' reliance** on these systems. Besides, the multiplication of endpoints and the increased use of the cloud result in as many **points of entry for potential attacks and a complication for surveillance**, thus potential vulnerabilities of the systems' integrity.

Moreover, the lack of harmonisation of security requirements between stakeholders and the complex coordination of legislative frameworks both represent, once again, as many additional threats for the networks' sovereignty.

4 Main Drivers & Restraints

Market Drivers — Cyberattacks

Source:

Hiscox 2020 report on cyber-risks management.

The followings are the four main cyberthreats:

- ◊ **Destabilisation:** Undertaken by hacktivists, these attacks aim at damaging the reputation of state entities or companies and spreading values or ideologies, *e.g. through distributed denial of service (DDoS), website defacement, or data theft/ disclosure.*
- ◊ **Espionage:** Undertaken by structured groups (*foreign states, proto-states or industrial rivals*) with economic or political motivations, these sophisticated attacks aim at exfiltrating strategic information, *e.g. through APT*.
- ◊ **Sabotage:** Undertaken by structured groups, these attacks aim at making systems inoperative, *e.g. through DDoS*, resulting in disorganisation and production/operation disruption. The consequences for the company or state entity are financial or even societal.
- ◊ **Cybercrime for profit:** Undertaken through leveraging vectors such as ransomware or phishing, these attacks may affect national security if directed against states entities or critical infrastructures. In general, around 6% of firms pay a ransom after an attack, but 1 out of 5 firms in France.

Below is a non-exhaustive list of the main types of attacks used by cybercriminals:

- **DDoS** (distributed denial-of-service): A disruption of the normal traffic of a targeted server, service or network by overwhelming it with a flood of Internet traffic, through the use of multiple compromised computer systems (botnets).
- **Ransomware**: A type of malware that infects the system and asks for a fee in order for the system to work again. It can be installed through many ways, *e.g. deceptive links in an e-mail or a website.*

4 Main Drivers & Restraints

Market Drivers — Cyberattacks

- **Trojan horse**: A type of malware, often disguised as a legitimate software, employed to gain access to a system.
- **Phishing**: An attempt to obtain sensitive data by posing as a legitimate institution.
- **Virus**: A malicious code or program written to alter the way a computer operates, designed to spread from one computer to another.

Sources:

Hiscox 2020 report on cyber-risks management.

2018 IFOP study for Kaspersky Lab and Euler Hermes

2019 Wavestone report

The most affected sectors are the **finance, manufacturing and telecommunications industries**, as well as, increasingly, the **energy and pharmaceutical sectors** because of their dependency on automation, and finally the infrastructures **that are critical to state sovereignty**.

Besides, some attacks are **indirect**: the cybercriminals compromise an intermediate target (*supplier, partner, etc*) and exploit the trust relationship that unites it with the final target to reach it. This threat is increasingly important as final targets become more and more secured.

Since the beginning of the Covid-19 crisis, **French local authorities have seen a 400% increase in cyberattacks on their systems**. Besides, more than 76% of the surveyed French medium-sized companies reported having suffered at least one cyberattack in 2017, and 21% of the SMEs.

The consequences of a cyberattack can be important in the short term (*interruption of activities, etc*), but also in the long term: difficulty in attracting new customers, loss of clients and/or business partners.

4 Main Drivers & Restraints

Market Drivers — The ANSSI

French public authorities have long positioned themselves in favour of the development of a framework conducive to cybersecurity activities, making France **a pioneer state in this field**: economic players were gradually made aware of their responsibilities regarding data and systems protection, while cybercrime was progressively defined and criminalised.

Founded in 2009, the ANSSI is responsible for fostering a coordinated pro-active response to cybersecurity issues in France and driving awareness actions. Indeed, digital sovereignty requires mastering cybersecurity and strengthening the French industrial base, as well as the foundation of a European cybersecurity industrial base.

Its missions are carried out through, among others, the **enactment of safety standards** and the **certification and qualification of cybersecurity methods and solutions** developed by the private sector.

Examples of certifications include:

- SecNumCloud: Initiative by the ANSSI aiming to improve public authorities and OIVs' protection, through a label that demonstrates the high level of security met by cloud solution providers.
- eIDAS (electronic identification, authentication and trust services): EU regulation on electronic identification and trust services for electronics transactions in the European Single Market.

Beyond these frameworks, internationally recognised security standards include ISO 27001 and ISO 27701.

4 Main Drivers & Restraints

Market Restraints — The Lack of Manpower

Sources:

OECD, quoted by PwC.

DECISION Etudes & Conseil

The lack of skilled labour specialised in cybersecurity is the **main restraint** to the French cybersecurity market. Indeed, the offer for specific cybersecurity undergraduate or graduate degrees is very limited, resulting in a **shortage of qualified training**.

The vast majority of the specialised graduates tend to be recruited by state services such as the DGA, or by large French industrial groups such as Thales, Airbus, Orange, etc.

Besides, **these graduates are mainly unapproachable** by SMEs which cannot afford their highly qualified salaries. Indeed, the salaries of French cybersecurity specialists are 2.6 times higher than the average in OECD countries, i.e. more than 80 000€.

SWOT Analysis of the French Cybersecurity Market

Strengths	Weaknesses
• Competitive clusters (*CICS, Bretagne Développement Innovation*); • Competitive edge in the field of personal data protection; • Skills leadership in several fields (*identity management, cryptography, IoT securing, machine learning, etc*); • Creation of cybersecurity trainings in public-private partnerships (*ex: training for engineering skills*).	• Lack of specialised resources; • SMEs specialised in a specific sub-segment with tailor-made offers tend to mainly work with large companies. As a result, SME clusters are developed to encourage partnerships (*ex: Hexatrust*); • Weak public order due to austerity policies; • Public requirements are still poorly implemented, especially by the critical operators.
Opportunities	**Threats**
• Implementation of the GDPR and security certification of IoT; • Increasing awareness regarding the necessity for a digital sovereignty; • Development of global cybersecurity offers bringing together various players; • Growing offers and markets (*ex: IoT securing, data sovereignty, digital identity, cryptography, AI, blockchain*).	• International competition, especially from the US (*increasing involvement of the GAFA, especially in the field of IAM – identity access management – where France is a leader*), and increasing presence of Asian companies on the market (*French SMEs cannot compete with their prices*); • Insufficient awareness regarding the importance of security issues, especially in the field of IoT and security by design.

5 Market Demand

There is a need for cybersecurity at every stage of an activity, in order to **develop resilience** through the following five phases – which also need to consider the people/processes/technology dimensions: Prevention, Protection, Detection, Response & Recovery, Improvement (PDCA cycle approach).

As a result, listed thereafter are two enumerations of activities that should be developed in a **cybersecurity value chain** in order to adequately manage cybersecurity risks.

Product / Platform

Product/Platform lifecycle → / Cybersecurity lifecycle ↓	Design	Production	Operation	Assurance	Crisis management
Prevention	- Security by design - Awareness - Training			- Security policies compliant to regulations - Security certifications - Awareness	- Training - Awareness - Consulting - Risk Management
Protection	- System and code redundancy - Cryptography (*encryption, digital signature, etc*) - Access control	- Execution of security by design: integration of security mechanisms (*protections, email filters, etc*)	- Execution of security by design: use of security mechanisms (*protections, email filters, etc*)	- Audits - Maintenance	- Training - Consulting - Processes (business continuity/recovery plans) - Risks matrix - Compartmentalisation - Non-digital services
Detection		- Integration of tools and processes to alert (*e.g. antivirus, endpoint detection & response tools – EDR*)	- Incident or breach reporting processes	- Training - Raise customers, third parties and suppliers' awareness	- Training - Consulting
Response & Recovery				- Consulting - Training - Cyber-insurance	- Processes - Mitigation technologies
Improvement	- Periodic review and improvement of the design efficiency following assessments	- Periodic review and improvement of the production process	- Periodic review and improvement of the conduct of operations	- Periodic review and improvement of controls efficiency	- Lessons learnt from incidents (post-mortem) - Periodic review of the processes efficiency and adjustment to the evolving regulations and threats

5 Market Demand

Critical Infrastructure

Critical infrastructure lifecycle → / Cyberprotection lifecycle ↓	Construction phase			Operations phase	
	Architecture	Design	Construction	Maintenance	Crisis management
Prevention	- Business environment (*identification of role/place, establishment of priorities & critical functions*) - Resilience requirements - Training & professional certifications	- Security policies compliant to regulations - Business continuity/ disaster recovery plans definition			- Training - Consulting - Risk Management strategy - Awareness - Identification of asset vulnerabilities - Business continuity/disaster recovery plans definition
Protection	- Security certifications and qualifications	- Identity management - Network access control	- Integration of protective technologies (*firewalls, etc*)	- Audits and maintenance operations - Comliance assessments	- Risks matrix - Processes (business continuity/ recovery plans) - Consulting - Training - Awareness
Detection			- SIEM deployment - Integration of detection and reporting processes	- Periodic vulnerability scans - SIEM operation - Continuous monitoring	- Training - Awareness
Response & Recovery	- Response, mitigation & recovery planning		- Mitigation technologies		- Business continuity/disaster recovery plans implementation - Communications - Analysis - Mitigation
Improvement	- Period review and improvement of the architecture following assessments - Compliance to new security certifications and qualifications	- Periodic review and improvement of the design efficiency	- Periodic review and improvement of the construction process	- Periodic review and improvement of controls efficiency	- Lessons learnt from incidents/ breaches (post-mortem) - Periodic review of the processes efficiency and adjustment to the evolving regulations and threats

6 Market Supply

Source:

2016 study by the DMISC of the French Home Office

The French actors are **at the cutting edge in terms of skills and R&D**: France is one of the world leaders in the field of cryptography, and is one of the top 3 in the world in post-quantum technologies; it is also in a good position regarding blockchain and IoT security.

Indeed in 2015, the average spending burden in R&D of French cybersecurity companies was around 50% of their turnover, while some invested up to more than 100% of their turnover.

These past few years, the French cybersecurity sector has seen the emergence of new players, as well as many mergers and acquisitions which have participated in the consolidation of the cybersecurity activities of the leading companies in the sector.

The main French cybersecurity providers are the following:

- **Pure players**, whose activities focus mainly on cybersecurity, with a high technical expertise (*CS-Novidy's, Securiview, Sysdream, Intrinsec, Conix, Advens, Synacktiv, etc*).
- Actors providing cybersecurity services **as a secondary occupation:**
  - ◊ **Digital services companies** (*entreprises de services du numérique* – ESN) that have developed a cybersecurity offer (*Capgemini, Atos, Sopra Steria, etc*);
  - ◊ Companies whose original activities are outside IT, such as **telecommunications companies** (*Orange Cyberdefense*);
  - ◊ Historical **defence industries** (*Thales, Airbus*).

Thereafter are the segmentations of the main cybersecurity products and services, with the numbers of firms in 2018 and some examples.

6 Market Supply

Products

Products segmentation	2016-2018 CAGR	Number of firms in 2018	Examples
Global products market	14%	669	Thales, Orange Cyberdefence, Airbus Cyberdefence
Cyber governance	12.1%	197	Brainwave, Egerie, Kun Cleaner, Straton-IT, Trustinsoft, Adec, Arcad Software, Leasia, Transformeo, Procompliant
Identity and access management	13.6%	196	Evidian, Ilex International, Idnomic, Inwebo, Neowave, Novalys, Wallis, Systancia, Icare, United Biometrics, Hubrix, KeoPass, Rubycat, HIAsecure
Data security	15.8%	313	Synacktiv, Fireeye, Atempo, Captain DPO, CDC Arkhineo, Edicia, Idecsi, Oodrive, Wooxo, Antemeta, ASP Serveur, Jaguar Network, Outscale, Ercom, Prim'X, Thegreenbow, Buster AI, Ugloo, Antiopea, Olvid, Transchain
Applications security	8.7%	153	ITrust, Fireeye, Vade Secure, 6cure, Efficient IP, Olfeo, Pradeo Security Systems, Rohde & Schwarz Cybersecurity, Trust-in-soft, Intuitem; eShard, V6Protect, Ozon, Diskyver
Infrastructures security	17.5%	312	Securiview, Synacktiv, Brandsays, Cyber-Detect, Fireeye, Holiseum, Seclab, Sentryo, Sunbren
Products & equipment security	8.6%	153	Securiview, Synacktiv, Prove & Run, Secure-IC, 6cure, Misakey, Datae, Didomi

Sources:

DECISION Etudes & Conseil

Hexatrust

Wavestone

Pôle Excellence Cyber

Note:

The addition of the number of firms by market segment isn't equal to the number of firms on the global market, as most firms provide several services and products, hence corresponding to several segments.

Services

The fastest growing segment among cybersecurity services is **Audit & Consulting**, which also has the largest number of firms.

Services segmentation	2016-2018 CAGR	Number Of firms In 2018	Examples
Global services market	9.6%	664	Thales, Orange Cyberdefence, Airbus Cyberdefence
Audit & consulting	10.2%	620	**Audit**: Apsys, Sysdream, Conix, Advens, Synacktiv **Consulting**: Accenture, Sogeti (Capgemini), Deloitte, CS Group, Wavestone, Conix, Advens, Sopra Steria, Beijaflore, Inetum, Amossys, DCI Group
Implementation	9.4%	425	Opteamis, Wizbii, Algosecure, GIP SIB
Operations outsourcing	9.4%	331	CS-Novidy's, Securiview, Conix
Training	4.6%	206	Sysdream, Intrinsec, Advens, Synacktiv, Conscio Technologies, Metsys, Synetis, Diateam

Glossary

- **NIS Directive:** Security of Network and Information Systems.
- **CSIRT:** Computer security incident response team.
- **GDPR:** General Data Protection Regulation.
- **ENISA** – European Union Agency for Cybersecurity: Contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow.
- **CER:** Critical Entities Resilience.
- **SOC:** Security Operations Centre.
- **Hacktivists:** A person who uses computer-based techniques as a form of civil disobedience to promote a political or social agenda.
- **APT** – Advanced Persistent Threat: A stealthy actor gains unauthorized access to a computer network and remains undetected for an extended period.
- **DGA:** Délégation Générale de l'Armement.
- **Hexatrust:** Cluster of innovative companies in cloud computing (on-demand availability of computer system resources, especially data storage) and cybersecurity.
- **PDCA Cycle Approach:** The Plan-Do-Check-Act approach is a cycle for implementing change which, when followed and repeated, would lead to repeated improvements in the process it was applied to.
- **Security by design:** Approach to security that allows to formalise infrastructure design and automate security controls so that security can be built into every part of the IT product lifecycle.

Contact

Victanis Advisory Services

Emma Vincent

Eric Lambert

18-24 Turnham Green Terrace

London, W4 1QP

+44 (0)20 8996 5088

eric.lambert@victanis.com

emma.vincent@victanis.com