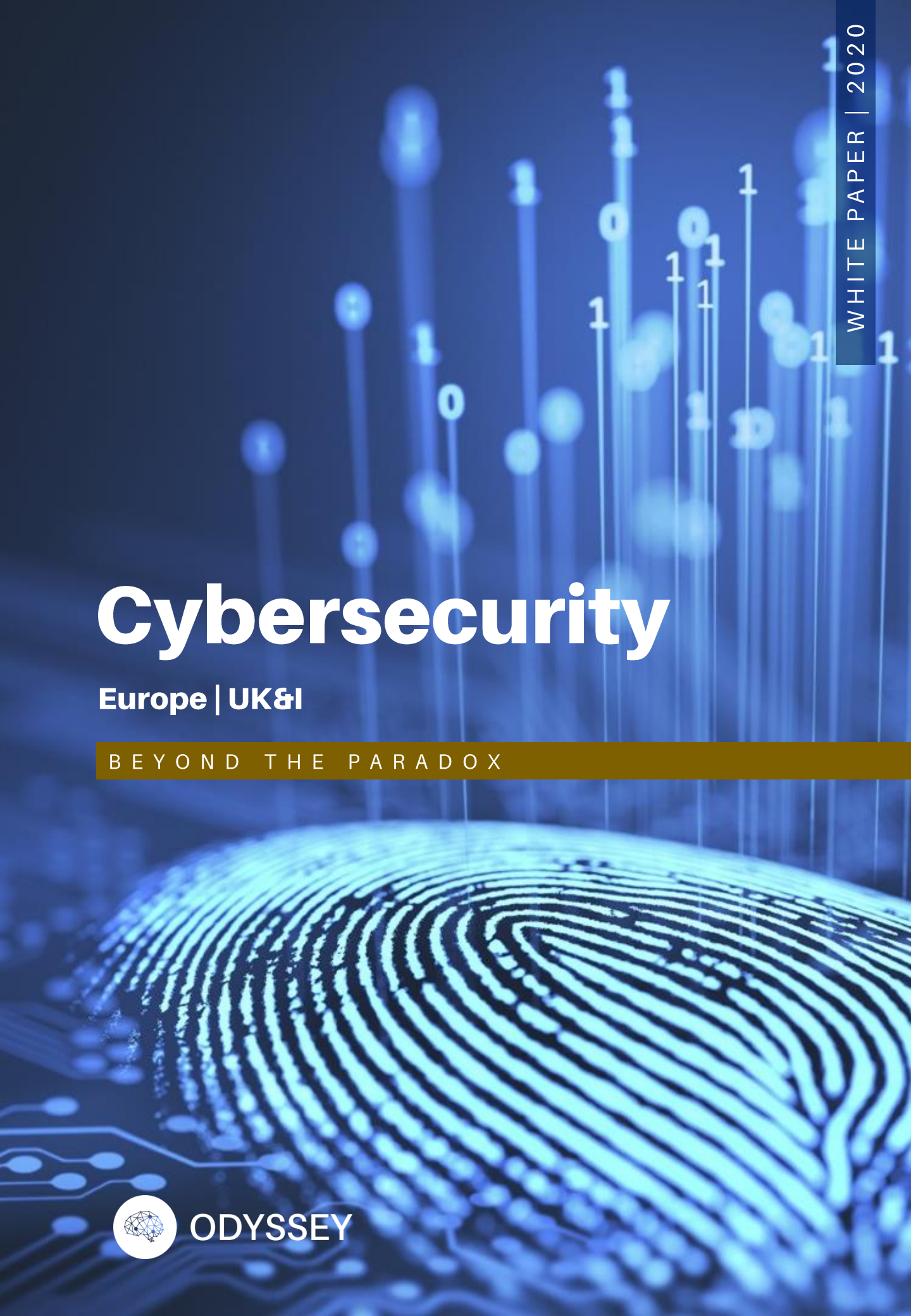


WHITE PAPER | 2020

Cybersecurity

Europe | UK&I

BEYOND THE PARADOX

ODYSSEY

ODYSSEY

A unique offering of bespoke strategy and corporate finance services to technology companies

Odyssey explicitly refers to a fascinating journey, such as the journey back home undertaken by the king of Ithaca, which was sublimely narrated by Homer in the ancient eponymous Greek poem.

Odyssey is a FinTech company that aims at providing technology companies with a unique offering of (1) bespoke strategy and corporate finance advisory services, and (2) innovative SaaS solutions dedicated to financial strategies, to be soon released.

Odyssey is the best strategic partner to ease **your** corporate journey in an era of continuous digital transformation. Both companies and private equity firms face a plethora of unprecedented challenges, while navigating a technology-centric and data-driven world in increasingly volatile, uncertain, complex and ambiguous environments.

Odyssey operates across Europe and the UK to deliver value-adding financial advisory to startup companies, SMEs, large corporates, and PE/VC sponsors, supported by our proven technology market expertise.

La FRENCH TECH

« As a strategic partner for growth, our mission consists of reinforcing the competitiveness of European and UK-based technology companies through our bespoke corporate finance services and solutions »

Axel Tombereau, CEO

STRATEGIC ADVISORY | MARKET INSIGHTS
M&A | BUILD-UP | EXITs
FINANCING ADVISORY | FUNDRAISING | LBOs

Our tech markets expertise

- Cloud & Digital Services
- Cybersecurity Products & Services
- Data Science, Data Analytics & Big Data
- SaaS, Softwares & Marketplaces
- FinTech, Payments & InsurTech
- Artificial Intelligence & Deep Tech
- Semi-conductors & Electronics
- MedTech & Healthcare Tech
- GreenTech, PropTech & CleanTech
- E-sports & Gaming
- Blockchain & DLTs
- Edge Computing & IoT/IIoT
- Media & Digital Agencies
- Quantum Computing

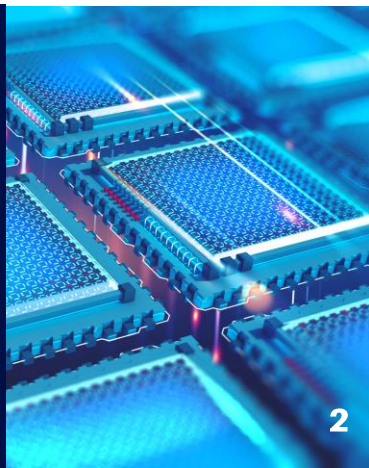


Table of contents

1. Introduction |p.4|
2. Beyond the paradox |p.5|
3. Deciphering the market |p.8|
4. Main industry challenges |p.10|
5. Ahead of the curve |p.12|
6. Investor highlights |p.14|

Introduction

In 2020, Cybersecurity tightens its belt, while offering a brighter long-term outlook

The first key message Odyssey conveys on Cybersecurity is that the industry foundations remain extremely solid over the long-term, despite moderate to strong short-term shockwaves that are subsequent to the Covid-19 multiple crises.

The market growth forecasts effectively rely on the robust assumption of an acceleration of digital transformation of companies across Europe and UK&I. The Covid-19 outbreak has notably triggered a sudden and steep pervasion of remote work practices. This speeded-up trend, whatever its sustainability may be, adds up to major background trends, such as the data deluge, the implementation of 5G services, or the SMEs massive shift to the cloud, just to name a few. Enabling the security of the whole digital value chain, from telecom and cloud infrastructure to endpoints is thus a major challenge for the cybersecurity industry in this fast-changing context, requiring up-to-date competencies.

In this context, sustainable or green cybersecurity practices may hopefully expand across market segments and across the region.

Europe, a world-class cybersecurity ecosystem that lacks adequate funding

The Europe and UK&I regions have been developing word-class ecosystems of cybersecurity products, solutions & services , ranking among other globally reputed leading hubs such as the US, China, Russia, Israel, and Switzerland.

The augmented awareness around cybersecurity stakes triggered by Covid-19 in Europe and the UK&I is a unique opportunity to tackle the scale-up challenge, as most security providers are stil below the radar of public authorities, financial sponsors, or potential large end-customers due to their limited size.

In the UK&I, the end of the Brexit transition process and the enforcement of the adequacy principle with EU regulation from 1 January 2021 may offer new innovation opportunities and accelerate the access to private funding, mainly from the EU and the US.

Europe enters a new phase of coordination initiatives to reach regional digital sovereignty, or, more likely, autonomy. Cybersecurity is actually not only a significant support to economy recovery, but also the cornerstone of most business continuity plans in the ongoing crisis period, and the "glue" linking dominant technologies, as per the metaphor by the ECSO.

First, the creation of a European vision in that regard is utterly needed. Then, public and private initiatives are highly encouraged to efficiently invest in the cybersecurity of critical infrastructure and strategic applications. Finally, the success of the European cybersecurity ecosystem requires to dramatically accelerate the access to funding and liquidity for innovative cybersecurity startups, and to facilitate the emergence of European champions and unicorns, in order to offset the relative lack of midsized and large independent players.

Axel Tombereau
Founder & CEO
axel.tombereau@odyssey.tech
+33 6 43 82 00 12

Beyond the paradox

The Covid-19 health, economic, and social crises have actually been impacting the cybersecurity industry, though in a paradoxical manner.

Augmented Awareness

First, cybersecurity has been most often considered a key enabler of organizations' Business Continuity Plans (BCPs) in the ongoing crisis period. Security has increasingly been on the agenda of executive committees and boards., a rather new phenomenon. This augmented awareness of the security stakes is mainly due to the combination of (i) an unprecedented rise in cyber threats & cyberattacks, (ii) a sudden and radical rdeployment of emote work practices with endpoint security challenges, and (iii) more widely the accelerated digital transformation of SMEs.

The Covid-19 crises have highlighted the limited preparedness of most organizations as far as the sudden shift in work practices is concerned, as a direct consequence of unanticipated lockdown measures in certain European countries, such as France or Italy. In this period, the continuous involvement of CISOs, in-house and external security experts shall not be underestimated.

Short-term cuts in cybersecurity budgets

Second, augmented awareness can not prevent the cybersecurity providers of all types from facing a moderate to strong demand contraction in the short-term.

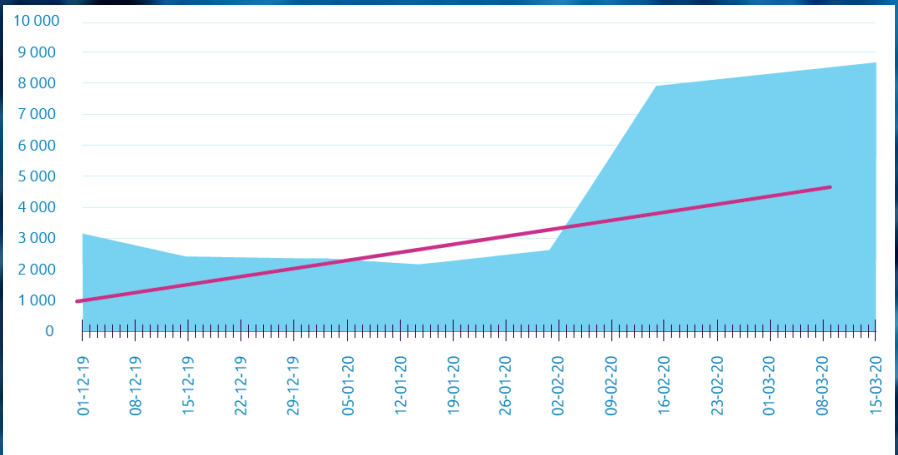
Indeed, as they duly refocus on their urgent business recovery, the vast majority of end customers do not consider cybersecurity a strategic priority. Several factors entice them to conduct a review of their cybersecurity products, SaaS solutions, and projects portfolio in order to streamline their expenses and investments. These confirmed budget cuts are a survival move from organizations that struggle to fulfill working capital commitments in a context of severe GDP contraction, uncertainty around the pandemic evolution, and looming threat of a global liquidity crisis or cash crunch, despite unprecedented quantitative easing stimuli from the ECB the BoE respectively.

As such, the cybersecurity paradox consists therefore of demand contraction in the short-term despite augmented awareness from customers that cybersecurity is a sustainable strategic stake, a mind shift which may positively affect the market over the long-term.

As a consequence of cybersecurity budget cuts, some organizations will increase their exposure to cyber threats, which may reveal a counterproductive strategy in terms of costs, brand image and reputation.

Beyond the paradox

A1. An unprecendeted wave of cyberattacks



+667%

Phishing email attacks increase in one single month in Italy (March 2020)

Graph: Number of phishing attacks in Italy
Source: Cynet, March 2020 & Cap Gemini, April 2020

A2. Key figures on the cost of cybercrime

€ 8m

average cost of data breach in 2020

Source: cybersecurityventures

$6,000,000 m

estimated cost of cybercrime in 2021

86%

of data breaches are financially motivated

Source: Verizon, DIBR 2020

A3. Organizations' limited preparedness

20%

of large corporates have no cybersecurity policy

Source: Varonis' statistics, 2020

40%

of companies acknowledge cyberattacks

40%

of boards consider CEO is responsible in case of cybersecurity failure

Beyond the paradox

Where to expect budget cuts?

Budget cuts may have a steep short-term impact on cybersecurity products, solutions & services providers.

First, there must be a distinction between B2B and B2C markets. In most countries, the augmented awareness of individuals is more than offset by their decrease in spendings due to shrinking purchasing power and economic uncertainty. In the B2B markets, portfolio reviews and budget cuts are confirmed by a rather significant percentage of large companies. Governments and public sector could follow the trend, while the situation is far more nuanced on the SMEs segment.

Cybersecurity products, software, and SaaS platforms might see their revenue at risk if screened as non core or non strategic tools by their end customers. Cybersecurity services may benefit from their certain agility to absorb the shock more smoothly depending on projects nature.

Basically, security projects that relate more directly to operations, and fall out from standard IT budgets are less likely to be affected by the crisis. Security projects that support companies in their short-term recovery, transition to cloud or to remote work may likely be preserved.

Conversely, large long-term projects requiring orchestration capabilities, such as the implementation of a standard security operations center (SoC) are in most cases subject to postponement when not cancelled. This is where the paradox hurts most, at a time when sustained investments in cybersecurity strategies seem utterly needed.

Obviously, the level of postponement will also heavily dépend heavily on the specific verticals addressed by cybersecurity providers. The European players that specialize in hospitality management, retail, aeronautics and other hard hit industries face a diversification dilemma that may lead them to jeopardize their differentiated positioning.

Which players may be the most resilient in the Covid-19 context?

Corporate customers, especially large companies, may leverage their existing relationships with large digital services providers that offer a rather comprehensive suite of digital offerings to negotiate full packages at a lower rate. Large providers may therefore prove the most resilient.

Cybersecurity providers with automation expertise may also somehow take advantage of the Covid-19 consequences.

Deciphering the market

How to read the increasingly complex cybersecurity market?

A standard dichotomy consists of distinguishing among cybersecurity products, solutions, and services. For example, security products include firewalls or malware scans. Enterprise solutions are generally SaaS platforms enabling for instance cyber threat analysis or online compliance solutions. The services segment comprises of monitoring and audits, incident management among plenty others. Products, solutions and services are quite often combined by providers to deliver the best added value to end customers.

Furthermore, the cybersecurity market is spreading and branching out. At a more granular level, the expansion of cybersecurity offerings triggers a deepening specialization of providers: (1) along the value chain from infrastructure to endpoint security, (2) along the threat management process from prevention to incident troubleshooting and forensics, (3) in verticals to address industry-specific challenges.

The market has become all the more fragmented since entry barriers, especially in the cybersecurity services segment, are low enough to allow the emergence of new incoming players.

The European ecosystem's diversity duly reflects the richness of a mosaic of technological expertise and ambitions.

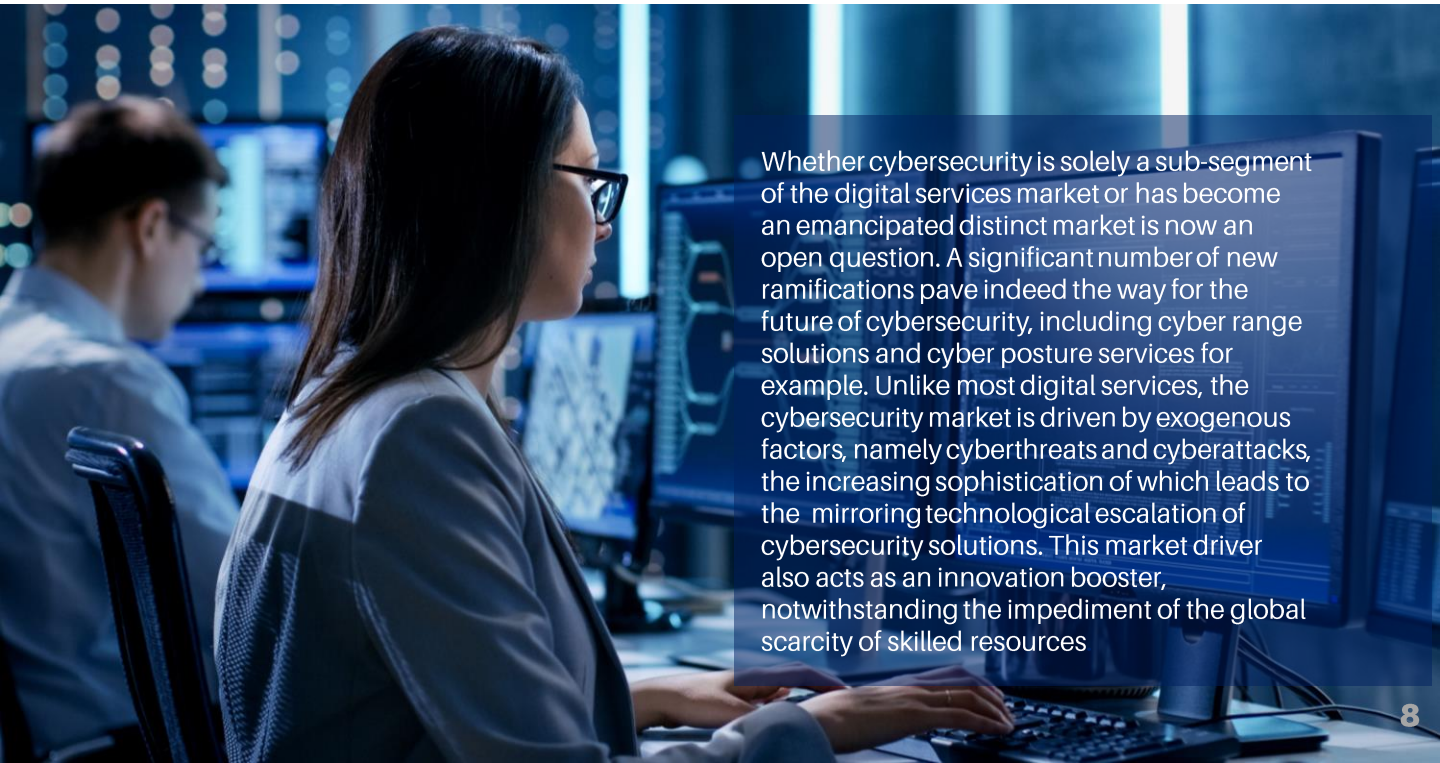
Where does value reside in?

Cybersecurity is far more than the promise to be one of the next big things in tech markets.

Cybersecurity is probably the industry that expresses today the best customer value proposition coming from a business model that combines SaaS solutions with services, relative to other tech industries, (as well as healthcare and medtech).

As a response to cybercrime's increasing sophistication, the cybersecurity industry relies on edge technologies & competencies to secure the building and development of general purpose technologies (cloud, IoT, 5G) and their far-reaching applications.

Besides, the value of cybersecurity companies mainly resides in the value protection they offer to their end customers, which face a continuous flow of costly and painful cyber threats. Most advanced players in the industry provide their customers with a comprehensive cybershield system, a key pillar of their defensive strategy to secure their digital and data assets. To a certain extent, the same logic applies to the B2C market.



Whether cybersecurity is solely a sub-segment of the digital services market or has become an emancipated distinct market is now an open question. A significant number of new ramifications pave indeed the way for the future of cybersecurity, including cyber range solutions and cyber posture services for example. Unlike most digital services, the cybersecurity market is driven by exogenous factors, namely cyberthreats and cyberattacks, the increasing sophistication of which leads to the mirroring technological escalation of cybersecurity solutions. This market driver also acts as an innovation booster, notwithstanding the impediment of the global scarcity of skilled resources

Deciphering the market

C1. The cybersecurity IT/OT value chain

C2. The cybersecurity services value chain

Source: from Cybersecurity Observatory, 2020

C3. Non-exhaustive list of trending cybersecurity businesses

- Training, education & awareness
- Network security
- Cloud security
- IoT & IioT
- Cyber threat intelligence
- Cyber range
- Governance & compliance
- Web security
- Endpoint security
- Mobile security

- Identity Access Management (IAM)
- Fraud
- Data security
- App security
- Detection & prevention
- Security Operations Centers (SOCs)
- Email security
- Cyber posture
- Incident response & forensics
- AI security

Main industry challenges

As a preamble to this section, rising cybercrime is obviously a permanent challenge specific to the industry that will on purpose not be addressed here.

Accelerating European cooperation

The Covid-19 crises have highlighted the importance of cybersecurity to such an extent that EU initiatives have been accelerating to reinforce European digital autonomy.

Cybersecurity is a significant support to European economic recovery, thanks to its strong market growth, its role as a digital transformation accelerator, and as business enabler for key technologies and apps (industry 4.0, ADAS…).

Odyssey brings its best encouragements to the recommendations lately disclosed by the ECSO to make cybersecurity pivotal in European undertakings to regain digital and cyber *autonomy*. By the way, European cyber *sovereignty* is nothing more than a mère illusion for now, as the presence of foreign tech giants, mainly from the US, continues to expand across European countries. Reducing regional dependency to these players would already be a giant leapfrog on the road to increased autonomy.

Fueling the growth of innovative cybersecurity companies through appropriate funding amounts & schemes is necessary to enable scale-up companies to emerge.

At least three layers of European coordination are needed to develop the regional cybersecurity fabric : (i) among EU States, governments, and local authorities, (ii) among companies in different countries, for example on joint cybersecurity projects, and (iii) public and private coordination.

The consistency between European policies, political guidelines and effective business practices in the public sector has to be improved. Indeed, non-EU cybersecurity suppliers continue too often to gain public contracts, strengthening thus the European dependency to foreign digital powers.

The Gaia-X initiative, launched in June 2020 to enable the creation of a federated cloud and data infrastructure for Europe, is the absolute epitome of a successful European public and private (OVHCloud, Amadeus, Atos…) cooperation in the cyberspace.

Seizing the Brexit opportunity

On 31 Dec 2020, the Brexit transition process will come to an end. The application of the adequacy principle for EU companies may be quite challenging. Nonetheless, the Brexit is not only factor of complexity but also a driver for opportunities for both UK-based and EU-based cybersecurity experts. The UK&I digital autonomy has indeed to be reinforced, in compliance with the new local framework (UK DPA) while maintaining some necerssary digital bridges with the EU ecosystem.

Main industry challenges

Tackling the global skills shortage

The shortage in cybersecurity skills is a global market concern that serously affects but is not limited to Europe and UK&I.

The main levers to solve this hindering issue are (i) security processes automation, and (ii) massive investments in training. The path to the automation of certain tasks along the value chain is inexorable, and might at the end of the day favour the most capex intensive cybersecurity companies as the main outcome of a Darwinian-like process.

Reskilling digital services consultants into cybersecurity experts may nonetheless result in uncertain ROI. Cybersecurity training for executives is a fast-growing niche that contributes to spread best security practices across organizations. Most importantly, the continuous development of educational programs in cybersecurity seems necessary, although requiring adequate funding, to actually supply an unambiguously dry market with talented youngsters.

External growth strategy is more than a valid option to increase a pool of skilled resources,and solve at a single organization level the growth limitations conundrum consecutive to the scarcity of resources.

Scaling-up

The European cybersecurity market is mainly comprised of (i) divisions of multinational digital services behemoths (>1bn€ revenue), such as Atos, Cap Gemini or Thalès, and (ii) small niche players, e.g innovative startups or tech-focused SMEs.

The void inbetween shows a blatant lack of midsized players that is highly noticeable in most European countries. Sophos (UK), with a € 710m revenue, and even F-Secure (Finland), with a € 219m revenue in 2019 are sort of market anomalies.

To complement European policies and public initiatives, the future role of PE firms investing in cybersecurity SMEs, and of VC firms investing in Series B to D funding rounds of innovative security startups, will be decisive in the Europe and UK&I ecosystems' capacity to scale-up and correctly address regional security challenges. Fueling financially the ecosystems is a prerequisite to the emergence of unicorns, and hopefully decacorns, aiming at portecting EU and UK&I data, infrastructure, and strategic applications.

Encouraging green cybersecurity

As global green and decarbonation strategies are currently implemented by large industry players, it's worth noticing that the combination of security and green IT would prove virtuous for the whole ecosystem. These emerging practices, such as lowered power consumption, may become mainstream in the coming months to make cybersecurity more sustainable, in consistency with other « tech for good » iniatives.

Cybersecurity companies must also think about investing sustainably in innovation to design the industry future and improve their positioning in a fast-evolving market. Innovation requires time, financial dry powder, and management attention on long-term strategic objectives, three conditions which are not that frequently met in 2020.

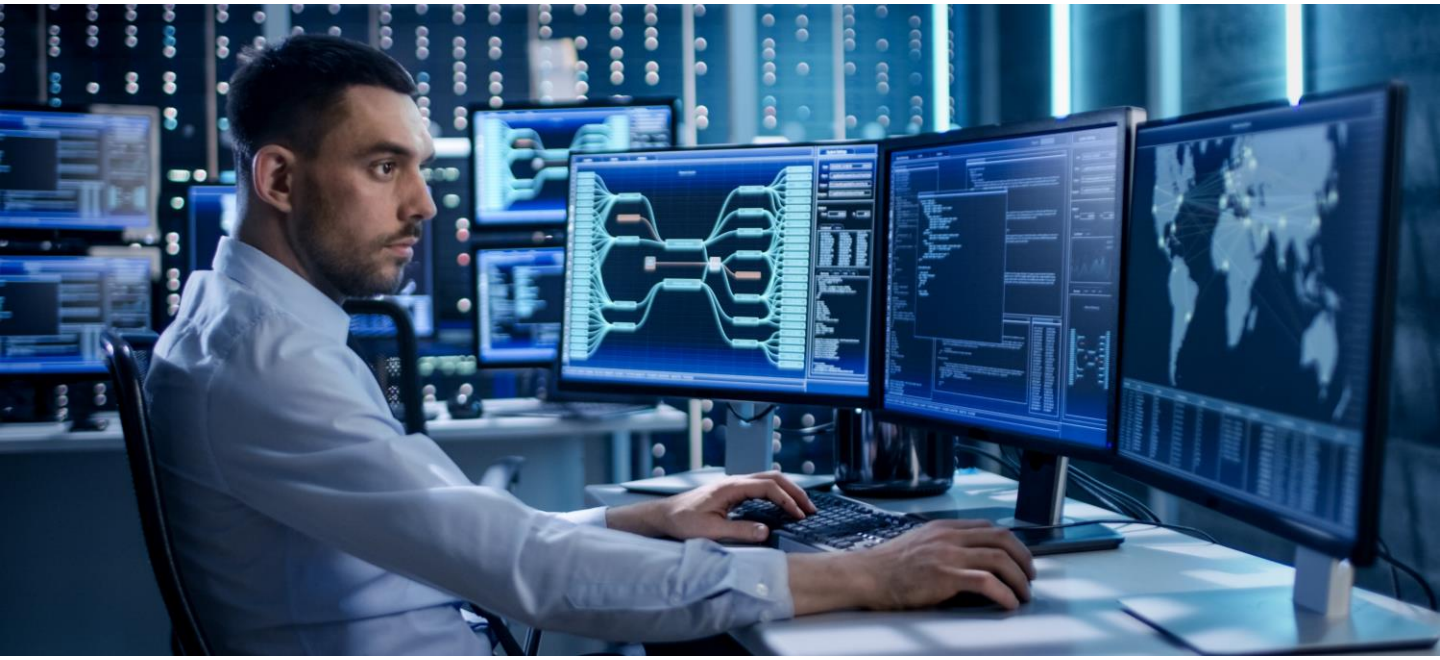
B1. Global shortage of cybersecurity resources

Source: ESG & ISSA, 2019

3.5m Nb of unfilled cybersecurity positions

0% Estimated industry unemployment rate

Ahead of the curve



Recovering from the shockwave and moving to a double-digit market growth

Despite the current impact of Covid-19, the market still relies on solid foundations for the future. There is little doubt the shockwave will gradually be absorbed by the fast-growing cybersecurity industry. The main outcomes of our meta-research, which is based on aggregated existing surveys* are the following:

1 **Uncertainty prevails** and becomes a constant feature in the market. As a consequence, market volatility is expected to remain significant whatever the scenario. Cybersecurity is a rather anti-fragile market as per Nassim Nicholas Taleb's definition, since it is reinforced by the occurrence of adverse events such as cybercrime. Market fluctuations are though exposed to VUCA environments.

8.4%
2020-25 CAGR

2 In terms of development stage, cybersecurity is **still an emerging market** that offers strong growth potential, despite accumulated years of existence. The needle may move from the «emerging » to an **accelerated « expansion » phase** within a couple of years, provided that all necessary conditions be met. The absence of a cybersecurity app fatigue at SMEs level is one clue, among others, that actual maturity has not been reached yet.

3 Market growth forecasts are expected to be capped at ca. **6.5% in 2020 and 7.5% 2021**, and perhaps beyond, but not in a central case scenario. On average, cybsecurity products and solutions may rise at up to 7%, while cybsecurity services may increase by up to 8% per annum over the next 18 months, with strong variations depending on categories of offerings, and subject to future Covid-19 impact.

4 The market may come back to a pre-Covid **standard growth rate of ca. 12% per year** as soon as 2022 in the central case, potentially one year later depending on the Covid-19 crisis exit scenario. The security products & solutions market segment might renew with a double-digit growth on average from 2022 to 2025. The security services may increase by up to15% per year pver the period.

5 **The 2020-2025 CAGR might reach 8.4%** on average, assuming a gradual smoothing of the long-term effect of Covid-19. Cybersecurity products and solutions shall face a slightly lower growth pace relative to cybersecurity services. Such a discrepancy was already acknowledged by the market, and is confirmed, if not sharpened, by the Covid-19 aftermath. Few other industries may offer such an attractive CAGR over the period.

*: including publicly available information from Gartner, Grand View Research, Mordor Intelligence, Markets & Markets

Ahead of the curve

Spotting the new areas for growth

A few emerging domains may constitute new drivers for higher growth over the next 3 to 5 years. Hereafter is a non exhaustive selection of forethoughts on trends and offerins that could unleash a strong potential.

Cyber range designates the preventive simulations of cyberattacks to orchestrate a defensive strategy, relying on virtual centers and skilled teams: attack management, IT/OT systems responses, assessments & improvements. The relevance of these preventive solutions is confirmed by soaring market fit. More generally, companies specializing in cyber threat intelligence solutions and predictive analytics may acknowledge accelerated growth.

Cybersecurity training, certification, and rating businesses may benefit from both favorable regulations and augmented awareness. Training of 3rd party IT & non-IT employees on cybersecurity practices is obviously a major trend. In 2019, the EU Cybersecurity Act introduced a cybersecurity certification framework for products, processes and services with the ambition to identify trusted EU providers and drastically reduce the harmful impact of fraudulent and low-end quality cybersecurity services on organizations. New golden nuggets may emerge soon in that sub-segment.

Security Operations Centres (SOC) play a key role in business continuity plans to protect infrastructure and applications. Nevertheless, the implementation of SOCs by SMEs is limited by the 3Cs: cost, complexity & c-level commitment. A call for agile, hybrid, cost-efficient, **green and predictive SOCs** offering bespoke services to customers could energize a market dominated by reactive centres.

Innovative companies that help protect sensors and new connected devices, basically endpoints, mobile and IoT cybersecurity, may welcome a soar in revenue, mainly due to the unprecedented rise in the number of connected devices (50 to 100 billion in 2025 globally) and 5G implementation.

Vertical specialization is a key emerging trend. Defence & public sector, banking, healthcare, telecom and digital, automotive and retail are currently the main end-markets for cybersecurity. Utilities, renewable energies and greentech are undoubtedly an upcoming outlet not to be overlooked.

Last but not least, **cybersecurity posture** consulting may offer long-term value protection to customers, despite some growth limitations in the short-term that flow directly from the cybersecurity paradox. **Cyberstrategy and cybersecurity orchestration services** may increasingly become part of the competitive landscape as large customers require a consistent approach to cyber risks across various divisions and geographies.

Convergence & partnerships strategies

Convergence and partnership strategies are also an effective method to differentiate in the fragmented European market.

While **partnerships with technology companies** remain relevant to legitimate and officially disclose an expertise (e.g Microsoft Azure), **the convergence of telco operators and cybersecurity providers** is becoming vital to combine appropriate skills to duly secure critical infrastructures.

Another example is the **powerful combination of user behavour analytics (UEBA) security competencies with fraud prevention & management expertise.** These two industries are indeed closely tied, as 86% of cyberattacks are driven by financial purpose.

As a conclusion, cybersecurity enters a new era of hyper-specialization that is a positive signal for increased security across the EU and UK&I region, and also for numerous innovation and consolidation opportunities.

Investor highlights

Despite the Covid-19 context, the cybersecurity market continues to attract premium valuations from European and US-based PE firms, VC sponsors, and strategic buyers envisioning lucrative synergies.

Two types of opportunities still prevail in the cybersecurity sector: (i) add-on acquisitions and (ii) take-privates, to a lesser extent.

Buy & build

Most transactions in the cybersecurity space have lately been add-on acquisitions as the race to critical size is definitely on, consistently with what has been for long the norm in the global digital services market. Build-up stragegies that focus on highly selected tuck-in acquisitions are a legitimate answer to the lack of midsized targets and sometimes of organic growth potential, restrained by the scarcity of resources.

Strategic buyers are expected to actively participate in the upcoming consolidation wave. Large multinational providers of digital services foresee cybersecurity as a major driver for growth relative to standard growth rates in other digital services. In such a case, one major challenge is to successfully implement extensive revenue synergies that compensate for the valuation gap between cybersecurity and other digital services.

Take-privates

In H1 202, the most iconic transaction in the region was certainly the acquisition of the UK-based B2B and B2C cybersecurity provider Sophos by Thoma Bravo, a US-based PE firm, for € 3.3 bn in a take-private deal. The number of other similar opportunities seems so limited that Sophos was likely an exception.

Fueling innovation

As described in previous sections, fueling cybersecurity innovation is quite a stake for Europe and UK&I.

Venture capital activity in cybersecurity may remain intense given the permanent creation of innovative startups across the European ecosystem.

The recent VC paradigm shift from skyrocketing growth promises to a refocus on seasoned management teams, cash burn rates, and time-to-breakeven may offer interesting outlook to cybersecurity services providers. The already vital importance of customer churn rate is reinforced for cybersecurity SaaS platforms.

Valuations & Exits

The adverse Covid-19 impact on valuations in cybersecurity has been low to moderate so far.

With strong variations depending on specializations and geographies, recent transactions in the industry rely on average on a 15x to 20x EV/EBITDA multiple, and final considerations could exceed that range.

In the VC market, the growing for interest for security may put the industry under the limelight rather soon . Competitive processes would undoubtedly trigger a rise in startups valuations, especially in Series A to D rounds.

Private equity firms face multiple challenges such as denominator effect, rising capital calls, liquidity squeeze in these unprecedented times. Exit is therefore a general concern, which has to be nuanced here by (i) strategic buyers' appetite and cash available, and (ii) massive public & private stimuli, as cybersecurity becomes a strategic priority within the EU and UK&I regions.

ODYSSEY

Odyssey.tech
128, rue La Boétie 75008 Paris
hello@odyssey.tech
Tel: +33 1 82 28 00 60