WAVESTONE

CYBERSECURITY START-UPS IN FRANCE:
TIME TO SCALE UP TO ACHIEVE POTENTIAL

The cybersecurity ecosystem continues to grow rapidly. It rewards expertise as well as innovation. This has not gone unnoticed in France, where numerous entrepreneurs have taken on the adventure of launching businesses in the sector. Conditions are favorable, so what factors are preventing young companies from achieving their full potential and going out to tackle the international market?

AUTHORS

GÉRÔME BILLOIS
gerome.billois@wavestone.com

JULES HADDAD
jules.haddad@wavestone.com

A THRIVING ECOSYSTEM

128 start-ups, a significant increase from 2017

Last year, there were 100 cybersecurity start-ups in France. This year, their number is up a full 28%. This goes hand in hand with the slightly growing number of jobs in the sector, which now employs 1,100 people. Numbers are expected to continue to increase thanks to the sector's strong growth, but remain weak for now given that 72% of the sector's businesses have fewer than 10 employees.

128 cybersecurity start-ups in France

28% up on 2017, representing more than

1,100 direct jobs
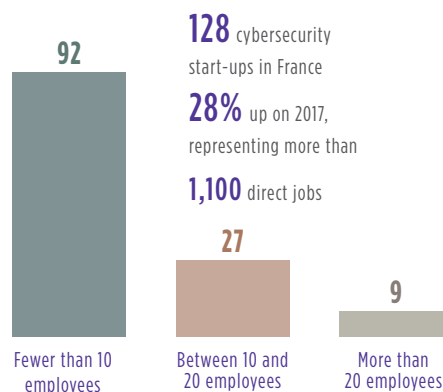
Number of employees per start-up

- 92 — Fewer than 10 employees
- 27 — Between 10 and 20 employees
- 9 — More than 20 employees

START-UP TEAMS RARELY INCLUDE A SALES SPECIALIST

In 70% of cases, the team that creates a start-up does not include anyone specialized in sales. A lack of commercial skills in a business's early stages can stunt its growth. However good a product or service may be, it needs to be designed from the outset to appeal to clients.

The ecosystem has a good geographical spread

Although more than half (57%) of these start-ups in France are based in the Paris region, other centers are developing with significant numbers of start-ups located in the cities of Rennes and Lyon, and in the PACA region. Having a base outside Paris may prove advantageous when recruiting talent.

Location of start-ups

French start-ups are strong in the most technically complex areas...

The French education system produces excellent mathematicians, and the country is generally strong in technology. This has enabled start-ups to develop expertise in highly specialized domains such as blockchain, with organizations including Woolet, Keeex and Utocat. Other start-ups such as Cryptosense and Skeyecode use complex cryptographic logic to solve application security and IAM challenges.

...and see where the potential lies.

The industrial systems security market offers great potential. Start-ups such as Cybellius, Seclab and Sentryo have responded to a need created by a recently developed awareness of the security issues surrounding critical industrial systems and the implementation of new legislation such as the LPM[1] and the NIS directive[2]. Other businesses have understood the growing importance of data privacy, and have focused their solutions on this market, and on GDPR in particular[3]. Onecub, for example, has set itself up as a trusted third-party handling data portability between online services.

A LACK OF AMBITION AND A LOW APPETITE FOR RISK

Although the cybersecurity ecosystem is thriving, it is not in fact achieving its full potential.

The field attracts high levels of investment. Major companies are increasingly keen not only to be in contact with agile start-ups, but also to access the disruptive technologies they offer. Despite this, the sector is not experiencing the boom we would expect to see, partly because of a lack of ambition and appetite for risk on the part of the start-ups.

Start-ups are innovative but not truly disruptive

We could expect these businesses to produce new, disruptive ideas. However, 70% of them choose to reinvent existing solutions, and the points of difference they add are often too weak. They consequently face competition from existing businesses, which catch up to them very quickly. Only 19% of start-ups create new security solutions. The remaining 11% are working on securing new usages such as the IoT. For example, start-ups Busit and Ackilo secure connected objects and the cloud. Tanker offers an encryption SDK that can be built into SaaS applications.

The potential for differentiation exists but is underused

All too often, start-ups regard their "100% French" credentials as their major point of difference. Although it can be an advantage in this market because some clients prefer a domestic partner, a business cannot succeed purely because it is French. These start-ups need to focus on other factors, in particular, key ones such as the features offered by their product and the technology used in it. While 79% of start-ups believe they do this, the market appears to disagree. This primarily suggests an issue with the way innovation is marketed.
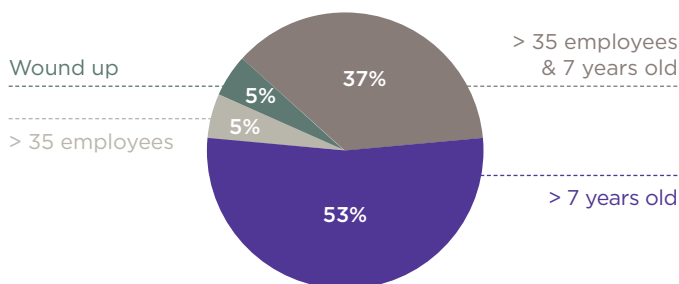
Certifications may help companies to stand out from their competitors, in particular, the CSPN[4] from ANSSI[5] which is coming back into vogue. And yet, just 22% of the start-ups either hold this certification or are working towards it. The most frequent reasons for the decision not to pursue certification are the cost of the process and the effort involved. Cybersecurity is seen as a "cross-functional" area, and sector-based differentiation is almost entirely lacking. However, major companies are attracted to solutions that relate to their specific industries and fit perfectly into their business contexts. Solutions therefore need to be presented in a way that takes into account these contexts
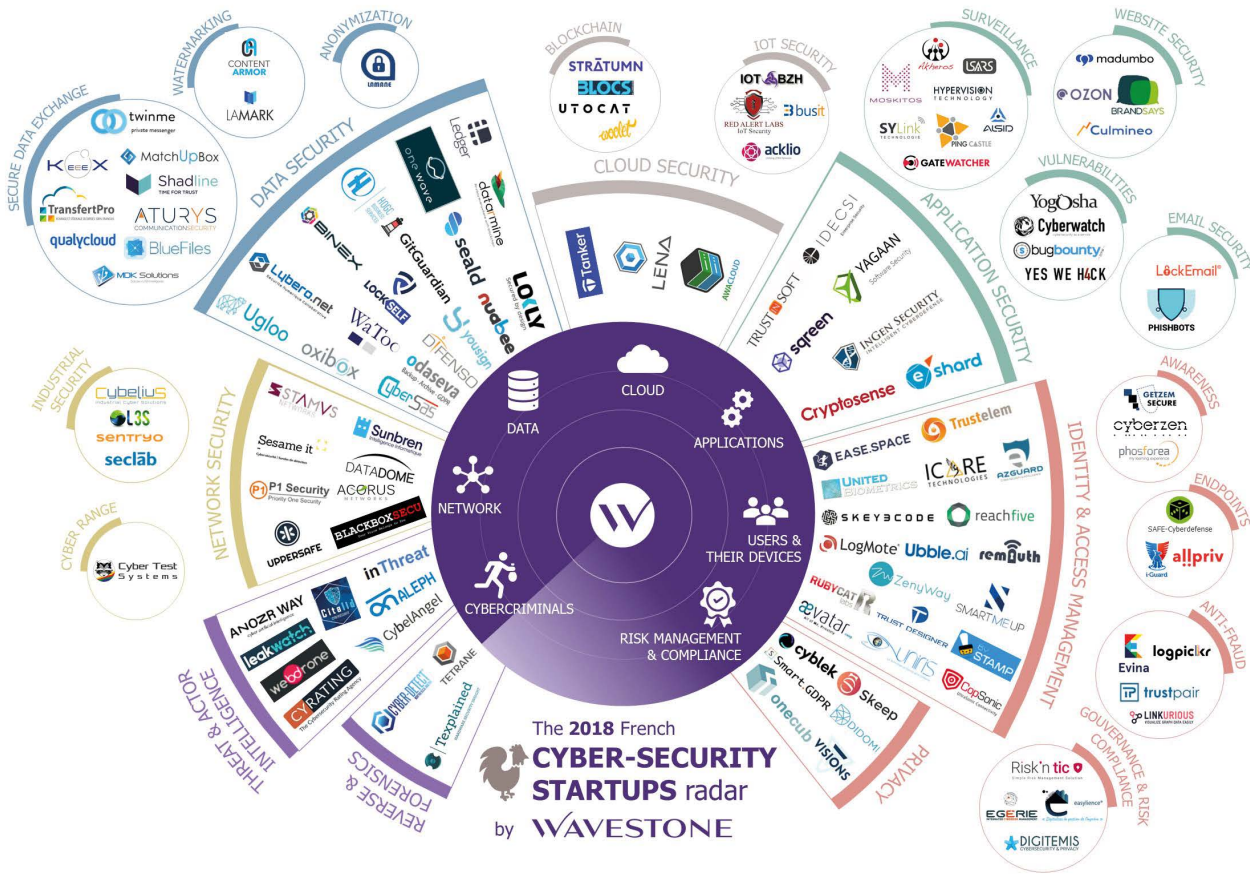
1- French Military Programming Law 2014
2- Network and Information Security
3- General Data Protection Regulation
4- Level One Security Certification
5- National Cybersecurity Agency of France

Positioning of these start-ups in terms of innovation

70% **Reinvent** existing solutions

19% **Create** new security solutions

11% **Secure** new usages

19 start-ups exited the radar between 2017 and 2018

Wound up

> 35 employees

5%

5%

37% > 35 employees & 7 years old

53% > 7 years old

The 2018 French CYBER-SECURITY STARTUPS radar by WAVESTONE

DEVELOPING THE START-UP RADAR

Since 2015, Wavestone has been actively monitoring start-ups as part of its ShakeUp program. As the company is actively involved in the French cybersecurity innovation arena, with numerous contacts, the radar lists almost 400 entities across Europe and internationally, with a particular focus on France. The criteria for including a company in the French radar are: head office in France, fewer than 35 employees and a legal structure which is less than 7 years old (unless a major repositioning has occurred). Following monitoring by our teams in the cybersecurity and digital trust practice, we meet with the most innovative start-ups to evaluate their solutions. Some may join ShakeUp, Wavestone's acceleration program. http://www.wavestone.com/shakeup

and highlights specific use cases that speak to clients. Certain start-ups such as Trustpair have created solutions specifically suited to finance departments.
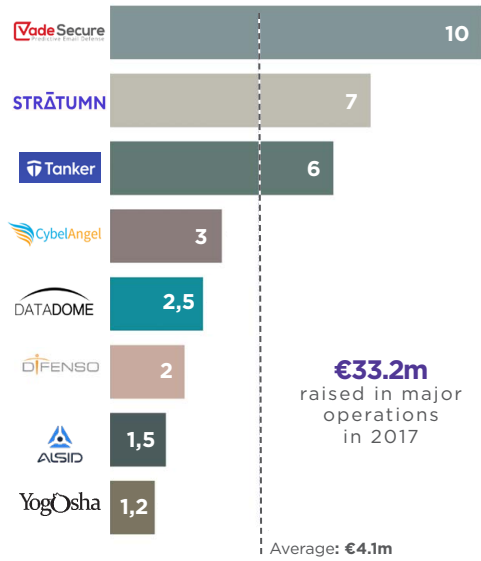
Observations show that companies struggle to grow

Looking at the 19 start-ups that exited the radar between 2017 and 2018, it is clear that growth is an issue. In 67% of cases, the company exited the radar based on age (more than 7 years old), which proves that companies can subsist without growing to employ more than 35 people. This lack of ambition is also supported by the surprising statistic that only 5% of start-ups in the sector are wound up. Studies suggest that, across the economy as a whole, the figure is around 50 to 75%[6]. Even more surprisingly, cybersecurity start-ups access the market very quickly. Half of them say they

signed their first clients after just 6 months. Investment, however, does not follow, and with the exception of a few highly visible fund-raising operations, it is rare for them to be able to access several million euros of capital.

An analysis of the French business funding ecosystem explains this issue. It shows that investors are willing to put money behind businesses in their very early stages (seed capital). However, there is a lack of funding for companies that have reached the stage where they need to raise higher levels of capital to finance rapid growth (series A). Consequently, start-up growth stagnates and they are unable to invest sufficiently in staff recruitment or R&D. It is important to note that 30% of start-ups wish to remain independent and do not seek to raise capital.

6- Source: *statisticbrain & Harvard Business School*

2017's major fundraising operations

Vade Secure	10
STRATUMN	7
Tanker	6
CybelAngel	3
DATADOME	2,5
DIFENSO	2
ALSID	1,5
YogOsha	1,2

€33.2m raised in major operations in 2017

Average: **€4.1m**

POTENTIAL FOR CHANGE

There are various ways in which the situation outlined above could be improved.

Firstly, major companies could help the ecosystem develop by paying for POCs

A POC (Proof of Concept) is an almost essential part of the sales process when working with major companies. Generally, well-established solutions publishers provide major companies with POCs free of charge. However, a start-up is too financially fragile to be able to do this. Indeed, it is hard to see how a start-up could invest the time and resources required to produce a POC without any guarantee that it would lead to a contract. To resolve this issue, it needs to become common practice to pay for a POC, for example in return for a discount on the contract if one is signed. In addition, the sums involved (in the region of ten thousand euros) are often trivial in the eyes of a major company, but significant for a start-up.

The market also needs to adapt to help these companies develop more quickly

Cybersecurity is a specialized field. Developing companies need specific support, in particular because of the technical dimension of the solutions they offer, and in some cases the preference for domestic operators. In the UK, promising young start-ups are brought to light every year by private accelerators such as Cylon and public ones such as the one operated by the NCSC[7]. In contrast, France has barely any accelerators dedicated to cybersecurity. Such structures would give French start-ups the help they need to develop, make themselves known and tailor their solutions to a market which is complicated and constantly changing.

Investment funds dedicated to cybersecurity could be created to combat funding issues. They would reassure investors by spreading risk and explaining market features, and enable companies to scale up and extend their operations beyond their national borders.

To succeed, start-ups need to improve their sales techniques, tailor their products to the market and take risks

It is vital for start-ups to concentrate on their unique selling points and the way they market them. Currently, there are issues with communication: it is hard for major companies to understand the added value to be gained by working with innovative young companies. These difficulties could be overcome if companies moved to a more mature business structure more quickly (80% of start-ups say they are still working "in start-up mode" up until operating for 5 years). This would give them high levels of expertise in key posts, especially sales and marketing. To succeed, start-ups need to be capable of selling products rather than technologies. Start-ups such as Copsonic and Difenso have developed disruptive technologies (an SDK[8] that communicates via ultrasound and an end-to-end encryption SDK respectively). Awareness of these technologies is growing, but the products would be more successful if they were marketed as packaged solutions that match the usage cases encountered by clients.

Internationalization is another challenge many companies face, regardless of the sector in which it operates. Israel is leading the way here once again. As the country has practically no internal cybersecurity market, businesses take an international approach to development from the very beginning. This, together with a highly effective ecosystem which offers them the backing they need, has resulted in a large number of success stories.

Although 72% of the start-ups in the radar say they wish to operate internationally, only 24% do so.

In France, companies tend to develop by widening the applications of their solution to meet the needs of domestic clients. This brings them up against more and more competitors. Others take the diametrically opposite path by working to sell a highly specialized solution to expert buyers on the international market. Examples include Vadesecure's anti-phishing solution recently purchased by Cisco and foreign telecoms operators, and Tanker's SDK which is used by Cisco.

The cybersecurity market is growing rapidly. It is clear that once the barriers discussed have been overcome and the highlighted adjustments are in place, the ecosystem has the potential to thrive so that France can take up its place as a major player. But breaking down these barriers will take concerted action from both the public and private sectors, from incubators through to major companies.

Today, everyone is behind innovation, but concrete actions are lacking.

7- National Cyber Security Center
8- Software Development Kit

Actions to boost the French ecosystem

Corporate:
Pay start-ups for POCs

Start-ups:
Focus on your key differentiators and know how to market them

Market:
Set up dedicated incubators

Market:
Need dedicated investment funds

WAVESTONE