STIFEL | IRIS

INTELLIGENCE • RESEARCH • INSIGHTS • SERVICE

CYBERSECURITY

Investor Playbook

CONTENT

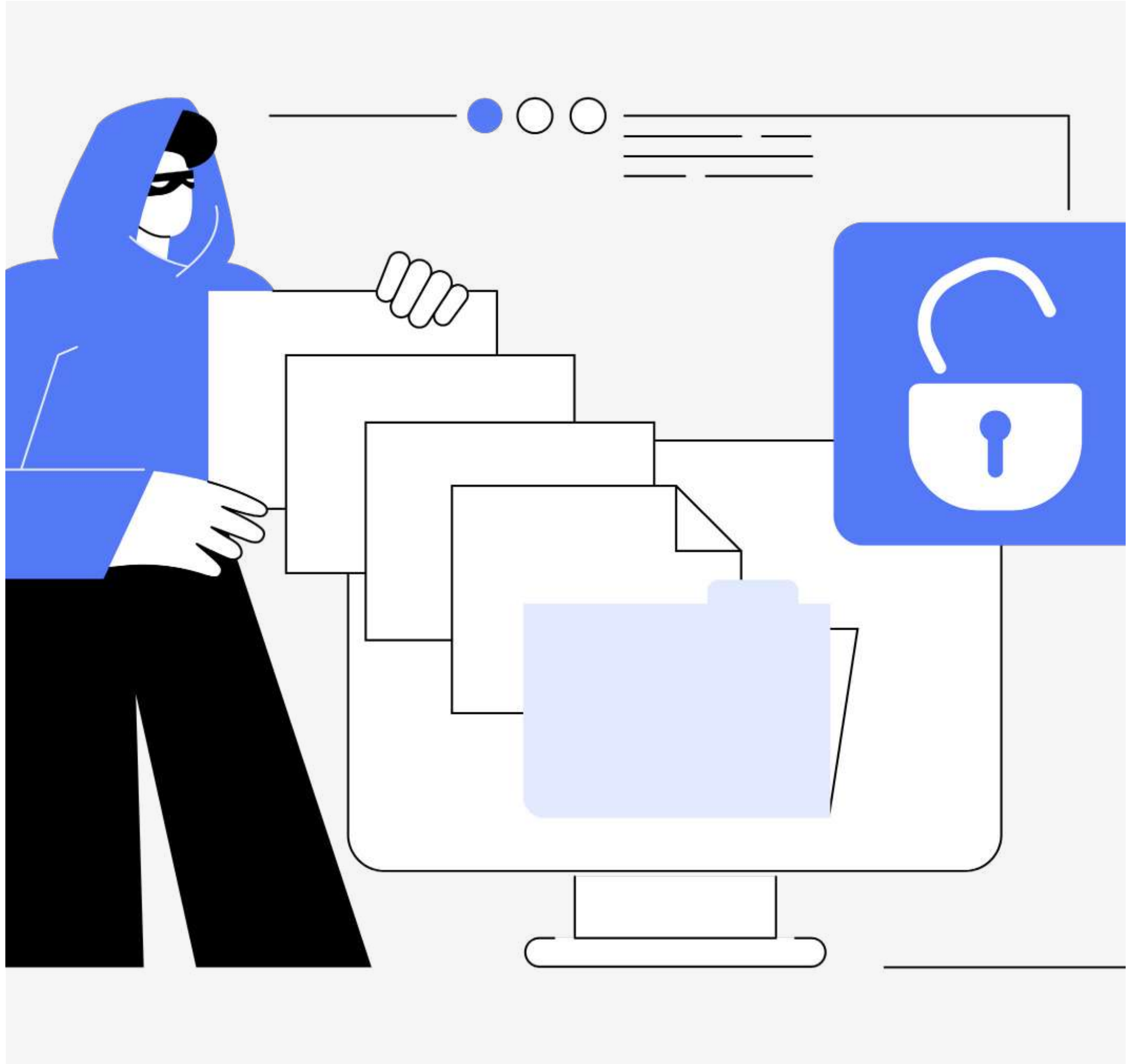
From blockbuster public infrastructure hacks to local SME data breaches, the risk of cyberattacks concerns all organisations, large or small, public or private. On the one hand, cyberattacks are becoming increasingly sophisticated and can be deployed on a global scale within minutes if not seconds. On the other hand, the stakes are high for victims. Indeed, in a digitalising economy, the quantity and value of data produced is increasing at a fast pace, while data and the information technology (IT) stack has become mission-critical for most businesses. Furthermore, constant innovation on the attackers' side and cyber staff shortages on the organisation side make the challenges posed by cybersecurity all the tougher.

While these risks have been known for decades, organisations are still not doing enough to prevent them. On some estimates, the value lost to cyberattacks exceeds the costs spent on preventing them by three to five times. Although measuring attackers' revenue is a complex task by design, the imbalance between risks and costs clearly supports the case for purchasing more cybersecurity tools and constitutes a huge catalyst for the cybersecurity sector as a whole.

As such, we believe the cybersecurity market has all it needs to thrive in a digitalising economy and should continue to grow at a double-digit rate. Nevertheless, finding winners in a rapidly evolving environment can be challenging. We therefore propose a framework of analysis to identify emerging players in the cybersecurity market to help investors navigate the rough seas of cybersecurity and take advantage of the five trends set to define the market in the coming years.

ATTACKERS **BREAD AND BUTTER**

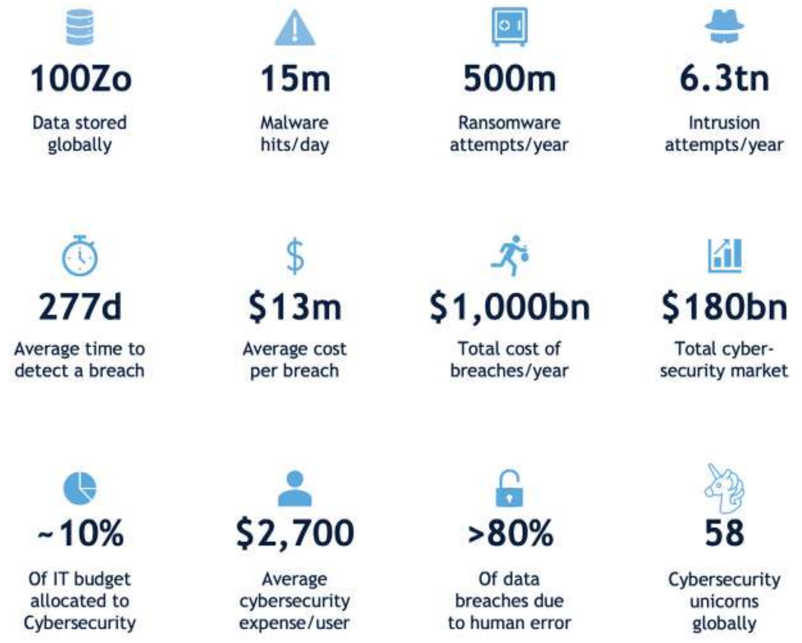
SECTION 1



This first section discusses the current backdrop in the cybersecurity industry. It provides general information about the sector and maps out the types of threats that exist, their perpetrators, and their associated costs. A few examples of landmark cybersecurity breaches are also presented at the end of the section.

The state of cybersecurity

FIG 1: THE STATE OF CYBERSECURITY



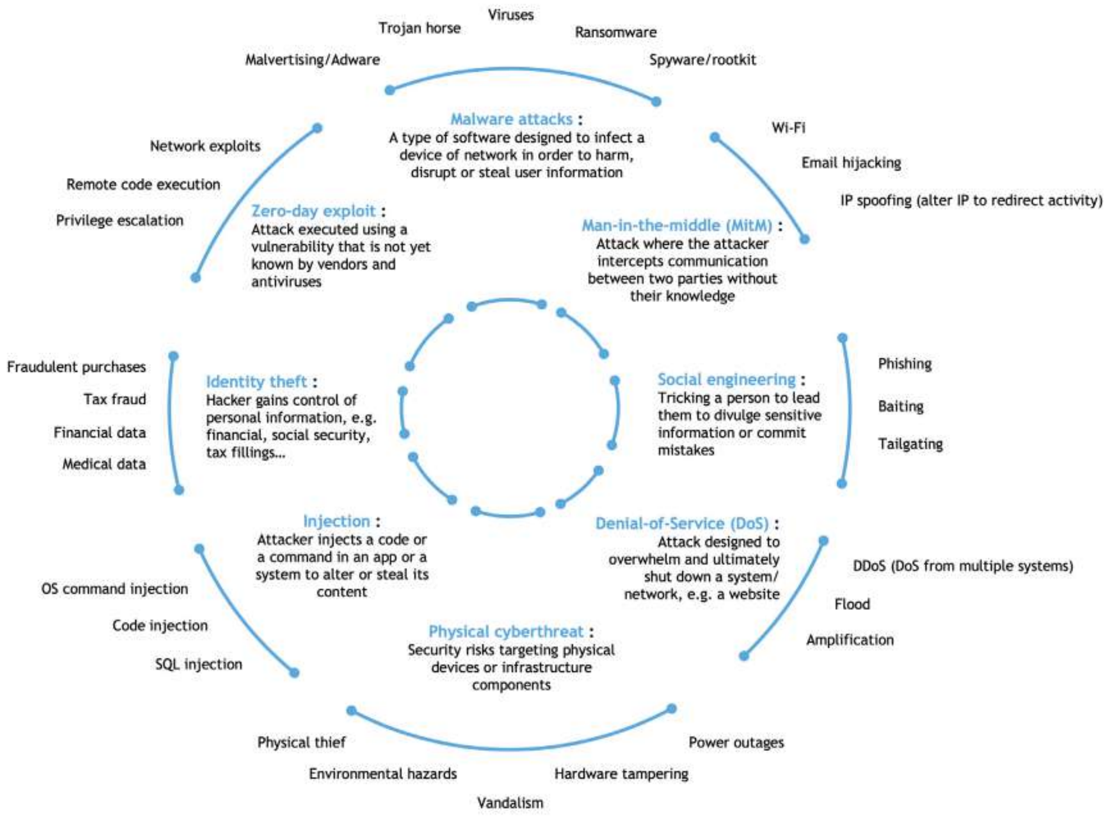
*Source: CBInsight, Deloitte; IBM, IDC; SonicWall; Stifel**

Finding reliable statistics on cybercrime is no easy task. Estimates can vary widely from one source to another, but we intend to display only the data points that match our understanding of the market reality.

Beyond malware

To understand the five trends driving the cybersecurity industry, an analysis ofthe complex and evolving nature of cyber threats is necessary. The threats go well beyond viruses and ransomware - they come in many shapes and colours and can be perpetrated by a wide range of attackers. The following chart sets out key types of threats. While some are basic like flooding a server with request stuffing, others require a much more complex organisation like social engineering.

FIG 2: BEYOND MALWARE


Trojan horse
Viruses
Ransomware
Malvertising/Adware
Spyware/rootkit
Malware attacks : A type of software designed to infect a device of network in order to harm, disrupt or steal user information
Network exploits
Remote code execution
Privilege escalation
Zero-day exploit : Attack executed using a vulnerability that is not yet known by vendors and antiviruses
Wi-Fi
Email hijacking
IP spoofing (alter IP to redirect activity)
Man-in-the-middle (MitM) : Attack where the attacker intercepts communication between two parties without their knowledge
Fraudulent purchases
Tax fraud
Financial data
Medical data
Identity theft : Hacker gains control of personal information, e.g. financial, social security, tax fillings...
Phishing
Baiting
Tailgating
Social engineering : Tricking a person to lead them to divulge sensitive information or commit mistakes
Injection : Attacker injects a code or a command in an app or a system to alter or steal its content
OS command injection
Code injection
SQL injection
Denial-of-Service (DoS) : Attack designed to overwhelm and ultimately shut down a system/ network, e.g. a website
DDoS (DoS from multiple systems)
Flood
Amplification
Physical cyberthreat : Security risks targeting physical devices or infrastructure components
Physical thief
Power outages
Environmental hazards
Hardware tampering
Vandalism

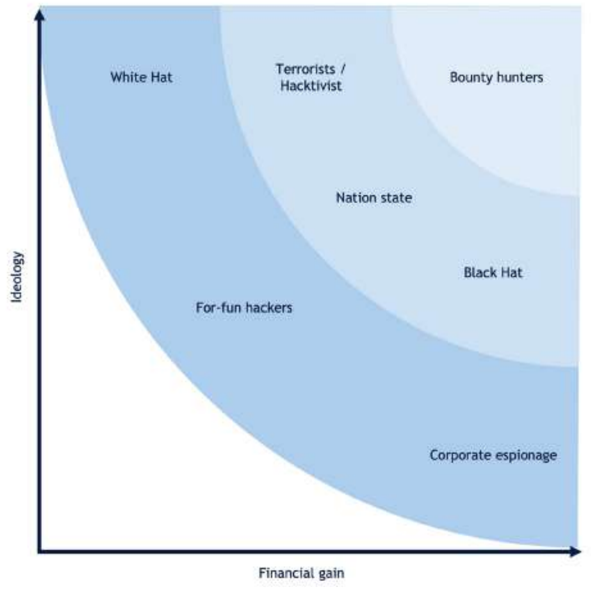
*Source: Stifel**

For each type of attack, cybersecurity organisations need to develop adequate protection and this landscape is widening on a daily basis. As the economy becomes more and more connected, the need for protection widens, and for every new solution, attackers will seek any vulnerability, meaning that threats evolve at a very high pace.

A diverse community

In the same way that we generally do not appreciate the full extent of cyber threats in themselves, we also underestimate the vastness of cyber attacker backgrounds. We have mapped them according to two types of motivation: financial gains and ideological incentive.

FIG 3: MOTIVATION-BASED HACKERS MAP



*Source: Stifel**

- Black hat hackers: typical attackers generally thought of, they operate for financial profit and work alone or in groups.

- For-fun hackers: these operate mostly for entertainment purposes, most often individually or in small groups, seeking neither financial compensation nor following ideologic agenda.

- White hats: operate for a specific ideological motive that they consider right, political, religious, or simply fighting black hats and criminals of all sorts.

- Bounty hunters: some organisations offer financial rewards (bug bounty) for hackers who will find security vulnerabilities in their websites, apps, systems, etc, in order to patch them before black hats spot them too. Some companies even specialise in this form of hacking as a service, like HackerOne, Ethiack or Intigriti for example.

- Terrorist or hacktivist groups operate for religious or political ideologies in order to spread fear, propagate their message and fight their opponents.

- Nation states: government-backed organisations hacking rival public instances or organisations either to weaken their adversaries, steal their information, or spy on them. In these cases, governments impersonate black hat attackers to mask their identity.

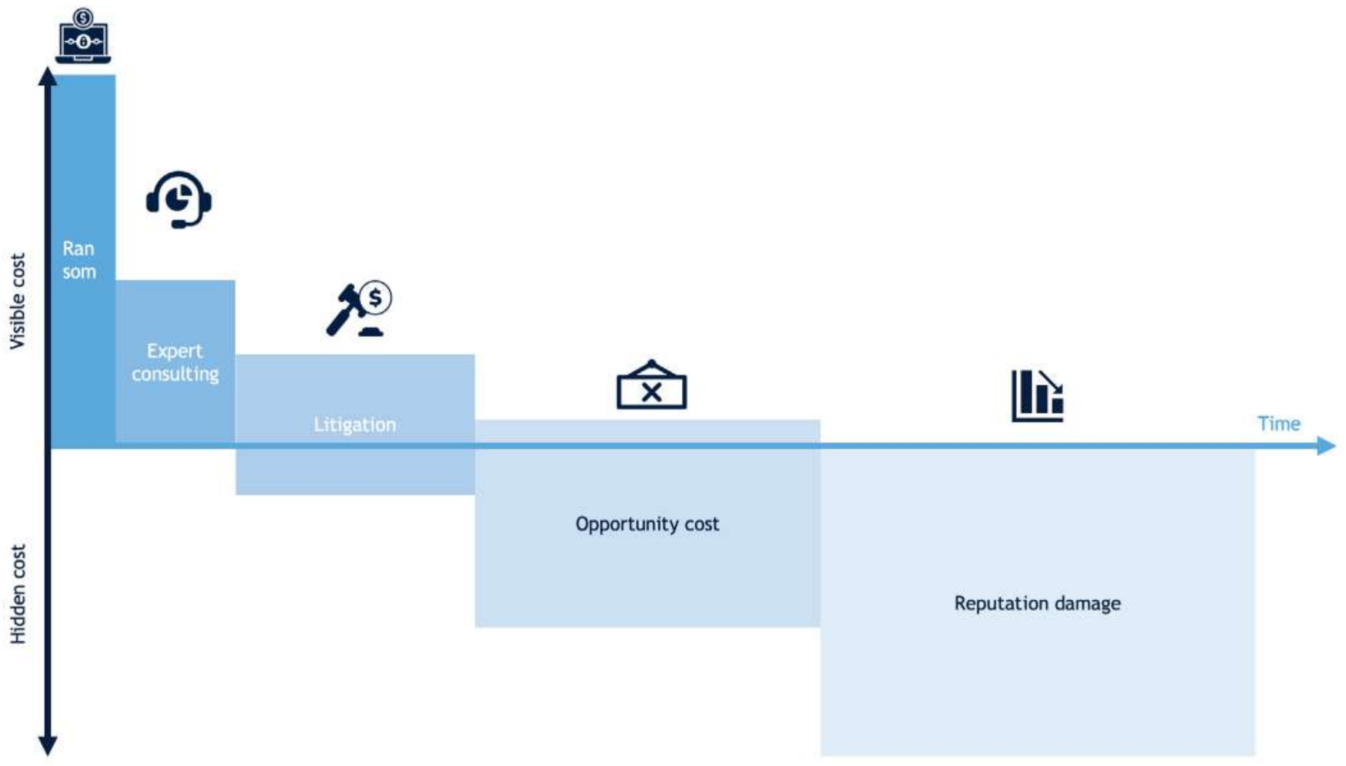
- Corporate espionage: some companies might resort to hacking in order to steal valuable information from their competitors or try to cause them harm.

Note that some (if not most) cyber threats come directly from insiders within the organisation being hacked, e.g. an employee selling, information to other organisations, or leaking, destroying or altering it. Cyberthreats are therefore not always perpetrated by a remote group of unknown attackers.

Hidden costs

Once an organisation is hacked, the cost does not stop at the ransom payment (if it chooses to pay it, although paying ransoms is banned in many jurisdictions). In reality, there are many costs associated with cyber breach, as summarised below. The key message is that the most visible part of costs related to a cybersecurity breach are only a fraction of the total, and the costs of lost business can be way more painful than the ransom itself.

FIG 4: CYBERATTACK-RELATED COST BREAKDOWN



*Source: Stifel**

- Ransom: in the case of a ransomware attack, the first and most visible cost is obviously the ransom itself. Note that payment of a ransom neither guarantees the stolen data will be returned, nor does it prevent the attacker from asking for a second ransom payment.

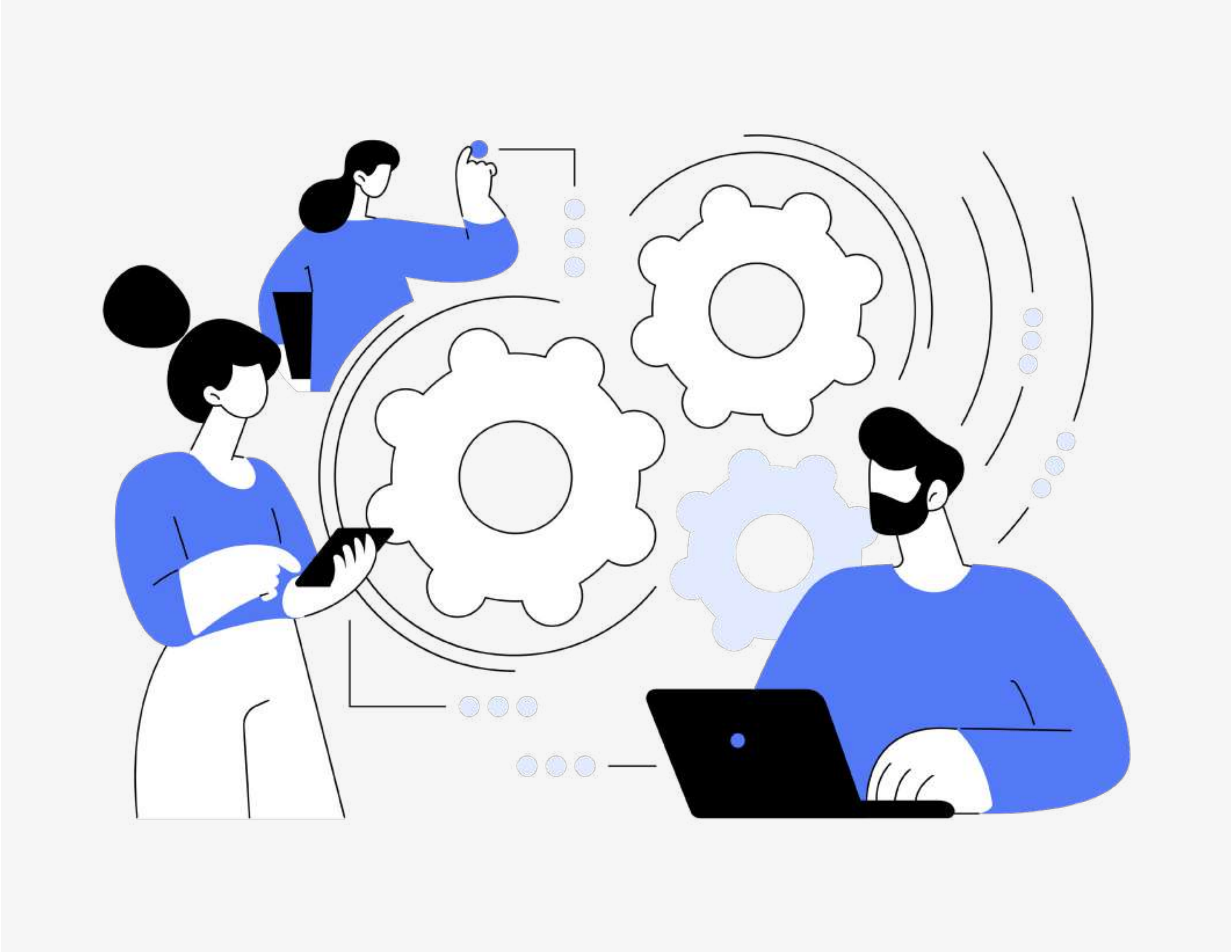
- Consulting: a targeted organisation will most often need experts to solve the breach and repair its effects and put the right system in place to prevent further attacks.

- Litigation: stakeholders affected by a hack caused by the company's negligence often seek compensation. The latter potentially triggers litigation and compensation expenses and sometimes fine payments.

- Opportunity cost: when a website or factory is out of service due to a cyberattack, it generates no income, thereby representing a missed opportunity.

- Reputation damage: stakeholders losing trust in an organisation's cybersecurity system tend to steer clear from it to avoid being affected by their security issues. This reputation risk damages the victim's business in the long run, and is typically the reason why some victims chose to pay a ransom to avoid any bad rap.

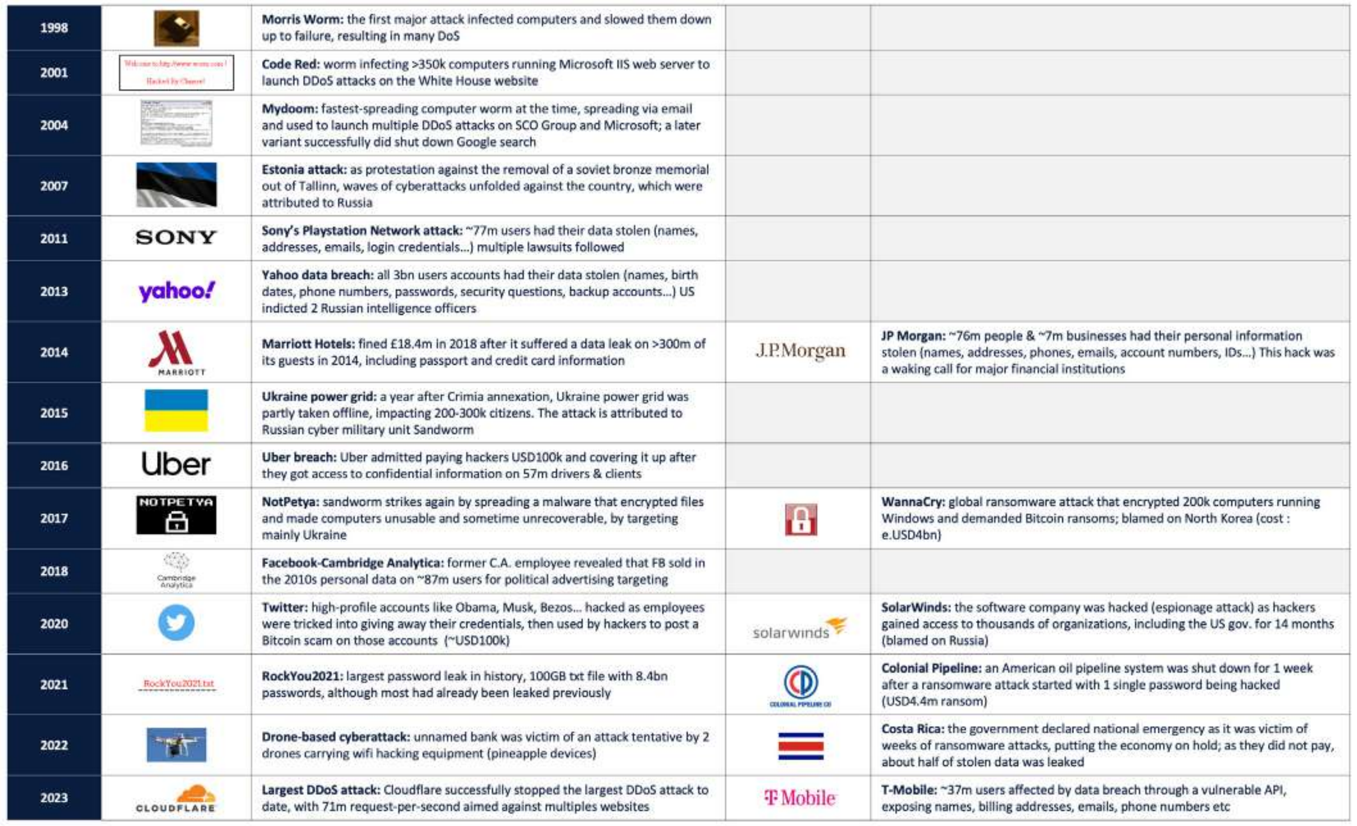
Through these elements, it is clear a cyberattack can have lasting effects on a business, even after the eventual one-off financial ransom is paid.



A rich history of cyberattacks

Previous cyberattacks leave clues for the future: a game of cat and mouse

FIG 5: A WALK DOWN THE MEMORY LANE

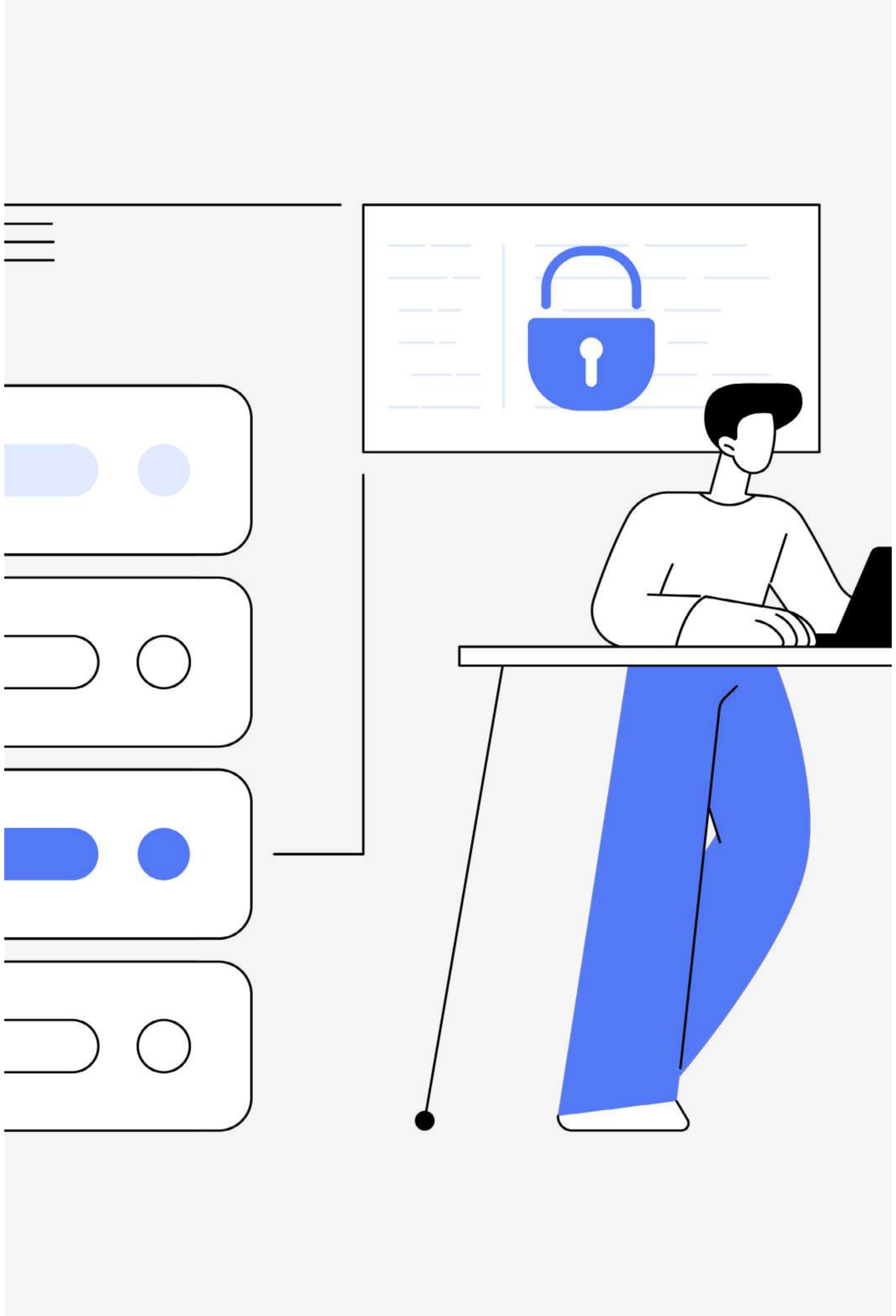


1998		**Morris Worm:** the first major attack infected computers and slowed them down up to failure, resulting in many DoS		
2001	Welcome to http://www.worm.com ! Hacked by Chinese!	**Code Red:** worm infecting >350k computers running Microsoft IIS web server to launch DDoS attacks on the White House website		
2004		**Mydoom:** fastest-spreading computer worm at the time, spreading via email and used to launch multiple DDoS attacks on SCO Group and Microsoft; a later variant successfully did shut down Google search		
2007		**Estonia attack:** as protestation against the removal of a soviet bronze memorial out of Tallinn, waves of cyberattacks unfolded against the country, which were attributed to Russia		
2011	SONY	**Sony's Playstation Network attack:** ~77m users had their data stolen (names, addresses, emails, login credentials...) multiple lawsuits followed		
2013	yahoo!	**Yahoo data breach:** all 3bn users accounts had their data stolen (names, birth dates, phone numbers, passwords, security questions, backup accounts...) US indicted 2 Russian intelligence officers		
2014	MARRIOTT	**Marriott Hotels:** fined £18.4m in 2018 after it suffered a data leak on >300m of its guests in 2014, including passport and credit card information	J.P.Morgan	**JP Morgan:** ~76m people & ~7m businesses had their personal information stolen (names, addresses, phones, emails, account numbers, IDs...) This hack was a waking call for major financial institutions
2015		**Ukraine power grid:** a year after Crimia annexation, Ukraine power grid was partly taken offline, impacting 200-300k citizens. The attack is attributed to Russian cyber military unit Sandworm		
2016	Uber	**Uber breach:** Uber admitted paying hackers USD100k and covering it up after they got access to confidential information on 57m drivers & clients		
2017	NOTPETYA	**NotPetya:** sandworm strikes again by spreading a malware that encrypted files and made computers unusable and sometime unrecoverable, by targeting mainly Ukraine		**WannaCry:** global ransomware attack that encrypted 200k computers running Windows and demanded Bitcoin ransoms; blamed on North Korea (cost : e.USD4bn)
2018	Cambridge Analytica	**Facebook-Cambridge Analytica:** former C.A. employee revealed that FB sold in the 2010s personal data on ~87m users for political advertising targeting		
2020		**Twitter:** high-profile accounts like Obama, Musk, Bezos... hacked as employees were tricked into giving away their credentials, then used by hackers to post a Bitcoin scam on those accounts (~USD100k)	solarwinds	**SolarWinds:** the software company was hacked (espionage attack) as hackers gained access to thousands of organizations, including the US gov. for 14 months (blamed on Russia)
2021	RockYou2021.txt	**RockYou2021:** largest password leak in history, 100GB txt file with 8.4bn passwords, although most had already been leaked previously	COLONIAL PIPELINE CO	**Colonial Pipeline:** an American oil pipeline system was shut down for 1 week after a ransomware attack started with 1 single password being hacked (USD4.4m ransom)
2022		**Drone-based cyberattack:** unnamed bank was victim of an attack tentative by 2 drones carrying wifi hacking equipment (pineapple devices)		**Costa Rica:** the government declared national emergency as it was victim of weeks of ransomware attacks, putting the economy on hold; as they did not pay, about half of stolen data was leaked
2023	CLOUDFLARE	**Largest DDoS attack:** Cloudflare successfully stopped the largest DDoS attack to date, with 71m request-per-second aimed against multiples websites	T Mobile	**T-Mobile:** ~37m users affected by data breach through a vulnerable API, exposing names, billing addresses, emails, phone numbers etc

*Source: Stifel**

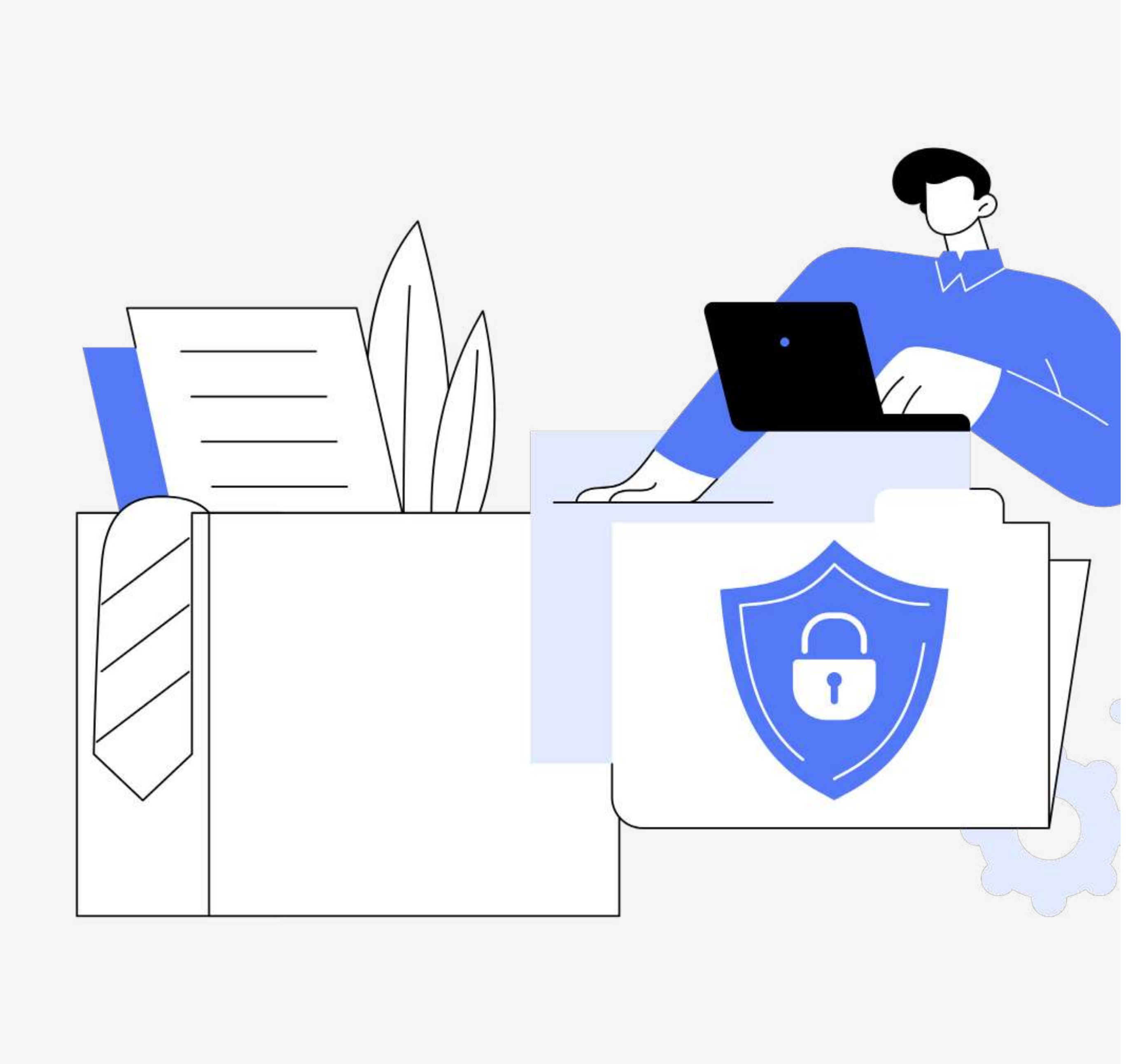
For as long as computers and networks have existed, people and organisations have tried to exploit their vulnerabilities either for personal gain or for larger goals and ideologies, and there is no slowdown in sight. We might think that with recent progress in technology we would be better at countering attacks but in reality, the number of cyberattacks increase year after year. It is unrealistic to think that technological innovations from cybersecurity solution providers will not be matched by attackers. Even ground-breaking solutions like quantum computing will ultimately be adopted by cyber criminals too. Artificial intelligence, for example, which when firstly implemented, revolutionised cybersecurity by spotting threats more effectively and faster thanks to its ability to apply judgement and to learn by itself, is starting to be implemented by attackers too. The future of cybersecurity is therefore very unlikely to deviate from its history, it will always centre around a «cat and mouse» game whereby attackers find new vulnerabilities, which are quickly patched by new updates, until the next ones are found.

The spread of generative Artificial Intelligence (AI) tools such as ChatGPT saw an immediate adoption among attackers. The program is used to make more convincing phishing emails, thanks to its ability to generate a person's voice from previous recordings (Youtube, Interviews...) and say any text that could fool employees, banks or even family and friends. This shows how quickly innovations are adopted by attackers, in ways that could not be predicted by any cybersecurity vendor.



UNPACKING CYBERSECURITY

SECTION 2



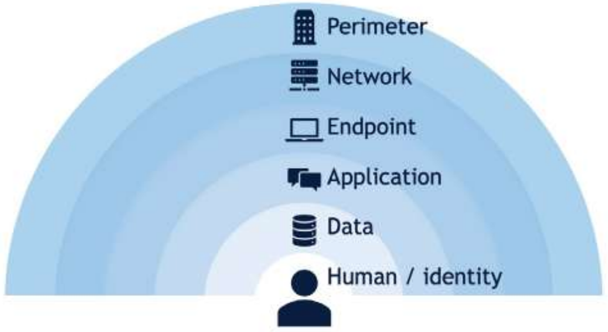
This section tackles the high level technical challenges of cybersecurity and identifies some important players in the sector in a mapping. When it comes to assessing the potential of a business, the key elements of our analysis framework are also provided in this section.

Defining the cyber perimeter or what needs to be protected

From an organisation's standpoint, the challenges of cybersecurity can be approached through two prisms: the type of attacks being perpetrated against an organisation and the attack surface exposed to potential threats. Defining the attack surface traces back to understanding what is the digital footprint of an organisation or outlining its Information Technology (IT) perimeter. Unfortunately, for Chief Information Security Officers (CISOs), the IT footprint is often a complex stack of layered assets and applications whose perimeter can be hard to grasp.

The following figure illustrates how the typical IT stack is organised:

FIG 6: THE IT STACK PERIMETER



*Source: Stifel**

- The outer layer represents the organisation perimeter, comprising every endpoint, application, data or participant that interacts within the organisation, and that can be monitored by it. In other words, the perimeter represents the IT boundaries of an institution.

- The network layer describes any subset of Local Area Network (LAN) or Private Area Network (PAN) that composes the outer perimeter. A LAN can encompass a local branch of a firm comprising thousands of endpoints as well as a two- device office.

- Endpoints describe all the devices connected to a network. Those include servers, desk computers, laptops, mobile phones, printers, cameras and so on. Note that endpoints are not necessarily physically connected to an organisation's network, they often access the network via external Internet providers.

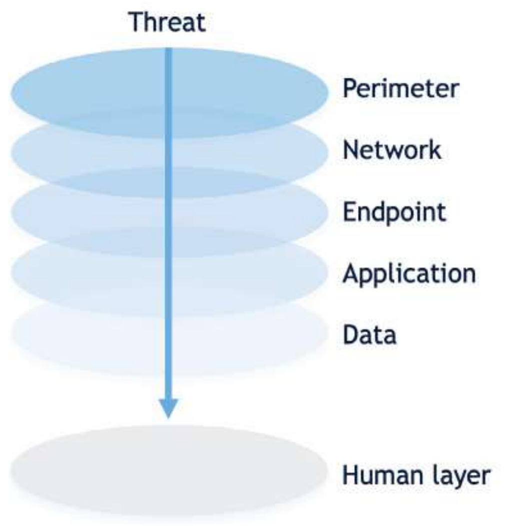
- The application layer encompasses the services that run on an institution's endpoints, whether being run on premise (own servers) or on the cloud (hosted by a third party).

- Data are the digital representation of the information being handheld by the organisations and its members.

- The human layer is basically the person accessing data, applications and networks within the organisation via an endpoint.

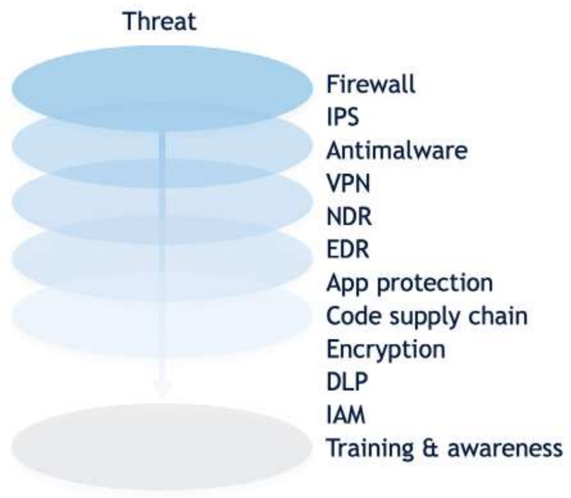
Of course the latter illustration is a simplified version of the complex reality: a company is rarely a standalone organisation sitting on a deserted island. Firms are connected with their staff, clients, suppliers and stakeholders through the Internet and are interdependent on each other, thereby blurring even more the definition of an organisation's perimeter. With the interconnections across businesses widening the attack surface, protecting the IT infrastructure is becoming increasingly challenging in the digital era. Organisations even struggle to determine the perimeter of their infrastructure as the popular 'bring you own device» policies and the recourse to unmonitored software or applications increase their shadow IT footprint.

FIG 7: STACKED LAYERS FILTER FOR POTENTIAL THREATS



*Source: Stifel**

FIG 8: STACKED CYBERSECURITY SOLUTIONS



*Source: Stifel**

A direct consequence of the stratified nature of the IT infrastructure is the need to protect every single layer with a specific software, tool or procedure. As such, several types of protective solutions have emerged 1) as a response to the innovations in cyberthreats, and 2) progressively moving from perimeter protection to more advanced preventive and response tools tailored to secure the inner (and more complex) layers of the IT stack: data and human vulnerabilities.

While there are dozens of cybersecurity tools available on the market, we will only describe the ones we consider to be the most important. We also acknowledge that one solution can protect several layers simultaneously.

Perimeter security:

- Firewalls act as a gateway to a perimeter by allowing or denying traffic based on its source and destination. They prevent malicious traffic based on its signature.

- Intrusion Prevention systems (IPS) work on the same logic as firewalls, except that they enable or restrict traffic based on the basis of behaviour patterns rather than signature.

Network security:

- Anti-malware is a detection program that prevents malicious files from running on an endpoint and spreading on a network.

- Virtual Private Network (VPN) solutions encrypt traffic to make it unaccessible by third parties.

Endpoint security:

- Endpoint Detection and Response (EDR) is a type of software capable of identifying malicious files or activity based on signatures or user behaviour analytics. (see more details in the dedicated inset). This segment is one of the most dynamic of the cybersecurity market.

- Network Detection and Response basically offer the same solution, applied to an entire network.

Application security:

- Application-specific tools can be paired with other systems to protect specific business applications like emails, Microsoft Teams, Salesforce...

- Application protection can take many forms, whether in terms of the development, deployment or runtime stage.

- Code supply chain security encompass solutions aimed at securing code at any stage (from writing to execution) and detecting vulnerabilities within open-source libraries.

Data security:

- Encryption or tokenisation systems transform a piece of data into a set of non-intelligible characters that, in the event of a breach, prevent attackers from exploiting without decrypting it.

- Data Loss Prevention (DLP) systems identify sensitive data and block their leakage in case malicious behaviour is detected on the network.

Identity security:

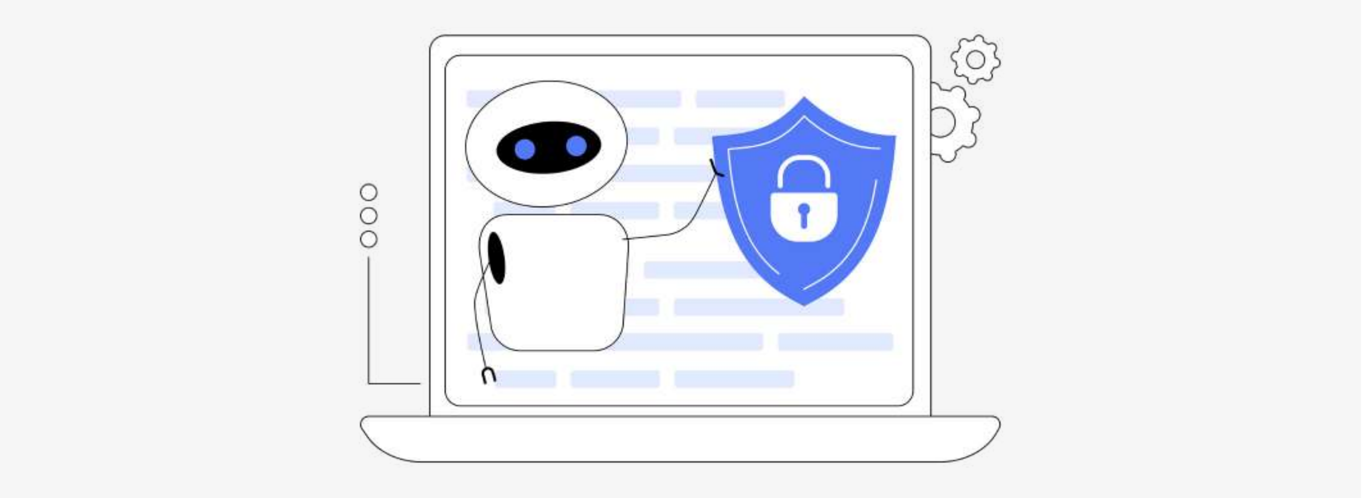
- Identity Access Management (IAM) tools enable an organisation to manage its users' digital identities (including login credentials and directory/file access management). This segment experienced significant consolidation in the recent years.

User security:

- Training and awareness is a set of services aimed at helping users to detect and circumvent potential threats. As most cybersecurity breaches come from human errors, this segment could attract some attention in the coming years.

Cloud security: the cloud is more a hosting and IT architecture choice than a specific layer of the IT stack. As such, most providers have tailored their solutions to fit with the specific requirements. We do not consider cloud cybersecurity as a market segment per se, but more as a sub-segment of those described above.

Mimicking their IT architecture, organisations tend to accumulate protection solutions from different vendors, rendering maintenance and visibility of the IT stack more cumbersome. As such, the attempt to secure IT perimeters sometimes results in counterproductive accumulations of specific software that usually work in a parallel manner rather than in a collaborative way. As a result, the scope of cybersecurity has long consisted of defending every single layer of the IT stack rather than securing the entire organisation. This complexity is a key driver in the development of cybersecurity platforms (described in a latter section).

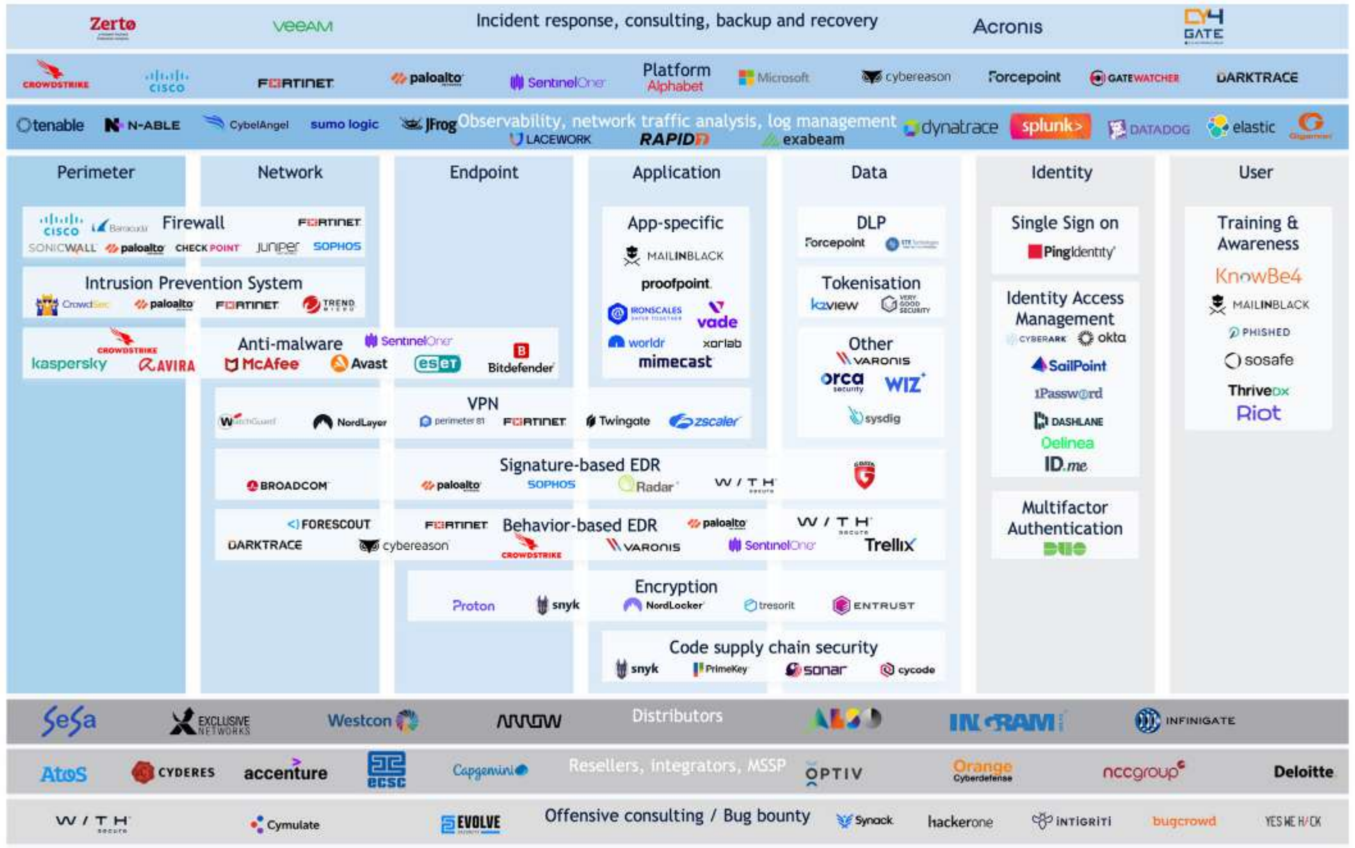


Market segmentation

As a result, the market for cybersecurity naturally segmented vendors according to the layer their solution intends to protect, resulting in acute competition among providers in each sub-category.

The following chart maps some key players of the cybersecurity industry according to the segment they address. We acknowledge many have wider reach than what is indicated on the chart, but for simplicity's sake, we have restricted the number of appearances of each vendor.

FIG 9: MARKET MAPPING BY SEGMENT



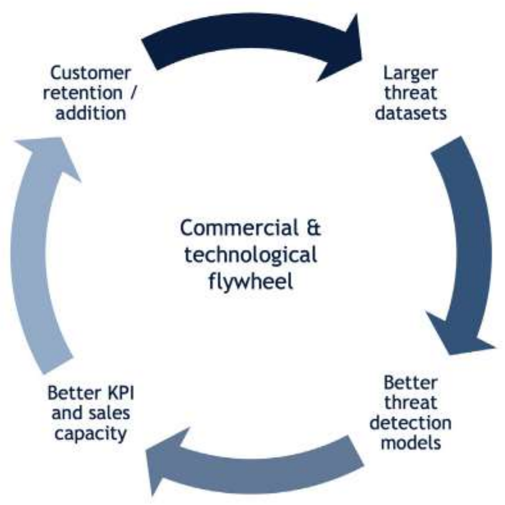
*Source: Stifel**

Thrive or die

As per the high degree of segmentation in the cybersecurity market, each category is faced with many incumbents offering similar technologies. Indeed, quickly after being discovered, a protection or detection technique becomes a new standard that competitors have to adopt or replicate to remain in the business. As such, one player's innovation attracts another's R&D spending, thereby swiftly spreading innovations in the sector.

This feature is particularly true as cybersecurity solutions are under permanent scrutiny from a performance standpoint. Indeed, the development of observability and log management tools provided CISOs access to a real-time vision of how IT and operating systems function. Therefore, any decline in cybersecurity solution effectiveness is immediately spotted, prompting customers to consider better-performing alternatives, quickly ejecting bad-rap solutions from the market. For this reason, R&D investments are of prime importance to keep up with competition in the field of cybersecurity.

FIG 10: THE COMMERCIAL AND TECHNOLOGICAL FLYWHEEL


Customer retention / addition
Larger threat datasets
Commercial & technological flywheel
Better threat detection models
Better KPI and sales capacity

*Source: Stifel**

As for most digital businesses, data is the crux of the cybersecurity industry. New generation behaviour-based EDR software is becoming more effective as the dataset against which their AI/ML models are trained becomes larger. As a consequence, the commercial success of a solution is often ultimately correlated with a firms' capacity to attract and retain customers. For this reason, even marginal improvements in customer retention or acquisition can be determining factors to maintain a competitive scale. As such, the importance of brand image, distribution channelsand sales and marketing efforts should not be ignored when assessing a cybersecurity vendor's capacity to thrive. We label this feedback loop as the 'commercial and technological flywheel'.

So, who's thriving and who's dying? We believe firms that are most efficient in allocating their R&D and S&M resources should experience the benefits of the commercial and technological flywheel while players underinvesting and misallocating resources are sooner or later declining.

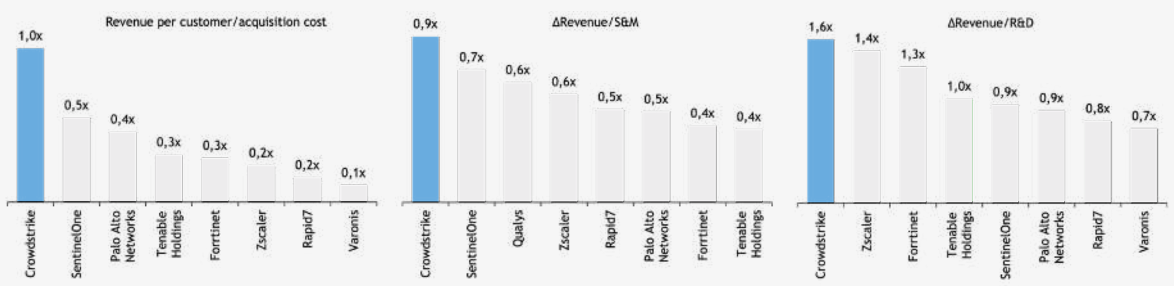
CROWDSTRIKE

CROWDSTRIKE EXAMPLE

The CrowdStrike example: how brand image contributes to the commercial and technological flywheel.

Crowdstrike is often cited as one of the most successful businesses in the cybersecurity space, notably in terms of revenue growth or brand image. The American software vendor has developed (among others) a cloud-based EDR solution integrated with a proprietary platform that boasts industry-leading detection fatigue and churn rates, making it both a technological and commercial success. We observe this distinction is associated with best-of-breed R&D and S&M efficiency metrics, as shown below. The CrowdStrike example is a perfect illustration of the commercial and technological flywheel: its best of breed technology attracts new clients, retains the existing ones, thereby growing the scale of the dataset against which its model can train, further strengthening its competitive advantage.

FIG 11: OPERATIONAL EFFICIENCY DRIVES BEST IN CLASS REVENUE/ACQUISITION COSTS



*Source: Stifel**

Contrary to Crowdstrike, Cyberrason failed to maintain the flywheel effect. The Softbank-backed firm that over-hired during the 2021-2022 period had to cut off staff and experienced a sharp deceleration in revenue. While it struggles to scale, the privately held company saw its valuation collapsing by 90% to USD300m, while its CEO Lior Div was announced to be replaced by Eric Gan, SoftBank's executive vice president in 2023.

Half life of innovation: a shortening cycle

Innovation is obviously a key component of the competitive advantage cybersecurity solution providers seek to develop. The half life of an innovation (or its capacity to represent an advantage for a firm) is shrinking as competition and automation accelerate the discovery process and the time to market for new solutions. As such the decade-long lifecycles of innovations is shortening, while the magnitude of these innovations diminishes.

Cybersecurity solutions typically appear in response to emerging innovations in digital threats. As such, a new software addressing a specific need experiences a period of significant growth as demand surges, and then stagnates as the number of innovations in a segment drops, while the number of threats and security tools reach an equilibrium. This feature implies the cybersecurity market experiences successive growth waves as a solution appears, spreads and reaches maturity. As a consequence, the overall cybersecurity market evolves with the cohorts of new products being developed in response to cyberthreats. The cybersecurity market is therefore hardly predictable as the bulk of growth should come from breakthroughs rather than from existing products.

As an illustration, antiviruses thrived from the 1990s to the 2000s as innovation in both threats and remedies constantly fuelled growth. The latter stalled however as the addressable market reached its full potential in the post 2000 decade. The same goes with legacy hardware firewalls that are gradually being replaced with cloud-based solutions. The same is true for VPN software solutions that have now largely spread across organisations.

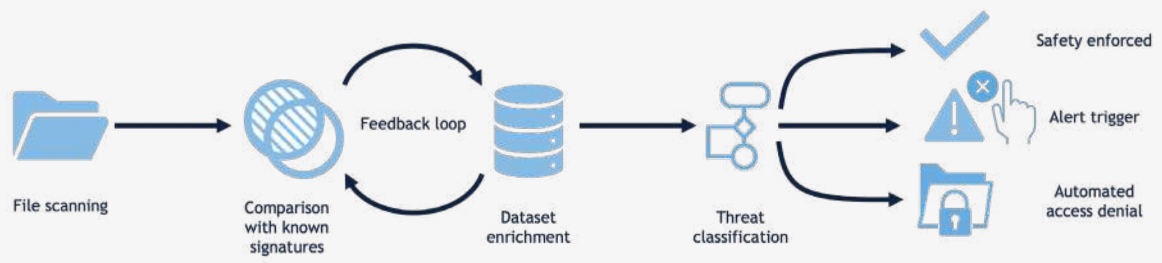
To sum up, the half life of an innovation in cybersecurity, or the time it takes to reach maturity and for its growth to decay, is a function of the innovation attackers develop to circumvent the protection methods. Both hackers and software vendors are making increasing use of AI and are racing to discover Zero Day (i.e. unexploited vulnerability) attack opportunities. As a consequence, innovations are becoming obsolete at a quicker rate and the half life of a protection method should decline, meaning cycles in the cybersecurity market could become shorter.

HOW DOES EDR WORK?

Endpoint Detection and Response is a set of solutions designed to detect, investigate, and respond to security incidents at the endpoint level (i.e., servers, laptops, mobiles, and other network-connected devices). EDR is based on a model's capacity to automatically detect threats and remediate them. The cornerstone of EDR solutions is therefore the power of the Artificial Intelligence (AI) model and the depth of the dataset against which it is trained. Once a potential threat is detected, it gives rise to a response that can range between a simple alert trigger to outright access denial to the corrupted file.

We distinguish two categories of EDR technologies: signature-based and behaviour-based models. The first consists of comparing the files stored on a device to a database of known malicious files using their digital signature. While signature- based EDR can be effective at detecting and stopping known threats, it is ineffective to detect unknown (or 'Zero Day') threats.

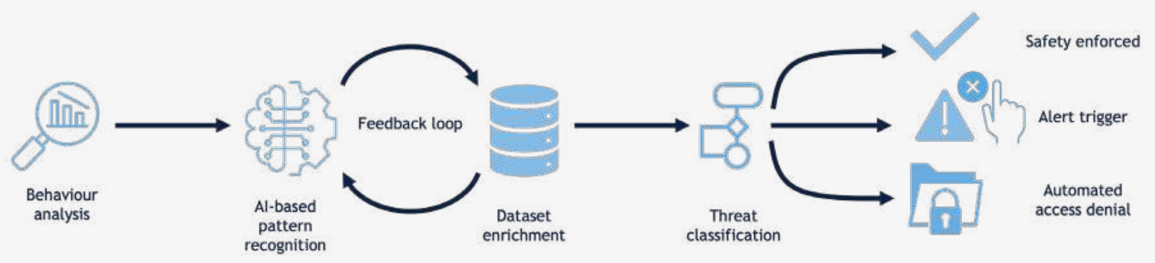
FIG 12: SIGNATURE-BASED EDR



*Source: Stifel**

The second type of EDR tool consists of identifying suspicious behaviour based on user or file activity. Here again, behaviour patterns are detected via an AI model comparing them with typical suspicious patterns. When a match is found, the EDR software triggers an action to prevent security breaches. Behaviour-based EDR software is capable of stopping Zero Day attacks.

FIG 13: BEHAVIOUR-BASED EDR



*Source: Stifel**

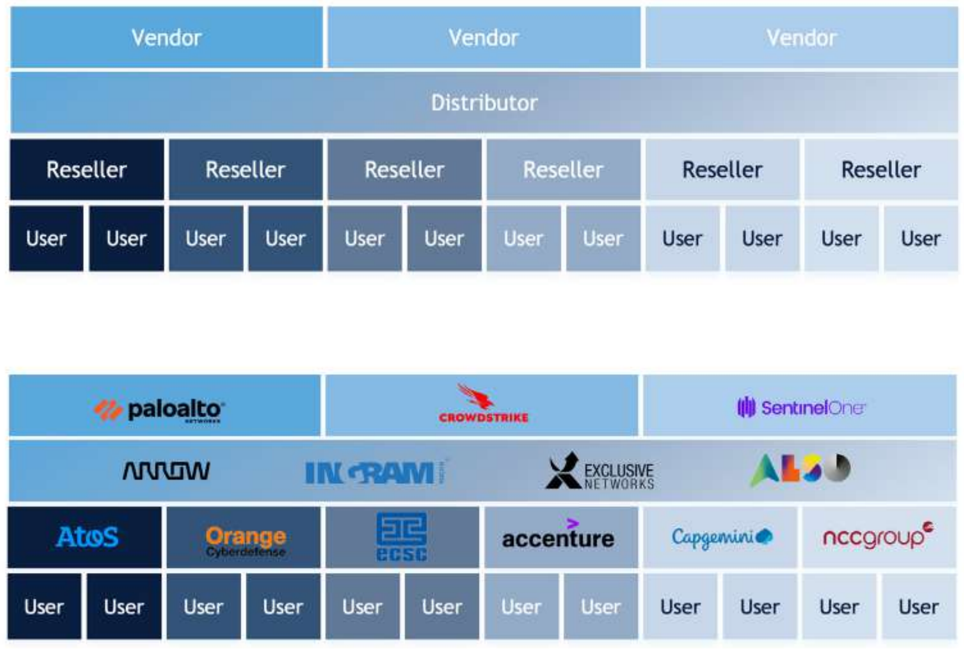
The distribution channel: passing on the fixed costs

Together with efficient resource allocation, we believe the distribution channel is a cornerstone of the success of a cybersecurity business. In this respect, two possible paths are open for cybersecurity software vendors to go to market: internalising or outsourcing distribution functions. Self-operated distribution channels internalise the commissions otherwise paid out to intermediaries, thereby lifting the margins of the editor. Nevertheless, developing and training a sales force in house might not be the best use of internal resources. Software vendors should indeed focus on R&D rather than tackle the cumbersome process of distributing and tailoring solutions to a large and diverse customer base expressing uneven needs. Furthermore, outsourcing distribution transforms a capacity-constrained sales department with a high proportion of fixed costs into a scalable function that comes at a variable cost, offering greater flexibility to the editor.

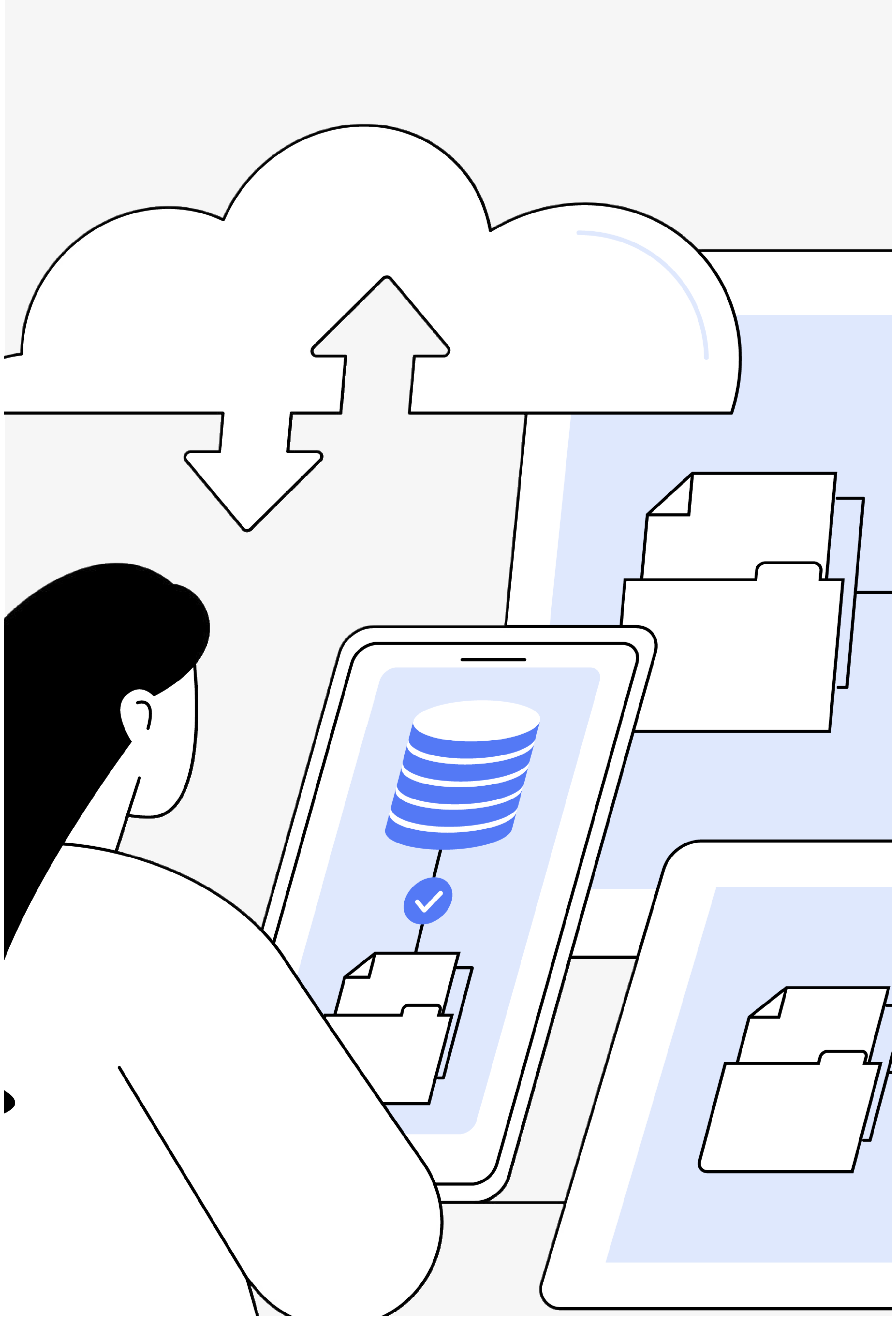
As a consequence and unsurprisingly, the cybersecurity value chain is organised around a professional, outsourced distribution channel. Depending on the geography, the latter is often based on a two-tier model featuring a distributor (or wholesaler) and a reseller. In this framework, the distributor acts as a sole customer for the software vendor, and assumes responsibility for distributing the most appropriate solution to resellers. These are the end-customer-facing intermediaries responsible for advising and adjusting the software to the needs of the end user. As such the wholesaling model dramatically streamlines go-to-market for vendors as it represents a single touchpoint to a multitude of resellers and users. We note this model is widely used in Europe and Asia, where the end markets are more fragmented and complex to address than in North America. There is no surprise Europe is home to some of the largest distributors like Exclusive Networks.

This market structure keeps the smallest vendors away from large distributors, forcing them to participate in the consolidation to access larger clients.

FIG 14: THE TWO-TIER CYBERSECURITY SOFTWARE DISTRIBUTION MODEL

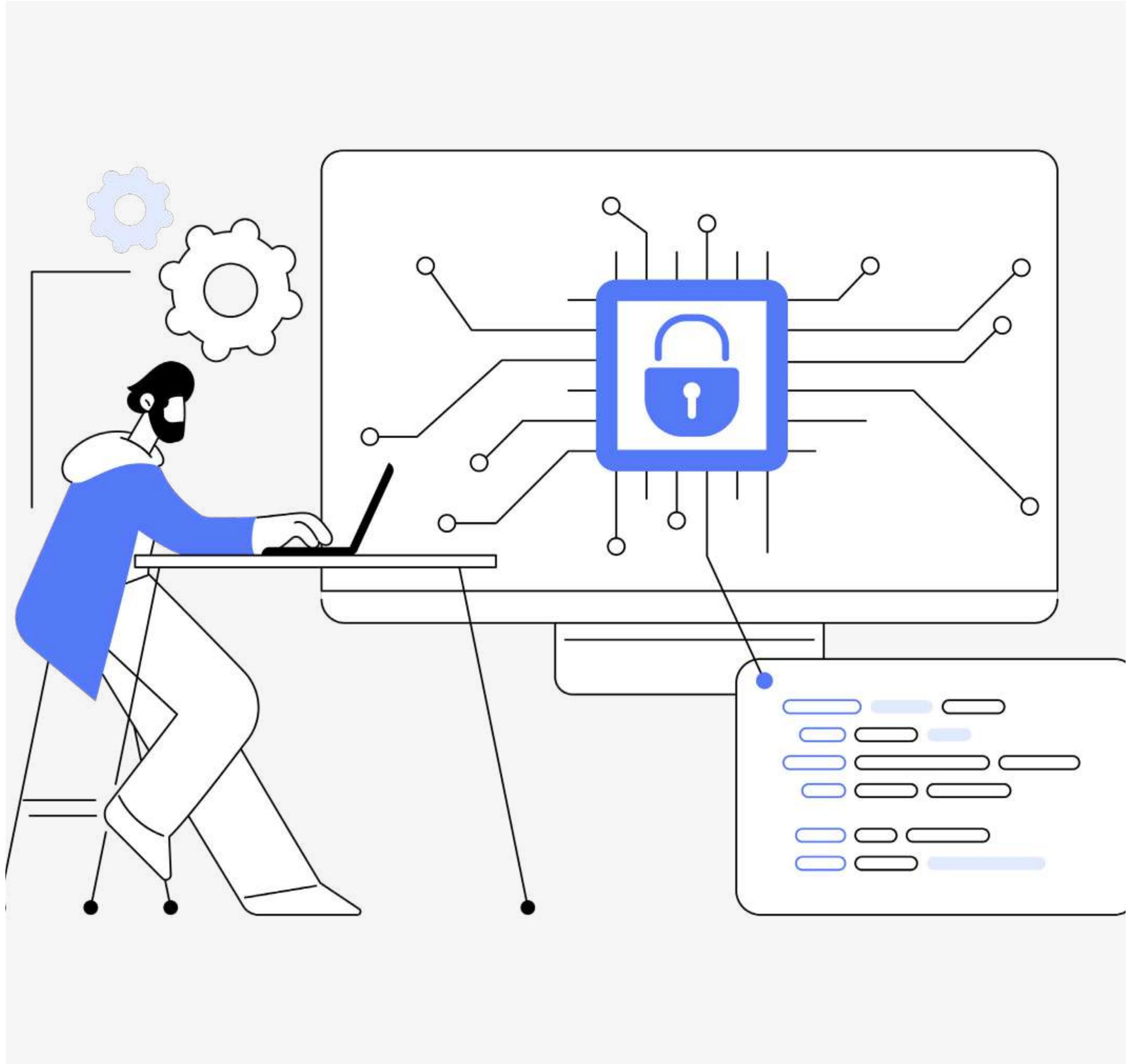


*Source: Stifel**



FIVE TRENDS **REDEFINING** THE SECTOR

SECTION 3



We have identified five trends that we expect to drive changes in the cybersecurity sector in coming years. We consider the future cybersecurity winners are those capable of embracing these trends.

TREND 1: Move towards platforms

Today's highly fragmented cybersecurity market is widely spread between countless different solutions, with each company having its own speciality. In this regard, most organisations are clients of multiple cybersecurity providers at the same time. A study undertaken in 2020 (Oracle and KPMG Cloud Threat Report 2020) found that 78% of organisations use more than 50 discrete cybersecurity products and 37% use more than 100 cybersecurity products.

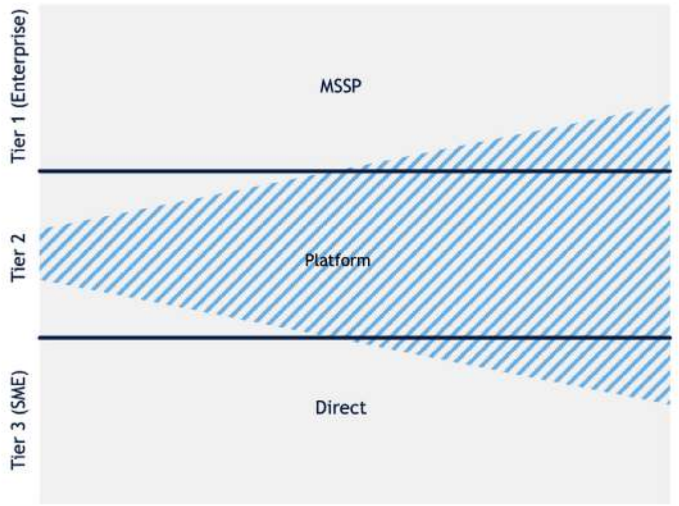
Although this approach offers the advantage of using the leader, and in theory the best solution, for each application, it is however not optimal and implies challenges. Firstly, cost is drastically increased as a result of having to pay for 50+ different solutions. Secondly, it requires significant staff efforts to master and operate each individual solution and its interactions. Usually, a greater number of providers is associated with more significant personnel requirements. Thirdly, having too many solutions running at the same time creates a conflict as they struggle to co-exist, by creating interferences and not effectively integrating all the available data. Fourthly, stacking multiple solutions covering very specific areas creates gaps of unknown coverage even if each solution is a leader in its field.

Due to the above issues, a consolidation in cybersecurity solutions towards a platform approach seems necessary. Platforms would provide organisations with a single plane of glass, encompassing all different needs, from device security, to network or application security, all integrated in a single touchpoint for users. Cybersecurity platforms streamline the day-to-day job of the involved teams, they save time and cut overall cost of ownership while improving security for the organisation.

Platforms are ubiquitous across an organisation's perimeter, network, endpoint or applications making the solution smarter and more effective at detecting threats. These also reduce the rate of detection fatigue, finding more accurate patterns and accumulating hints. For example, a network security solution spotting suspicious behaviour with too little information could easily raise a false alert, but a platform combining information from other layers could contextualise the event and classify it with accuracy.

Given their multiple advantages, we believe cybersecurity platforms could bite into both the large enterprise and the SME segments over time. Enterprises typically outsource their cybersecurity operations to Managed Security Services Providers (MSSPs) due to the high cost of monitoring a large IT stack on a 24/7 basis. As platforms streamline cybersecurity management, this function could be brought back in house by some of the largest companies. Conversely, SMEs tend to internalise the cybersecurity function as their scale makes it economically advantageous or because the cost of MSSPs are prohibitive for sub-scaled businesses. In that case, platforms can help to streamline complex security architectures, thereby slashing costs and cutting needs for dedicated teams. As a consequence, platforms should not only overtake traditional solutions in the mid market, but also in part of the SME and Enterprise segments.

FIG 15: CYBERSECURITY PLATFORM MARKET SHARE EVOLUTION VS TRADITIONAL SOLUTIONS



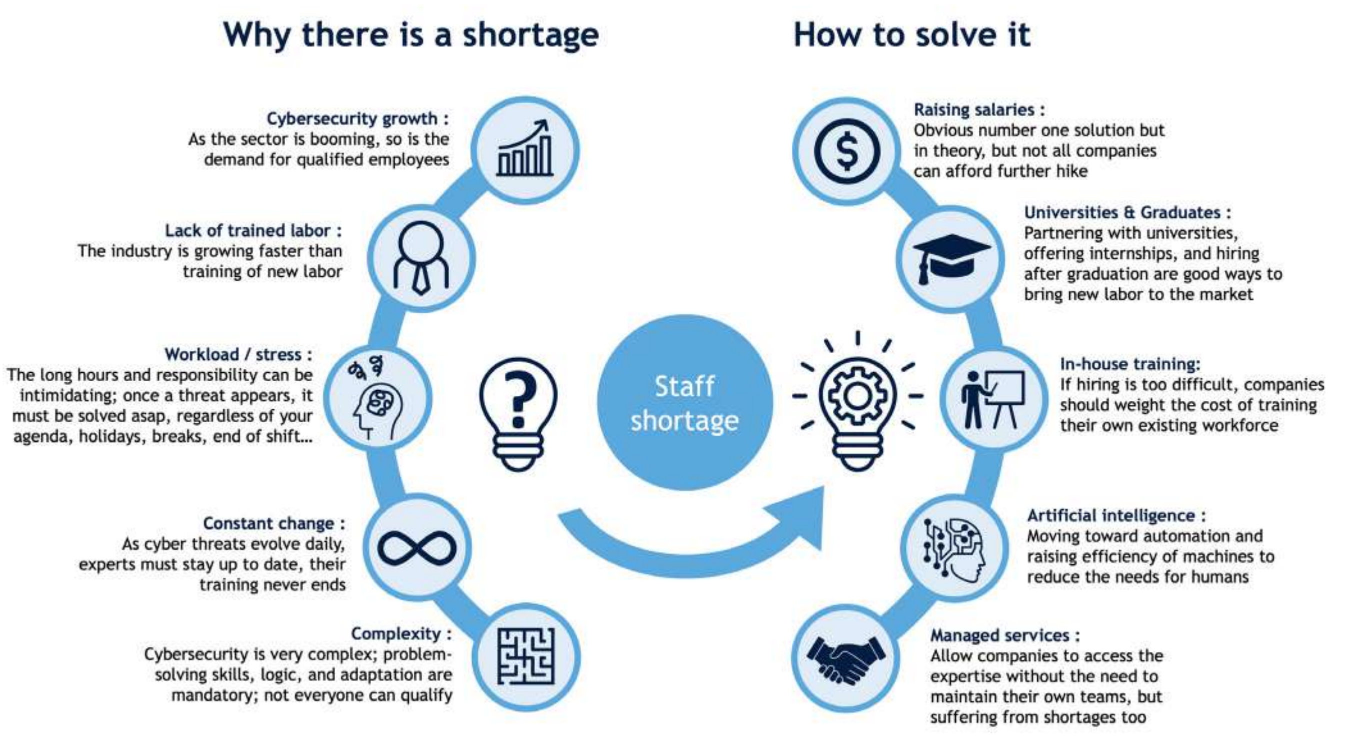
*Source: Stifel**

Key platform players include the likes of PaloAlto Networks, Forinet, Crowdstrike or SentinelOne. Most of them are based in the US and have experienced significant traction lately.

TREND 2: staff shortages, or the case for automation

While Cybersecurity as a sector is seeing very rapid expansion, the labour side is struggling to match the pace. According to the 2022 (ISC)2 Cybersecurity Workforce Study, 4.7m professionals worked globally in cybersecurity and 3.4m jobs were unfilled, implying that 42% of global positions remain unfilled. The mismatch between supply and demand for cyber staff could ultimately favour AI-driven software solutions given their greater scalability.

FIG 16: CYBER STAFF SHORTAGE TO DRIVE THE ADOPTION OF AI TOOLS



Cybersecurity growth : As the sector is booming, so is the demand for qualified employees

Lack of trained labor : The industry is growing faster than training of new labor

Workload / stress : The long hours and responsibility can be intimidating; once a threat appears, it must be solved asap, regardless of your agenda, holidays, breaks, end of shift...

Constant change : As cyber threats evolve daily, experts must stay up to date, their training never ends

Complexity : Cybersecurity is very complex; problem-solving skills, logic, and adaptation are mandatory; not everyone can qualify

Raising salaries : Obvious number one solution but in theory, but not all companies can afford further hike

Universities & Graduates : Partnering with universities, offering internships, and hiring after graduation are good ways to bring new labor to the market

In-house training: If hiring is too difficult, companies should weight the cost of training their own existing workforce

Artificial intelligence : Moving toward automation and raising efficiency of machines to reduce the needs for humans

Managed services : Allow companies to access the expertise without the need to maintain their own teams, but suffering from shortages too

*Source: Stifel**

As cohorts of cybersecurity engineers cannot be trained overnight, the imbalance between supply and demand for cyber workers is unlikely to revert any time soon. This paradigm should thus stimulate organisations' willingness to delegate and automate their cybersecurity tasks, driving demand for MSSP and AI-based solutions. While labour-intensive managed services offer limited scalability, AI-based cybersecurity solutions are highly scalable and likely to capture most of the demand stemming from staff shortages in the industry. In all, firms embracing the AI revolution should expect market share gains over traditional players. Integrated solutions comprising cybersecurity and automation capacities should therefore be in high demand. Generalists like Alphabet and Microsoft, or automation specialists like UiPath could benefit from this trend.

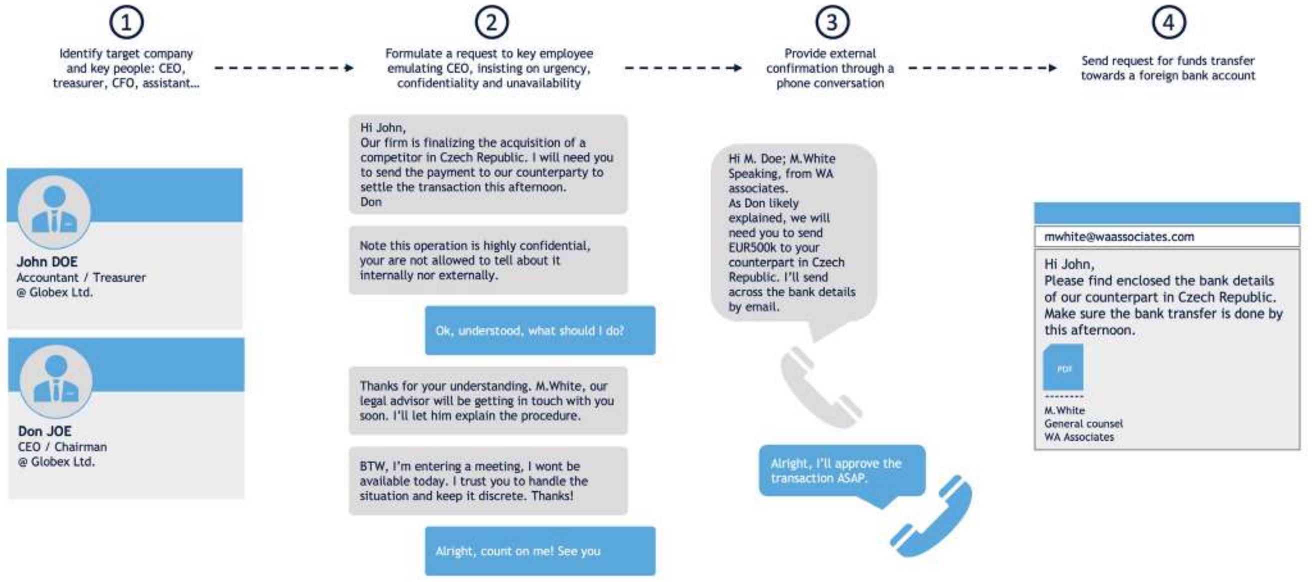
TREND 3: The human factor is the weak link

A study from Stanford Research carried out in 2020 concluded that 88% of data breaches were caused by human error (estimates typically range from 80% to 95%). Humans can indeed fall prey to social engineering techniques that leads them to divulge sensitive information and ultimately let attackers gain access to what they are after.

This was the case for example with the Twitter Bitcoin scam attack in 2020 where multiple high-profile Twitter accounts belonging to the likes of Barack Obama, Jeff Bezos, Apple, etc were hijacked and used to promote the scam. To do so, attackers simply found Twitter employees on Linkedin, and contacted them, pretending to be Twitter personnel then asking them to log-in to a fake internal Twitter VPN, exploiting the remote-working context.

Social engineering scams can even go further by emulating a manager's instruction to send funds to a foreign bank account. This type of scam is based on digital tools (including social media, phone number hacking and email address falsification), yet it almost entirely relies on social biases. Therefore, even the most sophisticated software would fail to detect it.

FIG 17: SOCIAL ENGINEERING EXAMPLE: FUND TRANSFER SCAM


1
Identify target company and key people: CEO, treasurer, CFO, assistant...
2
Formulate a request to key employee emulating CEO, insisting on urgency, confidentiality and unavailability
3
Provide external confirmation through a phone conversation
4
Send request for funds transfer towards a foreign bank account
PDF

John DOE
Accountant / Treasurer
@ Globex Ltd.

Don JOE
CEO / Chairman
@ Globex Ltd.

Hi John,
Our firm is finalizing the acquisition of a competitor in Czech Republic. I will need you to send the payment to our counterparty to settle the transaction this afternoon.
Don

Note this operation is highly confidential, your are not allowed to tell about it internally nor externally.

Ok, understood, what should I do?

Thanks for your understanding. M.White, our legal advisor will be getting in touch with you soon. I'll let him explain the procedure.

BTW, I'm entering a meeting, I wont be available today. I trust you to handle the situation and keep it discrete. Thanks!

Alright, count on me! See you

Hi M. Doe; M.White Speaking, from WA associates.
As Don likely explained, we will need you to send EUR500k to your counterpart in Czech Republic. I'll send across the bank details by email.

Alright, I'll approve the transaction ASAP.

mwhite@waassociates.com

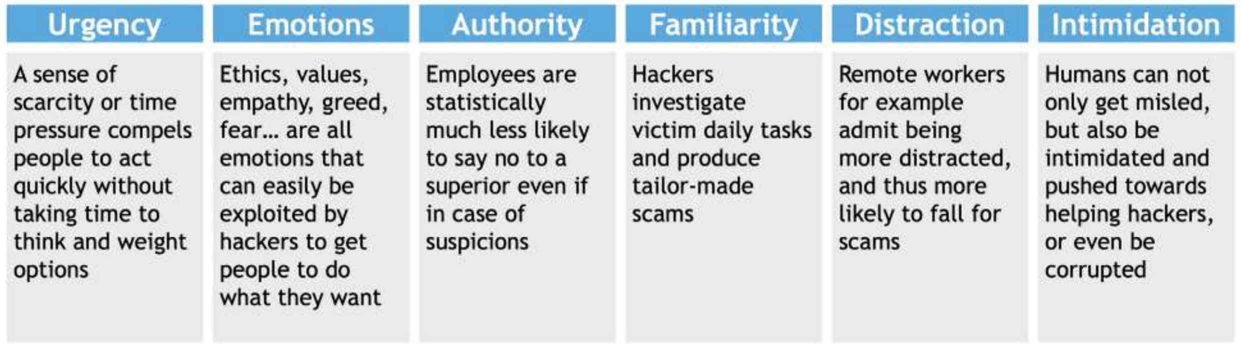
Hi John,
Please find enclosed the bank details of our counterpart in Czech Republic. Make sure the bank transfer is done by this afternoon.

M.White
General counsel
WA Associates

*Source: Stifel**

This type of scam exploits human vulnerabilities and biases including the following:

FIG 18: HUMAN ERROR AND SOCIAL ENGINEERING – WE ARE RICH IN VULNERABILITIES



Urgency	Emotions	Authority	Familiarity	Distraction	Intimidation
A sense of scarcity or time pressure compels people to act quickly without taking time to think and weight options	Ethics, values, empathy, greed, fear… are all emotions that can easily be exploited by hackers to get people to do what they want	Employees are statistically much less likely to say no to a superior even if in case of suspicions	Hackers investigate victim daily tasks and produce tailor-made scams	Remote workers for example admit being more distracted, and thus more likely to fall for scams	Humans can not only get misled, but also be intimidated and pushed towards helping hackers, or even be corrupted

*Source: Stifel**

In this regard, raising awareness and training employees is becoming increasingly important. While the cost of training staff might be significant, the cost of having even a single one of them fall for a scam can run to millions. It is therefore very likely that cybersecurity training and awareness will become more and more prominent and companies offering those services could enjoy high growth. This training could even become legally obligatory in the near future, as is already the case in certain sectors and countries. Just like fire alarm training in office buildings, cyberattack training could soon become mandatory to spot vulnerabilities and prevent them.

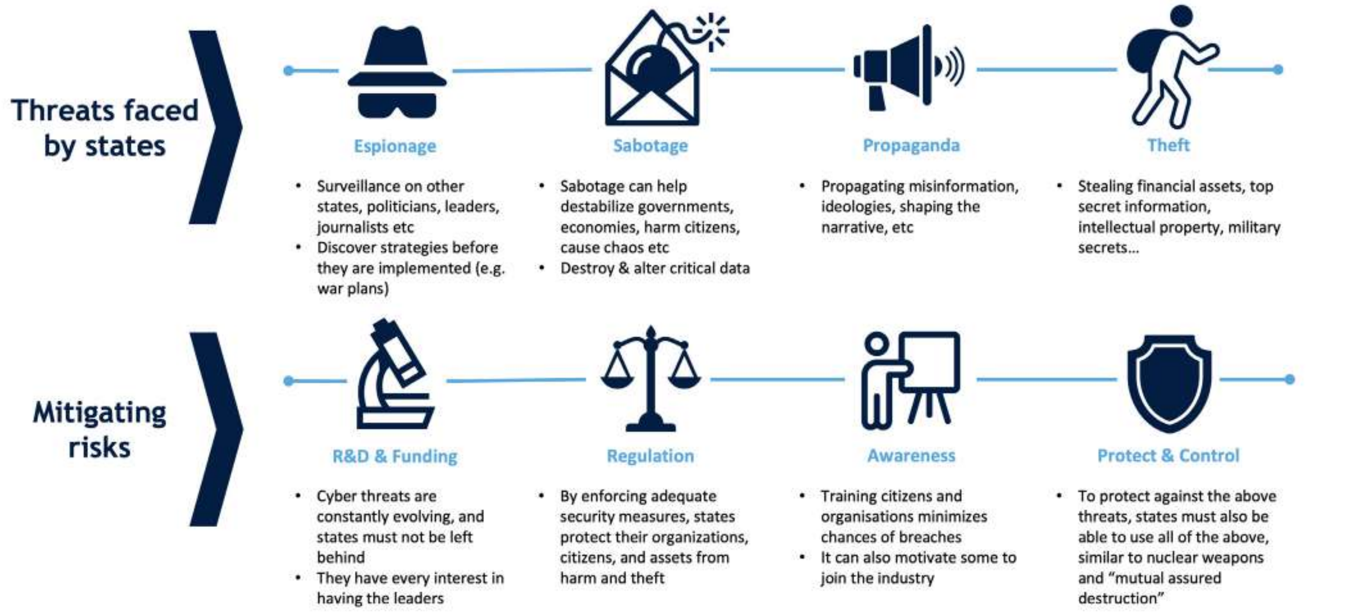
Firms like KnowBe4, SoSafe or Riot offer these services based on digital and interactive contents.

TREND 4: Public pressures

Cyberattacks are now considered a weapon of war, used to spy, fight, defend, control information or intimidate. A very severe targeted cyberattack could have the power to destroy an economy, financial assets, ruin the financial markets, steal classified documents, proprietary information, or shut down infrastructures (energy, communication…). Governments take these challenges seriously as their spending on cybersecurity globally reached USD45bn in 2022, a fourth of the total market size.

Public bodies may drive demand for cybersecurity solutions by pulling two levers: 1) their own demand for cybersecurity as public IT infrastructures modernise, 2) regulations pushing adoption of such solutions by third parties.

FIG 19: THREATS FACED BY THE PUBLIC SECTOR AND MITIGATION TOOLS



Threats faced by states

Espionage

- Surveillance on other states, politicians, leaders, journalists etc
- Discover strategies before they are implemented (e.g. war plans)

Sabotage

- Sabotage can help destabilize governments, economies, harm citizens, cause chaos etc
- Destroy & alter critical data

Propaganda

- Propagating misinformation, ideologies, shaping the narrative, etc

Theft

- Stealing financial assets, top secret information, intellectual property, military secrets…

Mitigating risks

R&D & Funding

- Cyber threats are constantly evolving, and states must not be left behind
- They have every interest in having the leaders

Regulation

- By enforcing adequate security measures, states protect their organizations, citizens, and assets from harm and theft

Awareness

- Training citizens and organisations minimizes chances of breaches
- It can also motivate some to join the industry

Protect & Control

- To protect against the above threats, states must also be able to use all of the above, similar to nuclear weapons and "mutual assured destruction"

*Source: Stifel**

The current geopolitical scene shows how critical cyber weapons can be for governments. Examples include the Russia- Ukraine conflict that came with thousands of cyberattacks, the infection of several government members by the infamous Pegasus spyware that hacks mobile phones (Pegasus customers are almost exclusively governments), or North Korea's revenue streams 10% of which is presumed to come from hacking. While the threats accumulate, governments continue to invest in cybersecurity to protect their IT infrastructure. We expect these trends to continue, and even accelerate, with public spending continuing to hike.

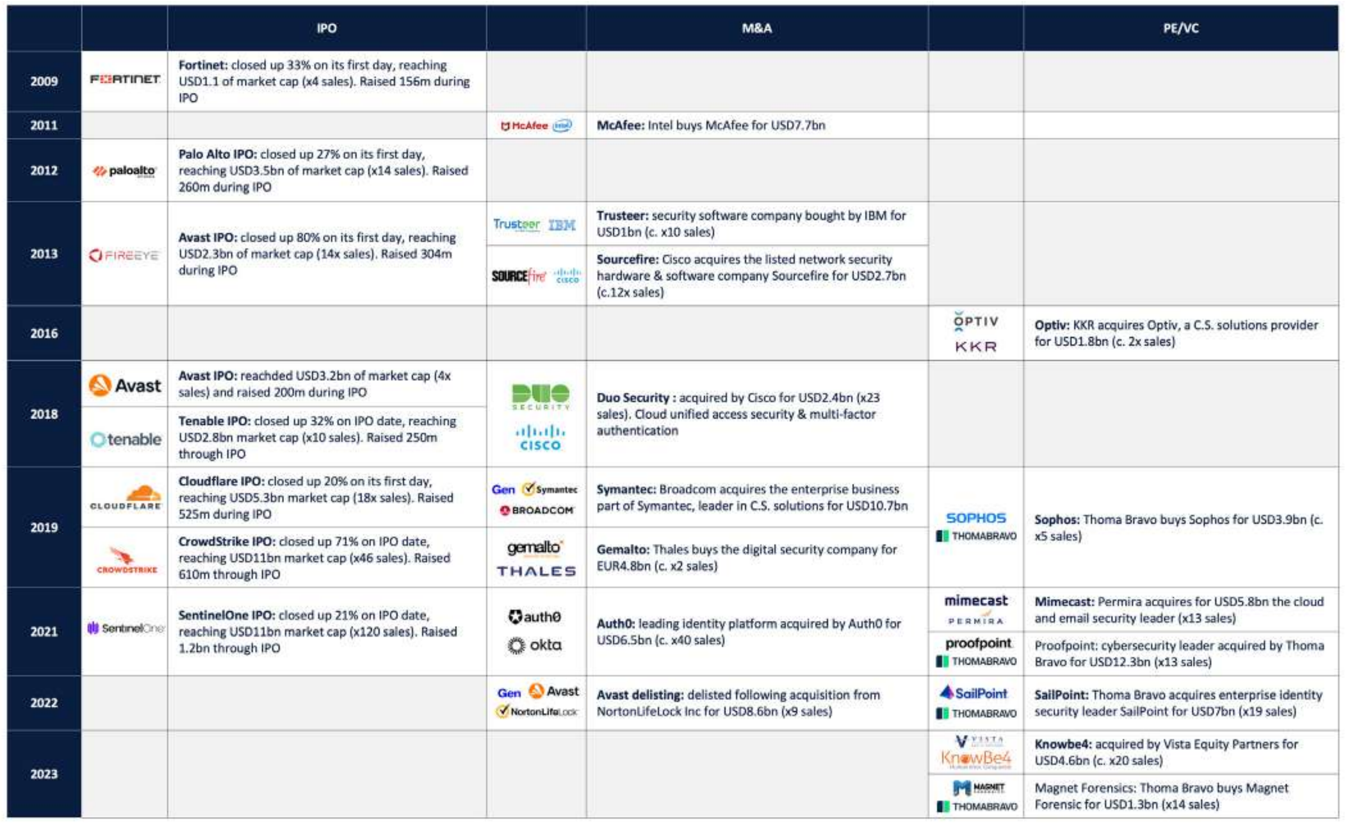
In an attempt to prevent individuals and organisations from being hacked by foreign entities, European public powers have developed strict regulationsthat companies must apply. These include among others, the GDPR, the Cyber Resilience Act (CRA), and the Network Information Security (NIS)2 regulation. While the GDPR is more tilted towards consumer data protection, the NIS aims at creating computer security incident response teams and fostering collaboration between member states of the European Union. Although it is yet to enter into force, the CRA will impose cybersecurity requirements on connected devices and software processing data remotely. Altogether, this legislatory framework is acatalyst for cybersecurity adoption within the European Union. Furthermore, the greater degree of regulation and the quest for sovereignty could lead some governments and public agencies to favour local cybersecurity vendors over foreign ones, as suspicions of espionage activities grow between rival countries.

To sum up, both government demand and regulations are powerful catalysts for the cybersecurity market. Firms offering solutions fostering compliance should thus take advantage of the public powers' move towards cybersecurity adoption.

TREND 5: Consolidation towards a fully integrated model?

As a consequence of the move towards platforms, leaders absorb their most innovative peers while smaller firms get passed from one VC & PE firm to the next, until they reach the critical size to appear on the leader's radar or become listed. The industry is therefore extremely active in terms of M&A deals. Activity in the sector is driven by both investment firms seeking exposure to fast growing industries and strategic investors seeking technology bricks to add to their platform.

FIG 20: TIMELINE OF SIGNIFICANT ACQUISITIONS IN CYBERSECURITY



		IPO		M&A		PE/VC
2009	FORTINET	**Fortinet:** closed up 33% on its first day, reaching USD1.1 of market cap (x4 sales). Raised 156m during IPO				
2011			McAfee intel	**McAfee:** Intel buys McAfee for USD7.7bn		
2012	paloalto	**Palo Alto IPO:** closed up 27% on its first day, reaching USD3.5bn of market cap (x14 sales). Raised 260m during IPO				
2013	FIREEYE	**Avast IPO:** closed up 80% on its first day, reaching USD2.3bn of market cap (14x sales). Raised 304m during IPO	Trusteer IBM	**Trusteer:** security software company bought by IBM for USD1bn (c. x10 sales)		
			SOURCEfire cisco	**Sourcefire:** Cisco acquires the listed network security hardware & software company Sourcefire for USD2.7bn (c.12x sales)		
2016					OPTIV KKR	**Optiv:** KKR acquires Optiv, a C.S. solutions provider for USD1.8bn (c. 2x sales)
2018	Avast	**Avast IPO:** reachded USD3.2bn of market cap (4x sales) and raised 200m during IPO	DUO SECURITY CISCO	**Duo Security :** acquired by Cisco for USD2.4bn (x23 sales). Cloud unified access security & multi-factor authentication		
	tenable	**Tenable IPO:** closed up 32% on IPO date, reaching USD2.8bn market cap (x10 sales). Raised 250m through IPO				
2019	CLOUDFLARE	**Cloudflare IPO:** closed up 20% on its first day, reaching USD5.3bn market cap (18x sales). Raised 525m during IPO	Gen Symantec BROADCOM	**Symantec:** Broadcom acquires the enterprise business part of Symantec, leader in C.S. solutions for USD10.7bn	SOPHOS THOMABRAVO	**Sophos:** Thoma Bravo buys Sophos for USD3.9bn (c. x5 sales)
	CROWDSTRIKE	**CrowdStrike IPO:** closed up 71% on IPO date, reaching USD11bn market cap (x46 sales). Raised 610m through IPO	gemalto THALES	**Gemalto:** Thales buys the digital security company for EUR4.8bn (c. x2 sales)		
2021	SentinelOne	**SentinelOne IPO:** closed up 21% on IPO date, reaching USD11bn market cap (x120 sales). Raised 1.2bn through IPO	auth0 okta	**Auth0:** leading identity platform acquired by Auth0 for USD6.5bn (c. x40 sales)	mimecast PERMIRA	**Mimecast:** Permira acquires for USD5.8bn the cloud and email security leader (x13 sales)
					proofpoint THOMABRAVO	Proofpoint: cybersecurity leader acquired by Thoma Bravo for USD12.3bn (x13 sales)
2022			Gen Avast NortonLifeLock	**Avast delisting:** delisted following acquisition from NortonLifeLock Inc for USD8.6bn (x9 sales)	SailPoint THOMABRAVO	**SailPoint:** Thoma Bravo acquires enterprise identity security leader SailPoint for USD7bn (x19 sales)
2023					VISTA KnowBe4	**Knowbe4:** acquired by Vista Equity Partners for USD4.6bn (c. x20 sales)
					MAGNET THOMABRAVO	Magnet Forensics: Thoma Bravo buys Magnet Forensic for USD1.3bn (x14 sales)

*Source: Stifel**

We summarise below the main 10 acquirers of cybersecurity companies, ranked by size, highlighting as a result the difference between VC funds, investing in a vast amount of smaller players and PE firms, with fewer deals but higher bets.

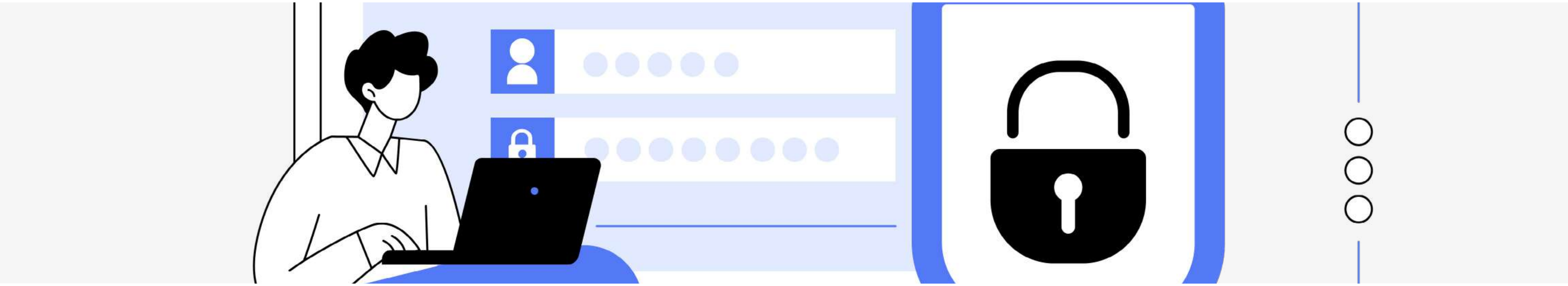
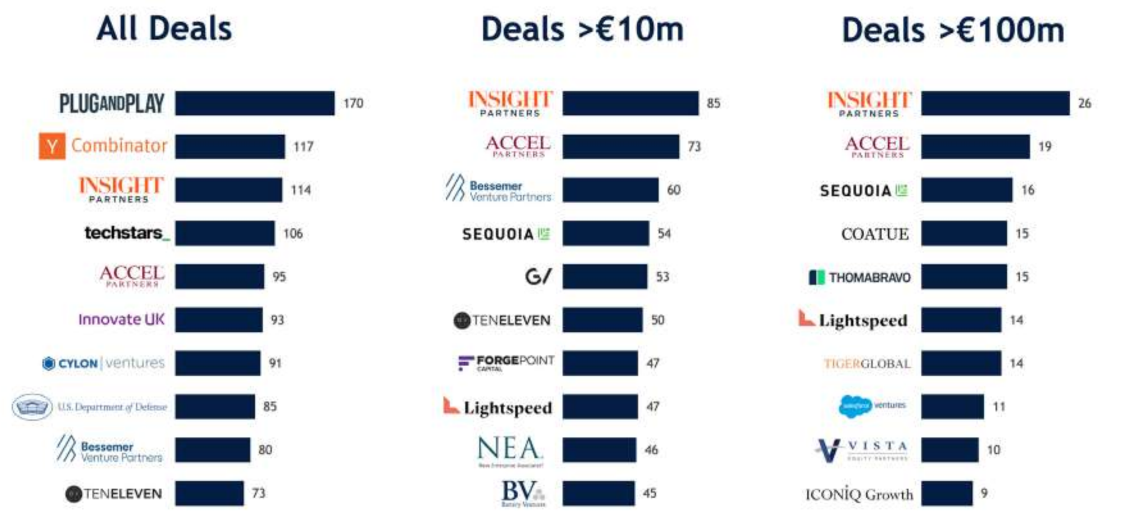
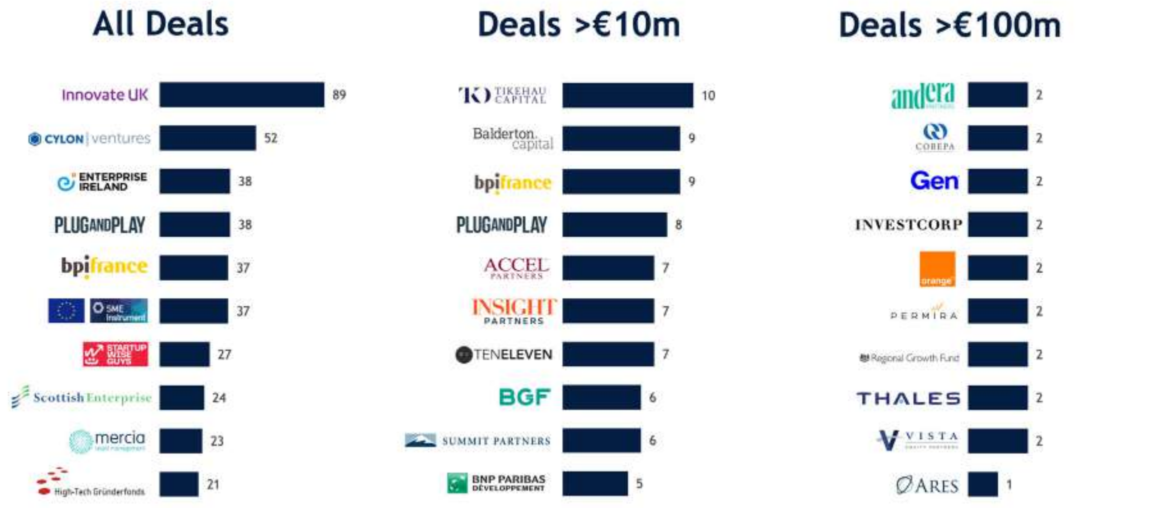


FIG 21: TOP 10 INVESTORS IN CYBERSECURITY WORLDWIDE BY NUMBER OF DEALS IN THE LAST 10 YEARS



Source: Pitchbook; Stifel*

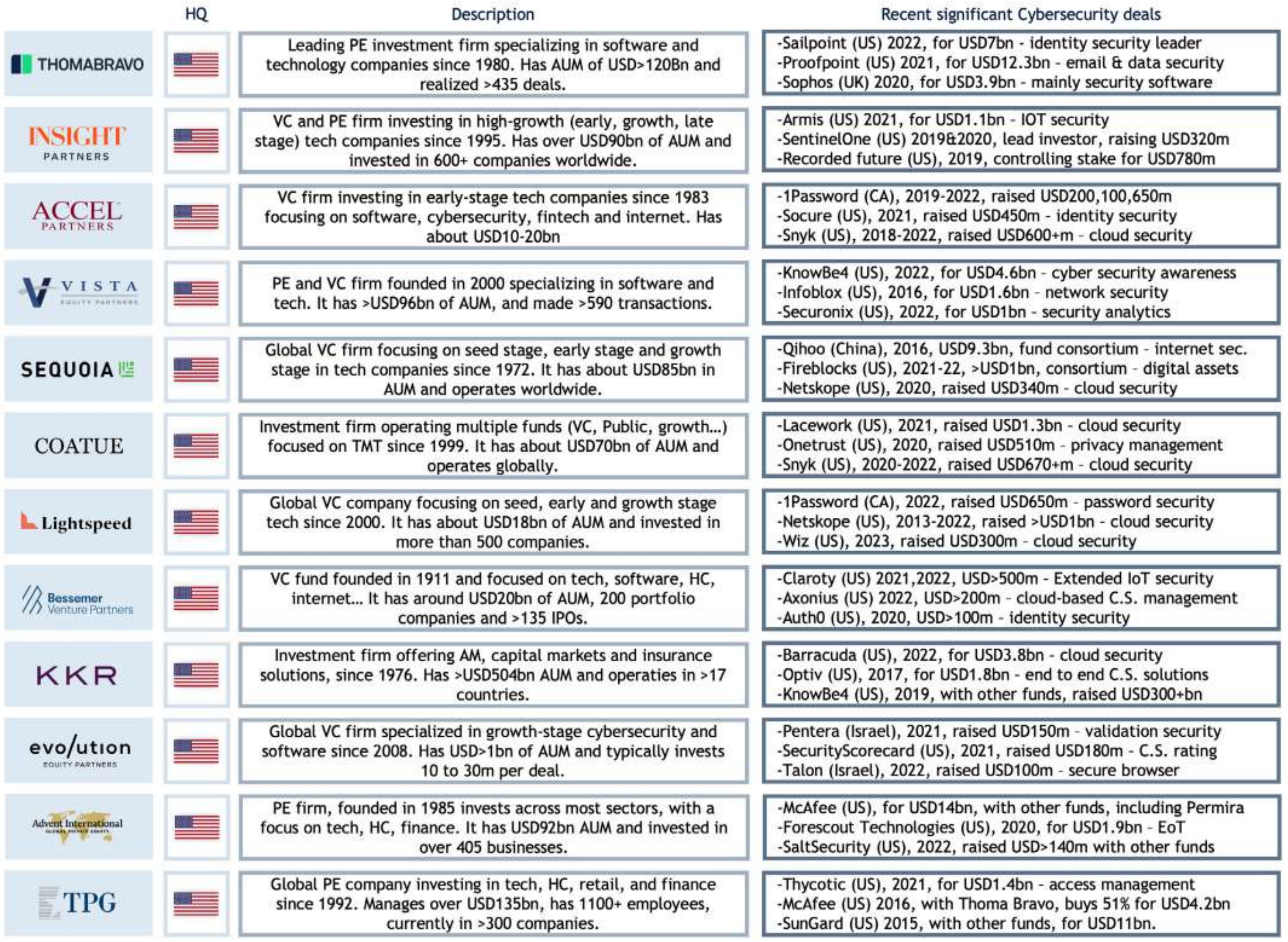
FIG 22: TOP 10 INVESTORS IN CYBERSECURITY IN EUROPE BY NUMBER OF DEALS IN THE LAST 10 YEARS



Source: Pitchbook; Stifel*

Despite its multi-billion dollar size, the industry nonetheless feels like a small world as we keep seeing the same players over and over again, like Thoma Bravo, Insight Partners, Accel Partners or Vista Equity Partners.

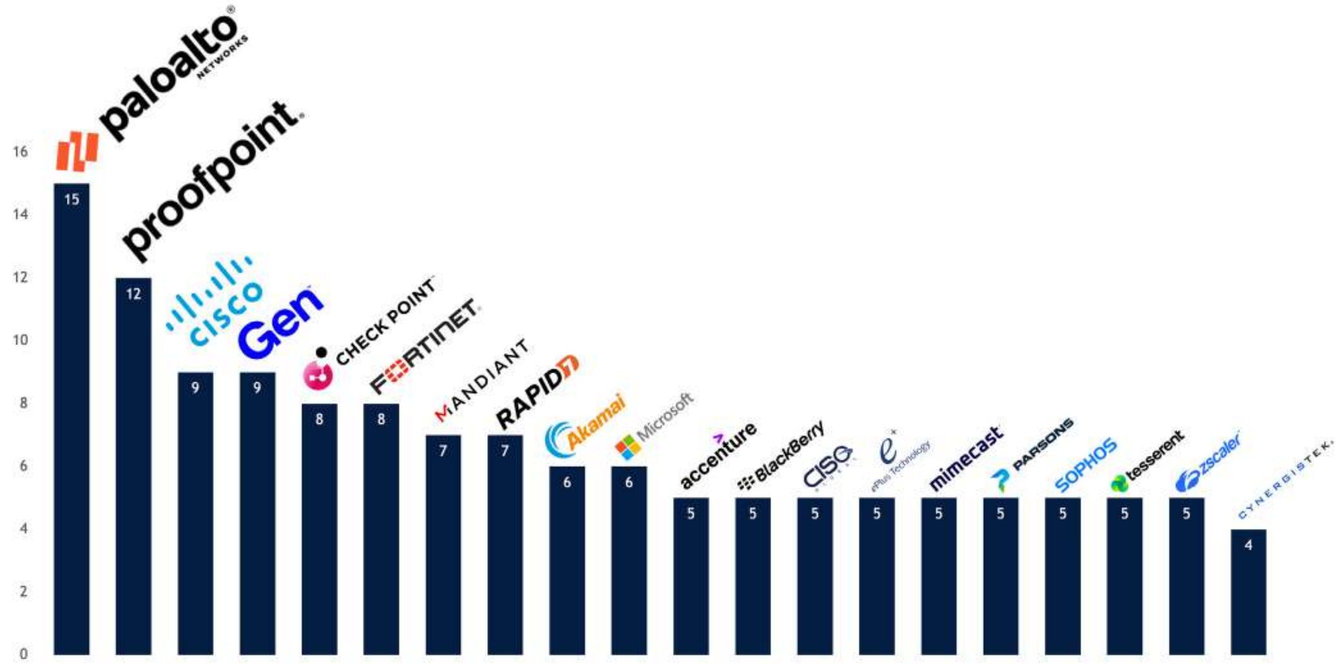
FIG 23: MAIN VC & PE ACQUIRERS IN CYBERSECURITY



	HQ	Description	Recent significant Cybersecurity deals
THOMABRAVO	🇺🇸	Leading PE investment firm specializing in software and technology companies since 1980. Has AUM of USD>120Bn and realized >435 deals.	-Sailpoint (US) 2022, for USD7bn - identity security leader -Proofpoint (US) 2021, for USD12.3bn - email & data security -Sophos (UK) 2020, for USD3.9bn - mainly security software
INSIGHT PARTNERS	🇺🇸	VC and PE firm investing in high-growth (early, growth, late stage) tech companies since 1995. Has over USD90bn of AUM and invested in 600+ companies worldwide.	-Armis (US) 2021, for USD1.1bn - IOT security -SentinelOne (US) 2019&2020, lead investor, raising USD320m -Recorded future (US), 2019, controlling stake for USD780m
ACCEL PARTNERS	🇺🇸	VC firm investing in early-stage tech companies since 1983 focusing on software, cybersecurity, fintech and internet. Has about USD10-20bn	-1Password (CA), 2019-2022, raised USD200,100,650m -Socure (US), 2021, raised USD450m - identity security -Snyk (US), 2018-2022, raised USD600+m - cloud security
VISTA EQUITY PARTNERS	🇺🇸	PE and VC firm founded in 2000 specializing in software and tech. It has >USD96bn of AUM, and made >590 transactions.	-KnowBe4 (US), 2022, for USD4.6bn - cyber security awareness -Infoblox (US), 2016, for USD1.6bn - network security -Securonix (US), 2022, for USD1bn - security analytics
SEQUOIA	🇺🇸	Global VC firm focusing on seed stage, early stage and growth stage in tech companies since 1972. It has about USD85bn in AUM and operates worldwide.	-Qihoo (China), 2016, USD9.3bn, fund consortium - internet sec. -Fireblocks (US), 2021-22, >USD1bn, consortium - digital assets -Netskope (US), 2020, raised USD340m - cloud security
COATUE	🇺🇸	Investment firm operating multiple funds (VC, Public, growth…) focused on TMT since 1999. It has about USD70bn of AUM and operates globally.	-Lacework (US), 2021, raised USD1.3bn - cloud security -Onetrust (US), 2020, raised USD510m - privacy management -Snyk (US), 2020-2022, raised USD670+m - cloud security
Lightspeed	🇺🇸	Global VC company focusing on seed, early and growth stage tech since 2000. It has about USD18bn of AUM and invested in more than 500 companies.	-1Password (CA), 2022, raised USD650m - password security -Netskope (US), 2013-2022, raised >USD1bn - cloud security -Wiz (US), 2023, raised USD300m - cloud security
Bessemer Venture Partners	🇺🇸	VC fund founded in 1911 and focused on tech, software, HC, internet… It has around USD20bn of AUM, 200 portfolio companies and >135 IPOs.	-Claroty (US) 2021,2022, USD>500m - Extended IoT security -Axonius (US) 2022, USD>200m - cloud-based C.S. management -Auth0 (US), 2020, USD>100m - identity security
KKR	🇺🇸	Investment firm offering AM, capital markets and insurance solutions, since 1976. Has >USD504bn AUM and operaties in >17 countries.	-Barracuda (US), 2022, for USD3.8bn - cloud security -Optiv (US), 2017, for USD1.8bn - end to end C.S. solutions -KnowBe4 (US), 2019, with other funds, raised USD300+bn
evo/ution EQUITY PARTNERS	🇺🇸	Global VC firm specialized in growth-stage cybersecurity and software since 2008. Has USD>1bn of AUM and typically invests 10 to 30m per deal.	-Pentera (Israel), 2021, raised USD150m - validation security -SecurityScorecard (US), 2021, raised USD180m - C.S. rating -Talon (Israel), 2022, raised USD100m - secure browser
Advent International	🇺🇸	PE firm, founded in 1985 invests across most sectors, with a focus on tech, HC, finance. It has USD92bn AUM and invested in over 405 businesses.	-McAfee (US), for USD14bn, with other funds, including Permira -Forescout Technologies (US), 2020, for USD1.9bn - EoT -SaltSecurity (US), 2022, raised USD>140m with other funds
TPG	🇺🇸	Global PE company investing in tech, HC, retail, and finance since 1992. Manages over USD135bn, has 1100+ employees, currently in >300 companies.	-Thycotic (US), 2021, for USD1.4bn - access management -McAfee (US) 2016, with Thoma Bravo, buys 51% for USD4.2bn -SunGard (US) 2015, with other funds, for USD11bn.

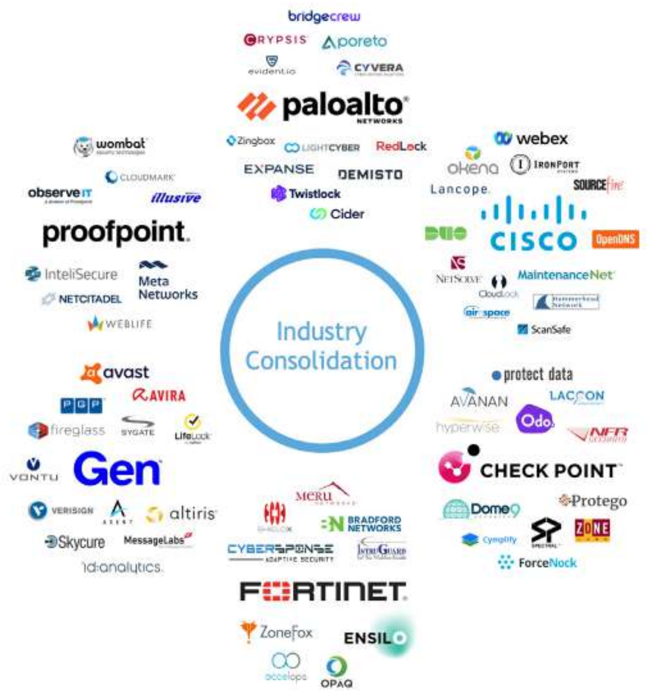
Source: Stifel*, Pitchbook, Fund's website

FIG 24: TOP 20 M&A INVESTORS IN CYBERSECURITY WORLDWIDE BY NUMBER OF DEALS >€1M IN LAST 10 YEARS



*Source: Pitchbook; Stifel**

FIG 25: STRATEGIC CONSOLIDATORS AND THEIR ECOSYSTEM



*Source: Pitchbook; Stifel**

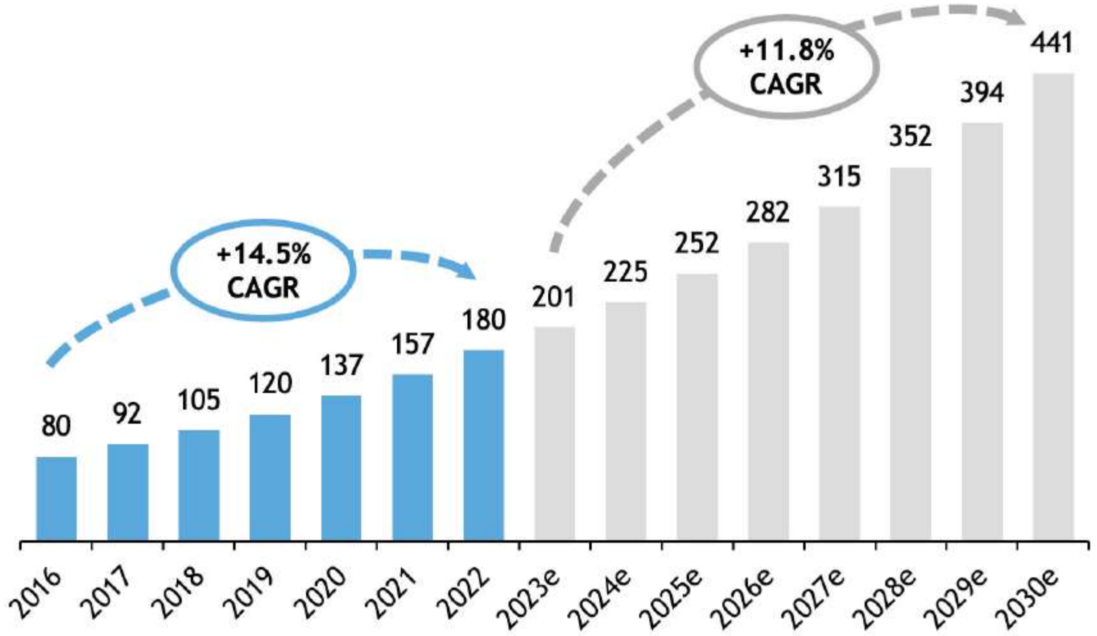
We see no reason at all for this trend towards consolidation, maturing, and ultimately platformisation to stop. On the contrary, we expect it to accelerate, for reasons similar to those seen in Trend#1.

Mainly, having a single cybersecurity provider would involve lower costs, easier use, less training time, less time wasted on finding the best solutions, and preventing bugs that emerge due to conflicts between each solution. Companies understand this trend very well and are trying to match this demand before it is too late.

Opportunities for growth remain abundant

Over 2016-2022, the cybersecurity market ran at +14.5% CAGR to reach USD180bn globally. We consider the market should continue growing at a near 12% rate from 2023e onwards, to eventually reach USD440bn by 2030e.

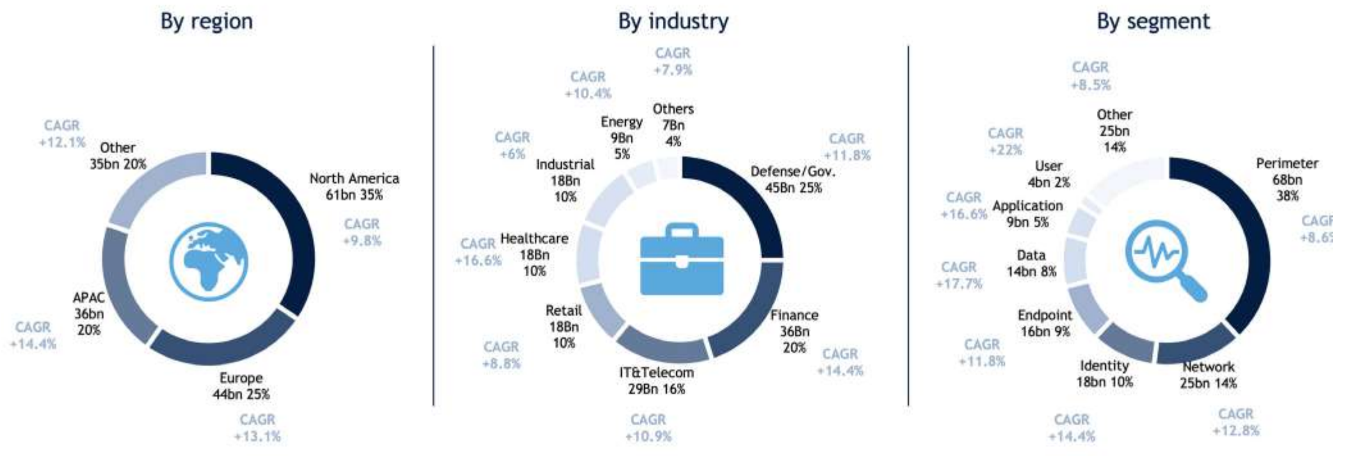
FIG 26: CYBERSECURITY MARKET SIZE EVOLUTION AND FORECAST



Source: Stifel*

The slowdown in market growth we anticipate reflects both the growing maturity stage of the market and a degree of conservatism on our side. We break down these estimates by geography, application and segment.

FIG 27: CYBERSECURITY MARKET BREAKDOWN BY REGION, APPLICATION AND SEGMENT



Source: Stifel*

- North America and Europe represent the two biggest markets.

- However growth is mainly expected to come from Asia Pacific and Europe, and not North America, contrary to what we have observed in the past. This is due to the maturity of the American market versus the lag that Europe and APAC need to catch up.

- We estimate that North America will account for 30% of the total market by 2030, 27% for Europe and 24% for APAC.

- Government spending occupies the top position due to its primordial importance in defence and we expect to it to remain at a fourth of the market.

- Finance, due to its high-stake nature and numerous regulations comes second, and we expect it to rise more than the total market, at 14.4%.

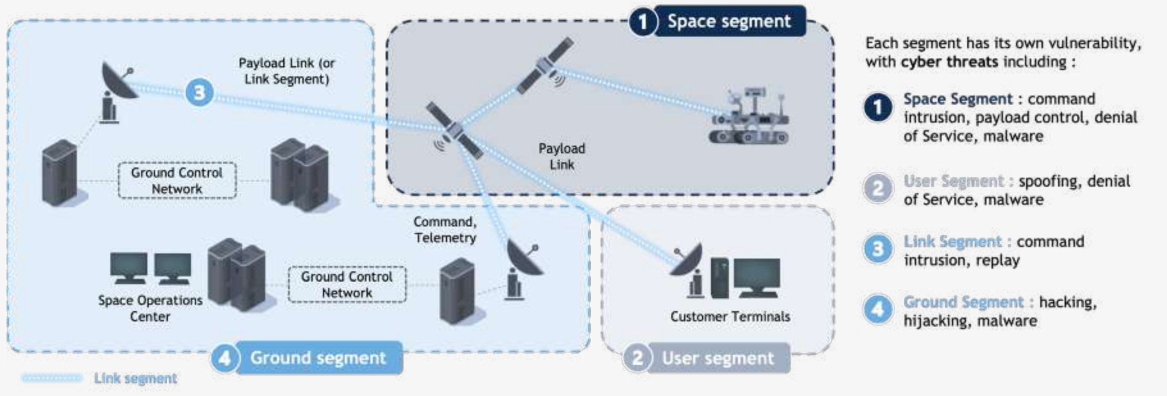
- By segment, perimeter comes first, with 38% of the market.

- Data, application and user segments are relatively smaller but offer the greatest potential as these technologies address relatively new segments.

CYBERSECURITY IN SPACE

New technologies are driving new forms of threats, even up in the sky. Indeed, satellites and the space-based services they provide are increasingly crucial to our modern economy and geopolitics and being in orbit doesn't mean being out of reach of attack. Besides anti-satellite (ASAT) weapons blowing up the hardware in orbit, cyberattacks are now tangible and harmful options for attackers. While, legacy space assets were based on expensive proprietary technologies, NewSpace technologies are relying on more common hardware and software components, opening up "terrestrial-like" IT vulnerabilities. A concerning illustration is Russia's deliberate cyber-attack on ViaSat's KA-SAT network in February 2022. Unprepared for such an attack, ViaSat saw its modems being affected all across Europe. Starlink satellites also underwent jamming attempts from Russia in the beginning of the Ukrainian war in 2022, but thanks to the company's ability to update satellite software within a few hours, Starlink was able to prevent the constellation from going down. China is also reportedly building sophisticated cyber weapons to seize control of enemy satellites, rendering them useless for data signals or surveillance during wartime. Beyond potential disruption to Internet services, loss of connectivity can disable remotely controlled systems and disrupt air transport, road traffic and shipping, while interference with satellite imagery services can compromise military intelligence and invalidate scientific studies by altering their source data. SSA data could also be targeted, artificially altering debris collision forecasts and causing direct harm to critical space systems. All of this can be achieved without firing a single rocket. The challenge is thus to ensure end to end protection of highly complex space systems that are distributed by nature, combining on premise (user segment), cloud (ground segment) and edge (space segment) computing environments.

FIG 28: CYBERSECURITY SOLUTION PROVIDERS FOCUSED ON THE SPACE SEGMENT


1 Space segment
Payload Link (or Link Segment)
3
Ground Control Network
Payload Link
Command, Telemetry
Space Operations Center
Ground Control Network
Customer Terminals
4 Ground segment
2 User segment
Link segment
Each segment has its own vulnerability, with cyber threats including :
1 Space Segment : command intrusion, payload control, denial of Service, malware
2 User Segment : spoofing, denial of Service, malware
3 Link Segment : command intrusion, replay
4 Ground Segment : hacking, hijacking, malware

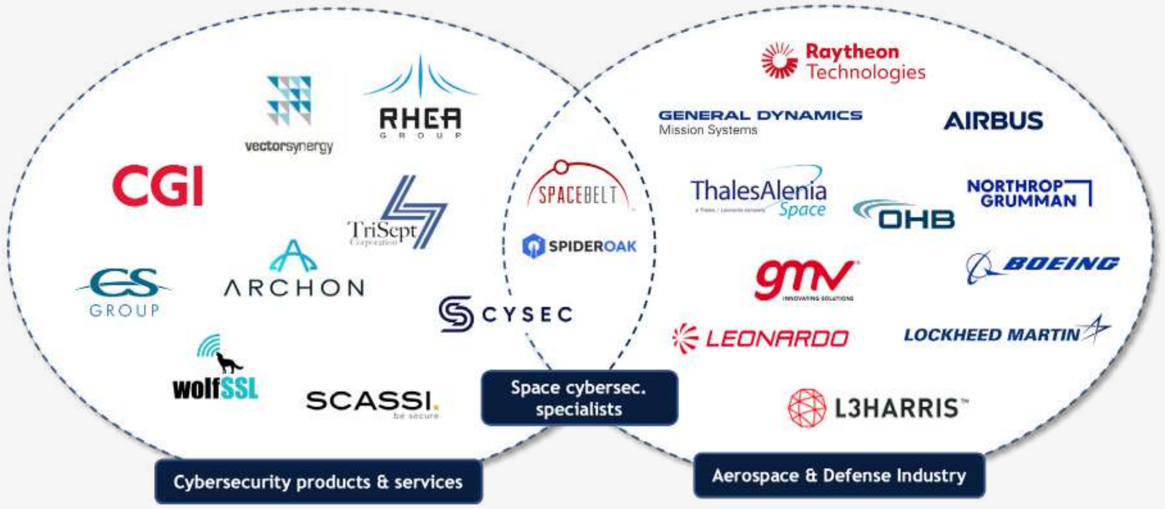
Source: Stifel*

Large organisations (governmental agencies, large satellites manufacturers) cannot afford to stick to traditional proprietary software and hardware architectures, in risk of lagging behind competitors. They need to move from a siloed approach to a zero trust architecture. All space players are to be impacted: satellite operators and distributors, ground segment operators, satellite manufacturers, SSA and In orbit services providers, but also launchers as well as all other players involved in the design, manufacturing and operations of space aircraft. Space cybersecurity encompasses similar dimensions to the terrestrial world, including network protection, detection and response or data encryption. There are significant opportunities laying ahead for IT services specialists with specific expertise in the space sector as well as for technology providers in domains such as network security, cryptographic key management, secure OS for the protection of embedded systems, applications and data, or authentication services.

Addressing concerns will require all players in the space sector to spend an increasing share of budget in cybersecurity services and products. We expect the space cybersecurity market to accelerate sharply in the coming years and forecast a 23% CAGR in spending between 2022 and 2030e to reach nearly USB16bn.

A number of companies are active in the delivery of space cybersecurity products and services. They include major legacy space players, more focused on large scale and governmental programmes, as well as IT services firms and smaller players such as Cysec, Spideroak or Spacebelt, riding on massive opportunities from the development of commercial applications.

FIG 29: SPACE VALUE CHAIN SEGMENTATION



Source: Stifel*

FROM OPS TO DEV, SECURITY IS SHIFTING LEFT

Shift-left security describes developers' efforts to embed cybersecurity within the code they write, i.e., at the earliest stage of program development. From a DevOps perspective, security is therefore moving from the operational stage to the development stage. The idea here is to circumvent attackers' capacity to find and exploit the vulnerabilities that lie within a piece of code. This illustrates, once again, how cybersecurity is moving closer to what needs to be protected: code and data. The fort approach to defending an organization's perimeter is no longer viable.

Modern programming heavily relies on open-source libraries. These libraries are built and maintained by companies or communities of developers who package functions that can be imported into code and used for free, thereby saving users hours of code development. While open-source libraries are convenient, they come with a limited degree of transparency. Non-proprietary resources are not easy to inspect and can potentially contain embedded vulnerabilities of which developers may be unaware. In that sense, open-source content can be a precarious foundation to build upon. Furthermore, even proprietary code can leave behind vulnerabilities, providing hackers with opportunities to exploit them.

As a result, code protection has quickly become a cornerstone of organizations' and software developers' cybersecurity approach. Specifically, the shift-left approach involves conducting extensive security testing before deploying and running the code to ensure its integrity. Companies such as Cast, Code Intelligence, IriusRisk, or Veracode help address these challenges.

The shift-left approach is not limited to code security; it also encompasses Application Programming Interface (API) protection. APIs facilitate data exchange between two systems based on requests, making them a prime target for attacks. Therefore, using encryption, gateways, or vulnerability detection tools is of paramount importance for securing APIs. Firms like Noname or 42Crunch offer solutions to prevent API-related cybersecurity breaches.

Mobile app security can also contain blind-spot vulnerabilities. For example, Guardsquare offers code hardening solutions to prevent attackers from modifying or extracting data from a mobile app's code. Promon has developed app shielding technology to be integrated at the code development stage. For instance, the solution can modify the code in case of a breach attempt to make it understandable to the attacker.

Although the market for shift-left solutions currently represents only a fraction of the total cybersecurity sector, we believe it is poised to experience significant growth in the coming years as developers strive to address the challenges posed by shift-left attacks.

INVESTING IN THE **CYBERSECURITY MARKET**

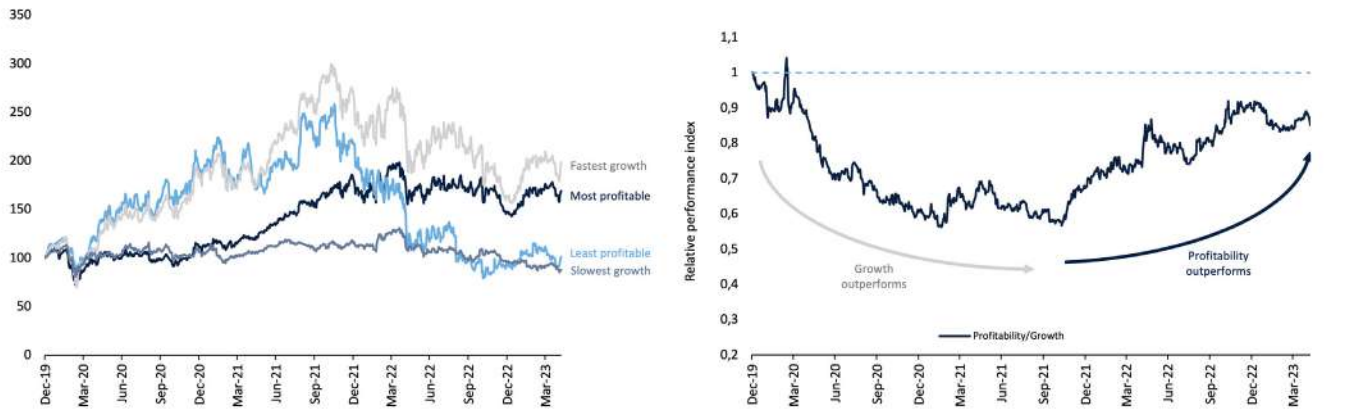
SECTION 4

Cybersecurity investors should consider two parameters: the shift in the valuation paradigm at the sector level and business efficiency at the specific level.

Valuation framework

Publicly-listed cybersecurity names experienced roller-coaster performances over the past three years. Fast-growing unprofitable firms like Crowdstrike or Zscaler skyrocketed on the stock market between Q2 2020 and Q3 2021, before going into meltdown as monetary conditions started becoming more restrictive in early 2022. We observed profitable firms were not as severely impacted by the rate-hike-induced contraction in valuation multiples as investors flew to more qualitative (profitable) names. Indeed, the top tier growth companies (TTG) started underperforming top tier most profitable (TTP) firms in relative terms as of November 2021, as illustrated by the contraction of the TTG/TTP ratio.

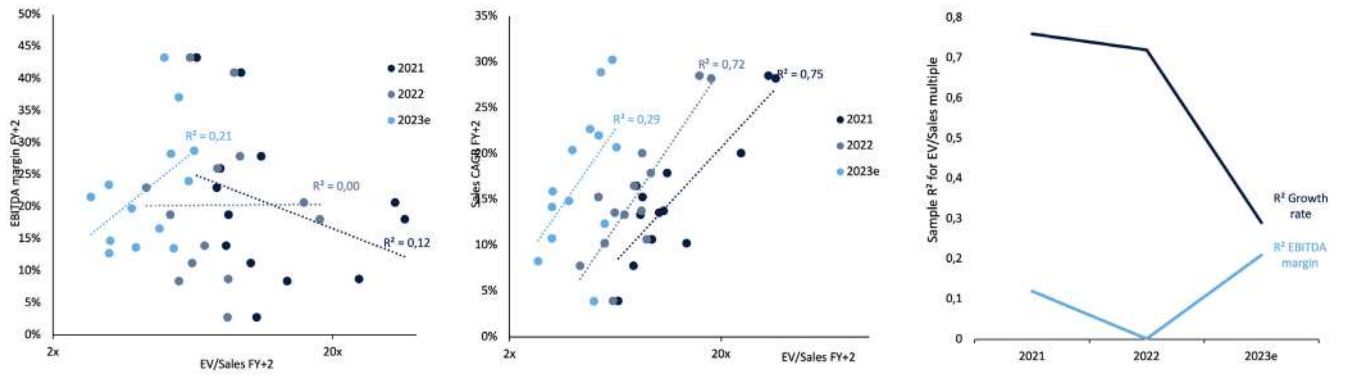
FIG 30: STOCK INDEX PERFORMANCE COMPARISON BY PROFITABILITY AND GROWTH TIER



*Source: Refinitiv; Stifel**

The latter signals a change in the market's attitude towards valuation: while growth at all cost was favoured until late 2021, profitability is clearly more in fashion now. The approach to value a cybersecurity business should therefore take this new paradigm into account. To confirm this assumption, we looked at the correlation between a firm's valuation (comparing its EV to the sales level expected by the consensus at FY+2) and its growth rate as well as the correlation between the valuation multiple and the EBITDA margin expected by the market consensus. We note the coefficient of determination (i.e. R2 representing the relevance the relationship between the two variables) dropped significantly for data involving growth parameters, while it simultaneously soared for profitability metrics after 2022.

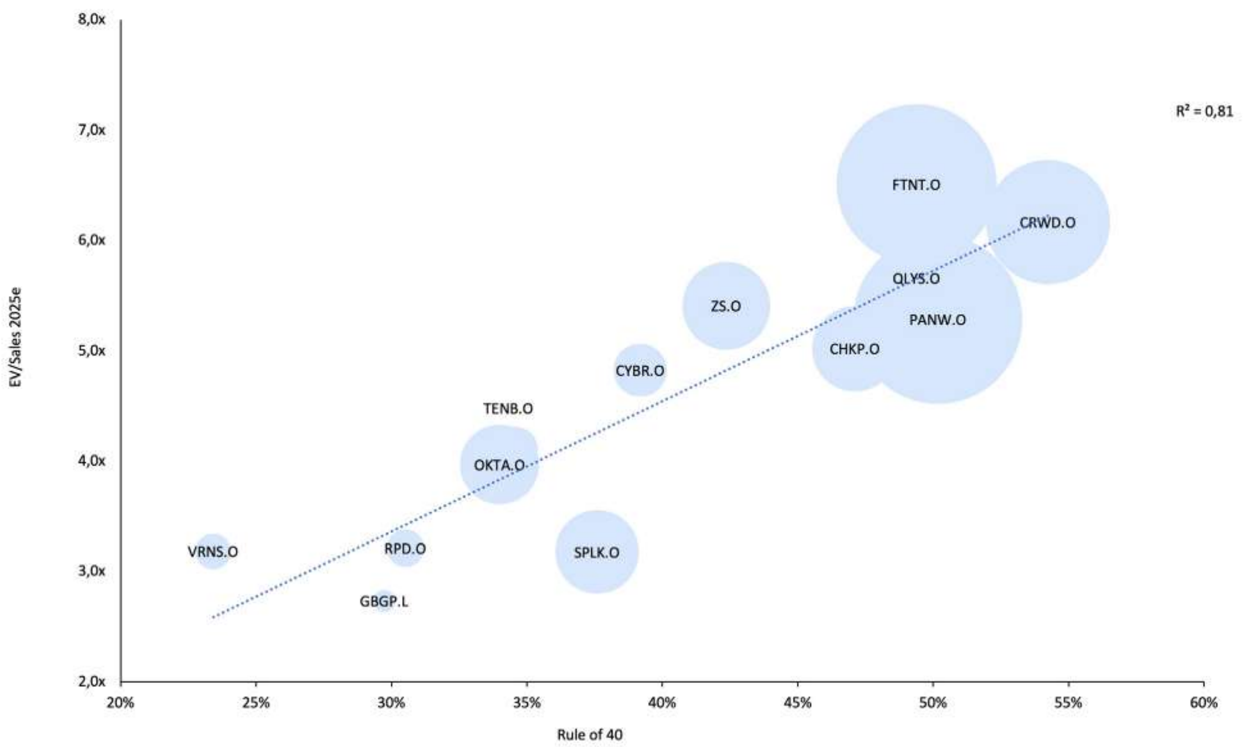
FIG 31: VALUATION MULTIPLES WENT FROM BEING DRIVEN BY GROWTH TO PROFITABILITY



Data set: listed cybersecurity companies average EV/Sales multiples, growth rate and EBITDA margins for 2021, 2022 and 2023
*Source: Refinitiv; Stifel**

These observations confirm that the most relevant determinant for valuing a cybersecurity firm has shifted from being the growth rate to EBITDA margin. We therefore advise investors to pay attention to the profitability levels of the firms they consider. Growth nevertheless remains an important parameter that can be accounted for in a «Rule of 40» valuation metric. The latter consists of summing the expected growth rate of a firm and its EBITDA margin. We see that the Rule of 40 parameter does a great job (R2=0.82) at explaining the valuation level of a firm, as illustrated below (data as of May 2023).

FIG 32: RULE OF 40 IS STILL A RELEVANT VALUATION METRIC



*Source: Refinitiv; Stifel**

Our analysis framework

Assessing the technological edge of a cybersecurity software is a complex task we leave to technical professionals. We nevertheless intend to gauge the efficiency of a business through our own analysis framework. We consider the following parameters should be taken into account when assessing a cybersecurity business:

- Large addressable market.

- Trend capturing: the solution should address the segments facing growing demand.

- Competitive intensity or capacity to differentiate. Competition is considered as a given in the cybersecurity industry, yet we recognise first movers can benefit from a competitive advantage linked with brand image and dataset gathering.

- High recurrence of revenue (Subscription, pay per use or SaaS model).

- High net retention rate or low churn rate among the customer base.

- Embracing the platform strategy. Cybersecurity platforms are likely to grab market share form traditional, focused competitors.

- Capacity to develop or replicate new technologies through R&D to remain competitive.

- Operational efficiency of R&D and sales & marketing efforts (high marginal revenue per R&D or S&M spending).

- Profitability or path towards profitability.

- M&A activity in a segment should also be considered for investors seeking an exit plan.

We consider EDR, identity or user focused solutions are currently hot topics in the market. We recall the move towards integrated platform is a key trend in the sector that cannot be avoided. Players lagging behind in terms of platform integration are exposed to high disruption risk.

Interviews

We conducted several interviews with private equity and venture capital investors to discuss the trends defining the cybersecurity market and the company-specific factors that drive their investment decisions. We summarised the key takeaways of our conversations in the following section.

CYLON | ventures

Interview with Grace Cassy, co-founder of Cylon Ventures - British Venture Capital investor typically participating to pre-seed and seed rounds globally with a focus on cybersecurity firms.

The market for cybersecurity remains resilient as there are still a lot of deals being made, despite the economic uncertainties. Cyber threats are still there, and organization need to equip themselves.

According to our interlocutor, the percentage of IT budget spent on cybersecurity overall could sit around 20% and could easily expand further.

The move towards platforms was described as complex process: "there is constant tension between best of breed and best of suite, but at the moment it is probably leaning to best of suite and a movement towards platforms to have a simpler stack and fewer products."

That being said, as threats are constantly evolving, "there is always a need for new solutions and innovations, which is easier in smaller teams, that are more agile, can be more responsive to threats", so it is likely that "there will always be a flow of new startups addressing specific problems which will over time become integrated into platform suites."

AI is definitely a big theme throughout the industry but "like any general-purpose technology, and you could say the same of quantum computing as well as AI, it can be used by people with bad intents as well as defenders". "It is probably going to make phishing at scale more effective and with higher hit rate, especially when using generative AI". Companies must also pay close attention to the safety of the AI they use and make sure it cannot be hacked or tampered with.

Quantum computing is a longer-term theme but it is likely to happen sooner than many expects.

Cybersecurity services were out of fashion for the past few years as investors sought products' attractive unit economics. Now, tech-enabled services are becoming a key trend in the sector, as users want to consume more security products that come with a range services.

The key parameters driving the investment decision include the segment of the market that the solution addresses, the uniqueness of this solution, its ability to differentiate from its competitors, which often comes down to the team's background, experiences, and execution capacity. Additionally, a "low friction to adoption" (i.e., can the solution integrate quickly and easily, does it need a lot of architectural adjustments?) was mentioned as a key parameter in assessing a business' quality.

In such a fragmented market, having a good IP is an important matter, but companies must not neglect the importance of having a strong Go-To-Market strategy and a commercial execution capacity.

The high valuation multiples of 2021 ended up reconnecting with the fundamentals and actual industry prospects. They fell by about 20-30% since those peaks, to more reasonable, yet hefty levels.

evo/ution
EQUITY PARTNERS

Interview with Richard Seewald, Founder & Managing Partner and Karel Obluk, Partner at Evolution Equity Partners – American venture capital investor with global reach.

The past 20 years have highlighted a clear correlation between market downturns and increase in cyberattacks and fraud. In the wake of Covid-19, followed by a period of increased geopolitical tensions and economic slowdown, the risk of seeing a new surge of cyberattacks is very high. The main characteristics of new attacks are a higher sophistication, velocity, funding and frequency, making them even more dangerous. Adversarial nation state activity is on the rise.

While the cybersecurity sector is one of the most recession-proof industries, this is not entirely the case. Best of breed platforms with suites of complementary products are better equipped than others to fend off budgetary constraints and will utilize the cycle to consolidate their position. – Palo Alto Networks is an example of a successful platform strategy implementation. Ultimately, the nature of the adversary and increase in severity of attacks will drive cybersecurity spend and not the economic cycle.

Cybersecurity solutions using artificial intelligence (AI) and machine learning (ML) have been around for more than a decade. What is new however is their efficacy and viability as they are improving at a very rapid pace. Particularly when it comes to detection and response, AI has progressively become very effective in this area.

Generative AI made AI and ML mainstream and easier to use, both for defenders and attackers. Tracking and protecting vulnerabilities is therefore more critical than ever. Shift-left solutions are hence becoming a key part of the security stack. "Providing developers with the tools and infrastructures to enable a safe development environment is foundational to a safe developer ecosystem. The whole shift-left phenomenon has also raised the tension in the supply chain, and how code and software is distributed throughout the ecosystem."

An example of a market that did not exist a few years ago is the cybersecurity risk rating category. Companies like Security Scorecard which rate the level of cyber risk a company faces, are becoming mission critical for all organizations including insurance and finance.

The human factor weakness is definitely starting to be understood by companies, as awareness and training is booming on the matter. Yet the ability to test and quantify the improvements in behavior before and after the training is still a missing layer. Indeed, training staff to tackle cybersecurity challenges is not a one-off exercise and continued analysis should be part of the process.

Evolution Equity Partners is a multi-stage cybersecurity investor focused primarily on growth and early growth stage companies. Quality of team, technology and total addressable market drive attractiveness of opportunities that we invest in.

One of the critical tasks for cybersecurity companies to navigate the market turmoil will be to manage a pathway to profitability while building growth opportunities. The challenge is to identify the right products and solutions to maintain a balance where Revenue Growth, Net Retention and Gross Retention are the most important factors. This is the «Goldilock Zone» that will be navigated successfully by the companies that will emerge as winners during the next several years. As we eventually turn the corner on this part of the cycle and we see the next generation of cybersecurity companies go public, mastering the Goldilock Zone will differentiate the winners from the others.

Rule of 40 is really just another way to speak about EBITDA and EBITDA margin, as private companies are often still on their pathway to being EBITDA positive". Investors should therefore focus on the art and science of a firm's ability to balance growth and profitability at the same time.

INSIGHT
PARTNERS

Interview with Thomas Krane, Managing Director at Insight Partners – a New York-based global software investor focused on software startup and ScaleUp companies with a large number of cybersecurity portfolio companies globally.

There is a general trend toward platforms, however, the appeal of best-of-breed solutions is definitely not going to disappear. Some users will still want the best possible protection, whatever the cost and the complexity of implementing it; and platforms are unlikely to be the best in every segment. "There is now more than ever, a resilient push towards staying with best of breed, mainly because cloud-native security has become so mainstream," which alleviates some of the needs for platforms.

Going too far with platforms implies two issues: a risk of "vendor lock-in," where clients would become dependent with too high switching costs, and a potential for sluggish innovation pace. However, "if you do not have anything, a platform could be a strong baseline strategy, but as you go into more depth, you will find that if you really want to have the most effective strategy, you will have to go for best-of-breed." A median way would consist in fostering integration of solutions via APIs, letting users build their own platforms.

The Shift-Left segment (which refers to code and application supply chain security) is described as a key trend. Indeed, code is no longer built from scratch, it is assembled and consolidated using various sources like open-source code, packages from third part apps, etc. The recent trends in coding consolidation and flexibility are progressing and vulnerabilities are progressing in line, triggering the need for greater code protection.

Insight Partners does not rigidly target any specific segment of the cybersecurity market. They use a bottom-up approach, looking for the best companies within the universe. But that being said, "it is informed by big secular trends." Recently, the market has slightly toughened, with sales cycles becoming longer, and more scrutiny being placed on each transaction, but ultimately the demand is still there, organizations are still buying the solutions they need.

Regarding the company-specific factors, "ultimately, it boils down to what are the fundamental inputs of profitability potential, namely gross margin, gross retention, and sales & marketing efficiency. Anything else, if it really is a SaaS company, can be throttled, without it being strongly negative."

The market today is focused on ScaleUps, the transition from early adopter to mainstream. Hence, key performance indicators to look at are "the signals of very clear, established and repeatable product market fit." This can put a flywheel in place, ultimately driving demand side economies of scale: "the more customers you get, the better the solution becomes, therefore you build various barriers to entry naturally." A great sign is when a company has a high transaction volume, driven by the addition of new contracts every quarter, "ideally without the founder being involved," indicating a great product market fit.

In terms of valuation, the market was asking for growth at all costs, but that changed overnight and profitability entered into the equation. As mentioned by Thomas, "we do not try to manage all of our companies to be exactly in line with the R^2 correlation chart of FCF + growth rate of the public market at any given time." However, profitability potential remains a key focus.

TempoCap

Interview with Damien Henault, Partner at TempoCap – a UK-based private equity investor focused on scale-ups with eleven participations in cybersecurity firms across Europe and the US.

On the debate between best of breeds and platforms, as "the innovation pace is set by the attack side and it is moving very fast", the cybersecurity industry will always need agile best of breed players to match the new needs, rendering the absolute shift towards platforms unlikely. In reality, even though platforms are on the rise, both approaches should continue to coexist while a constant flow of new best of breed players join integrated platform players seeking to diversify their offering.

Smaller organisations would find the ubiquitous platform approach most appropriate as they generally lack dedicated cybersecurity teams to assemble and maintain a patchwork of best of breed solutions, while they also have smaller attack surface to secure. Those smaller companies are also more likely to use managed services in addition to platforms.

A non-negligible benefit of platforms for cybersecurity companies is their ability to realize cross- and up-selling through their existing clients, as acquiring new logos can be challenging, creating a virtuous cycle in the process, strengthening sales, growth and retention.

Our interlocutor also discussed the idea of a tiered move towards platforms. The first level being the move towards ubiquitous integrated platforms offering comprehensive cybersecurity capacities ranging from perimeter protection to identity management. The second level being a platformisation at the sub-segment level, where players would create dedicated and specialised platforms addressing most use cases of the Identity Access Management segment for example. Platforms can therefore cover the entire value chain while others focus on specific subsegments, and both have seen an acceleration in recent years.

"Cybersecurity is probably the most resilient and recession-proof segment of IT, but it would be foolish to say it is totally recession-proof." Indeed, we are most likely going to observe a strong differentiation from the CISOs between the "must-have" and the "nice-to-have" solutions as mission-critical tools should continue to be in high demand. However, the way the macro pressures evolve, there will probably be some attrition and pressure on ARR during renegotiations.

Q1 2023 has been quite a repeat of Q4 2022, with a contraction in demand and longer sales cycles. Q2 2023e could be in the same dynamic considering the current market environment. However, H2 2023e might see a rebound as cybersecurity spending YTD remain below 2023 budgets and could catch up, especially if the macroeconomic challenges ease throughout the year.

Regarding the drivers of an investment decision, the strength of the IP was mentioned a key parameter. Best IPs are typical consolidation targets but also potential consolidators if they manage to scale their solution and develop addons.

"Given the market reset in valuation, there is an opportunity as valuations decreased quite sharply" The market for M&A should therefore remain active and liquid for the best firms.

TIKEHAU CAPITAL

Interview with François Lavaste, Executive Director at Tikehau Capital, and Partner in the cybersecurity and digital trust private equity investment team typically financing EUR10-50m per round, mostly in Europe. Tikehau Capital is a global alternative asset management group with EUR39.7 billion of assets under management (at 31 March 2023). Tikehau Capital has developed a wide range of expertise across four asset classes (private debt, real assets, private equity and capital markets strategies) as well as multi-asset and special opportunities strategies.

The move towards platforms is real and is reflecting a long-term consolidation trend but it is mainly being pushed and advertised by the big cybersecurity companies who themselves run platforms. In fact, the market is still more a balance between best of breed technologies and platforms. That situation should remain as best of breed solutions will continue to emerge, initiated by innovators before they eventually get acquired by platforms or themselves enlarge their feature set to become platforms.

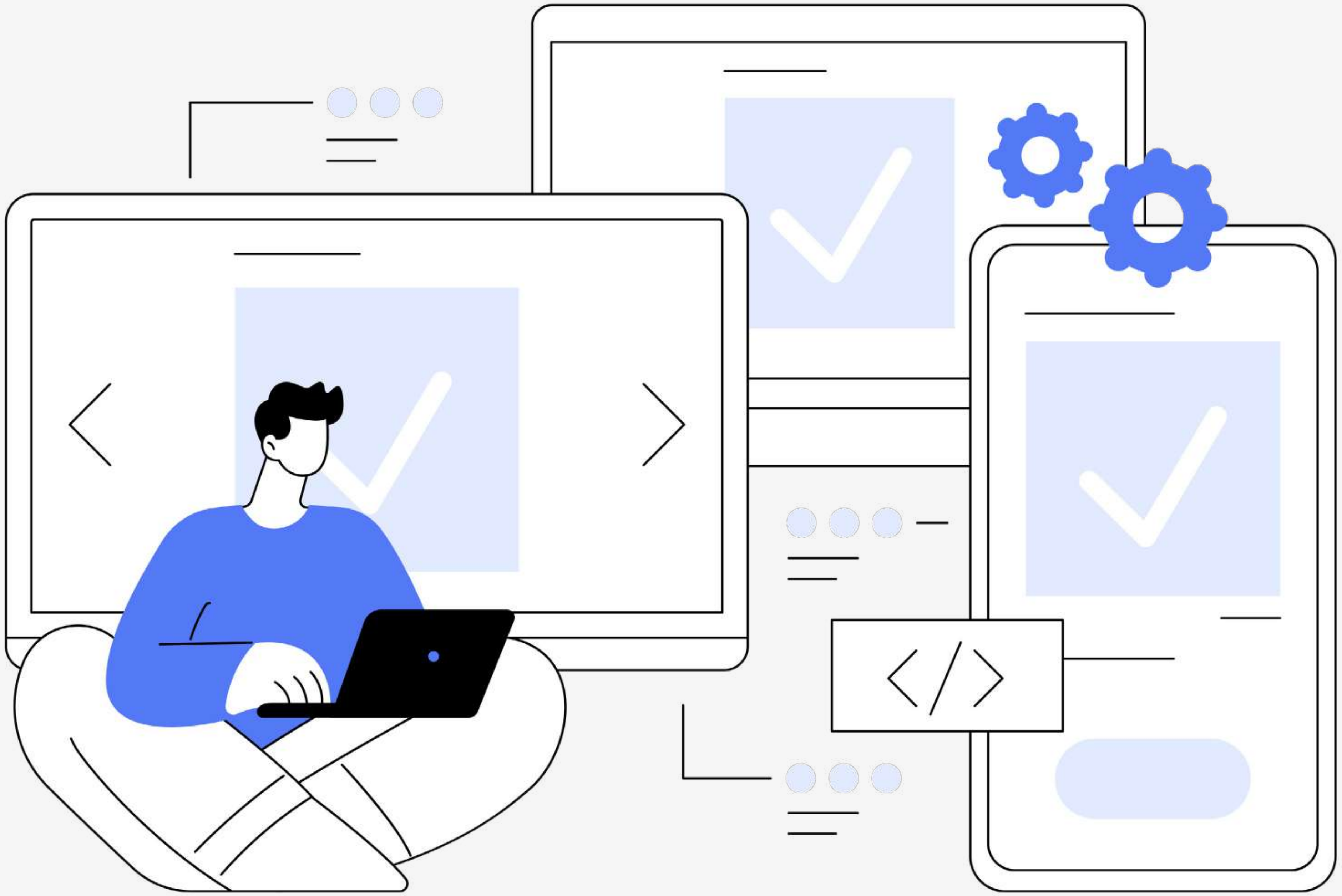
Training & awareness was discussed under the angle of professional cybersecurity staff education. The current deficit of cybersecurity experts is estimated at around 3 million positions to be staffed in cyber globally. We also see several new cybersecurity schools being launched that should in the end improve professional training and solve part of the staff shortages issue. Focusing on technologies to incorporate cybersecurity by design or stopping phishing attempts before users are exposed to them for example, should be the priority instead of training people to spot them.

The cybersecurity market is already expanding into adjacent domains like fighting disinformation, detecting fake news or preventing financial fraud.

"Shift-left" is another major trend in the sector, this trend addresses the need to secure technology infrastructure and applications in the design and coding phase. Four segments were identified, namely code security, application security, API security, and DevSecOps (Development Security Operations).

"We have seen a lot of consolidation in the services and consulting space because of the lack of resources. In that domain, the fastest way to grow is not just to try to hire more people but to acquire competitors". Products and services are often thought as two different buckets, but companies building their own technology and adding a layer of service should offer interesting opportunities, like security managed services.

In terms of valuation, growth remains the number one metric, particularly in the private market, whether through revenue or, even better, ARR. But of course, profitability prospects, gross margin levels, churn rate, net retention, CAC, S&M efficiency as well as return on funding in the case of privately-held companies, were considered important metrics too.



The cybersecurity market is driven by the significant mismatch between the risks posed by cybersecurity breaches and the means implemented to prevent them. Although the number, complexity and magnitude of cyberattacks grows exponentially, their total cost largely exceeds the amount spent by organisations to prevent cybercrime. Thus, there is no doubt that demand for cybersecurity solutions should continue growing in the future.

But investors should not buy cybersecurity assets blindly as the rapidly changing environment makes the market largely unpredictable. We therefore recommend focusing on long term trends, as well as on the business' operational efficiency. From a valuation standpoint, investors should bear in mind that growth is no longer the north star of valuation, as profitability has now become the key parameter to determine an asset's valuation multiple.

M&A activity in the sector should remain buoyant as the move towards platform induces consolidation among solutions providers. Furthermore, promising early stage technology should continue to attract capital as the market remains highly competitive.

Finally, investors should not disregard the disruption risk posed by hyper-scalers and software providers. The likes of Azure (Microsoft), AWS (Amazon) or GCP (Alphabet) have long been pointed as potential disruptors of the cybersecurity market as they edit or host a large part of the most commonly used software in the world. Although this threat has remained dormant so far, the move towards platform could waken their interest for developing and distributing their own solutions alongside other services, as hinted at by the development of their marketplaces.

Lexicon

CISO (Chief Information Security Officer): person in charge of assuring cybersecurity in an organisation. Malware: a type of software designed to infect a device or network in order to harm, disrupt or steal user information.

Crypto-jacking: hijacking a computer to use it to mine cryptocurrencies for the originator

Denial of service (DoS): attacks designed to overwhelm a system or network, e.g. a website, and make it inaccessible.

Detection fatigue: number of false positive alerts on the total number of potentially malicious behaviours detected by a cybersecurity solution.

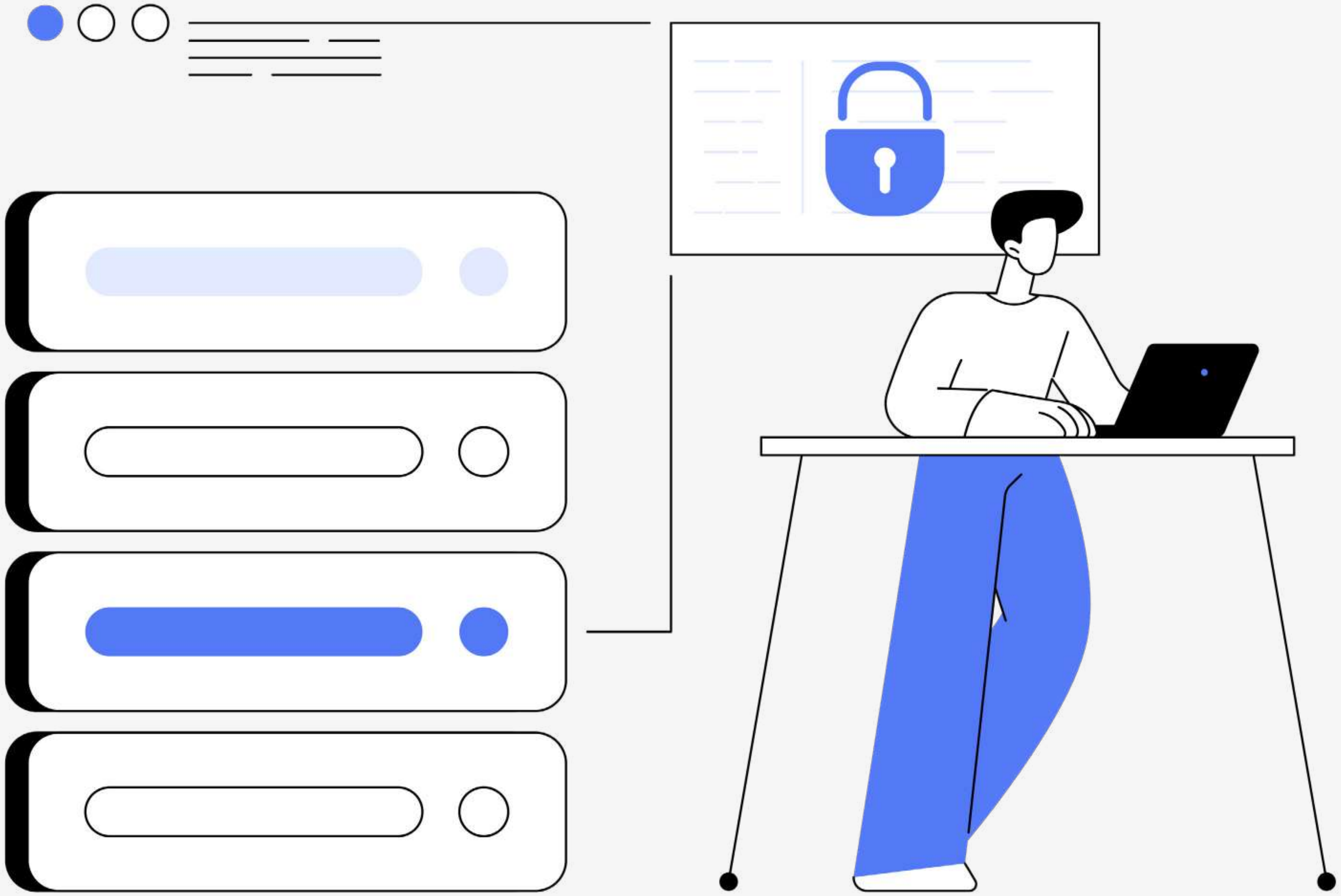
Man in the middle (MitM): attacks perpetuated when the attacker intercepts a communication and alters it to his advantage, for example to steal sensitive information.

MSSP (Managed Security Service Provider): offers outsourced security solutions to organisations.

Phishing: a social engineering attack which intends to trick victims into providing sensitive information such as login credentials, credit card information etc, by usurping the identity of someone else or a website, an organisation, the government... through emails, messages, websites.

Ransomware: a malware designed to block access to a system's data and offers to unblock it against payment, before a deadline whereby all data is lost or leaked publicly.

Spyware: a type of malware that secretly installs itself inside a system, to steal personal data such as credit card information, login credentials etc.



STIFEL | IRIS

WHITE PAPER **AUTHORS**

AURELIEN DESIDE
Analyst
Paris
aurelien.deside@stifel.com

RECENT **TRANSACTIONS**

metaco
Acquired by
ripple
$ 250 000 000
May 2023
Sole Financial Advisor to the Sellers

BRAINWAVE GRC
Acquired by
RADIANT LOGIC
Portfolio company of
TA ASSOCIATES
Undisclosed
April 2023
Sole Financial Advisor to the Sellers

MAILINBLACK
Acquisition of a majority stake by
Apax PARTNERS
NEW ALPHA
Undisclosed
July 2022
Sole Financial Advisor to the Sellers

vade
Investment from
TIKEHAU ACE CAPITAL
bpifrance auriga
€ 28 000 000
May 2022
Sole Financial Advisor

Bridgepoint Development Capital
Contemplated Investment in
CAST
€ 139 000 000
May 2022
Sole Financial Advisor to Bridgepoint

SWORD GRC
Acquired by
riskonnect
Portfolio company of
TA ASSOCIATES
Undisclosed
February 2022
Sole Financial Advisor

kompany
Acquired by
MOODY'S
Confidential
March 2022
Sole Financial Advisor to the Sellers

PARQUEST CAPITAL
Minority investment in
aDvens
Undisclosed
September 2021
Sole Financial Advisor to the Investor

EclecticIQ
Private Placement (Follow-on)
€ 15 000 000
September 2021
Sole Financial Advisor
and Sole Placement Agent

METSYS
Investment from
EUROPEAN DIGITAL GROUP
Undisclosed
March 2021
Sole Financial Advisor to the Sellers

LEGAL **DISCLAIMER**

This white paper is provided on a confidential basis for informational purposes only and is not intended to, and does not, constitute a recommendation with respect to any potential transaction or investment. Any opinions expressed are solely those of Stifel and applicable only as at the date of this white paper. This white paper is necessarily based upon economic, market, financial and other conditions as they exist on, and on the information made available to Stifel as of, the date of this white paper, and subsequent developments may affect the analyses or information set forth in this white paper. This white paper does not purport to give legal, tax or financial advice. Recipients should not rely on the information contained in this white paper and must make their own independent assessment and such investigations as they deem necessary. Stifel is not soliciting any action based upon this white paper. This white paper does not constitute or form part of any offer or invitation to sell, or issue, or any solicitation to any offer to purchase or subscribe for, any shares, financial instruments, or other securities, nor shall it (or any part of it), or the fact of its distribution, form the basis of, or be relied on in connection with or act as any inducement to enter into, any contract whatsoever relating to any securities, financial instruments or financial services of Stifel or of any other entity or constitute an invitation or inducement to any person to underwrite, subscribe for or otherwise acquire securities. The information in this white paper is not complete and is based upon information that Stifel considers reliable, but it has not been independently verified. Stifel does not represent, guarantee, or warrant, expressly or implicitly, that this white paper or any part of it is valid, accurate or complete (or that any assumptions, data or projections underlying any estimates or projections contained in the white paper are valid, accurate or complete), or suitable for any particular purpose, and it should not be relied upon as such. Stifel accepts no liability or responsibility to any person with respect to or arising directly or indirectly out of the contents of or any omissions from this white paper.

The distribution of this white paper may be restricted by law. Accordingly, this white paper may not be distributed in any jurisdiction except in accordance with the legal requirements applicable to such jurisdiction. Persons into whose possession this document comes are required to inform themselves about and to observe any such restrictions. This white paper is only be addressed to and directed at specific addressees who: (A) if in member states of the European Economic Area (the “EEA”), are persons who are “qualified investors” within the meaning of Article 2(e) of Regulation (EU) 2017/1129 (as amended) (the “Prospectus Regulation”) (“Qualified Investors”); (B) if in the United Kingdom, are Qualified Investors within the meaning of Article 2(e) of the Prospectus Regulation as it forms part of domestic law by virtue of the EU (Withdrawal) Act 2018 (as amended from time to time) and who are: (i) persons having professional experience in matters relating to investments who fall within the definition of “investment professionals” in Article 19(5) of the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005 (the “Order”); or (ii) high net worth entities falling within Article 49(2)(a) to (d) of the Order; or (C) are other persons to whom it may otherwise lawfully be communicated (all such persons referred to in (B) and (C) together being “Relevant Persons”). This white paper must not be acted or relied on in (i) the United Kingdom, by persons who are not Relevant Persons; (ii) in any member state of the EEA by persons who are not Qualified Investors; or (iii) in the United States (“U.S.”) by persons who are not Qualified Institutional Buyers (“QIBs”) as defined in and pursuant to Rule 144A under the U.S. Securities Act of 1933, as amended. Any investment activity to which this white paper relates (i) in the United Kingdom is available only to, and may be engaged in only with, Relevant Persons; (ii) in any member state of the EEA is available only to, and may be engaged in only with, Qualified Investors; and (iii) in the U.S. is available only to, and may be engaged in only with, QIBs. If you have received this white paper and you are (A) in the United Kingdom and are not a Relevant Person; (B) are in any member state of the EEA and are not a Qualified Investor; or (C) are in the U.S. and are not a QIB, you must not act or rely upon or review the white paper and must return it immediately to your Stifel representative (without copying, reproducing or otherwise disclosing it (in whole or in part).

No person shall be treated as a client of Stifel, or be entitled to the protections afforded to clients of Stifel, solely by virtue of having received this document.

This white paper was produced by Bryan, Garnier & Co Limited, prior to the acquisition by Stifel Financial Corp; some contributors may have since left the organisation.

INDEPENDENCE OF RESEARCH

Stifel prohibits its employees from directly or indirectly offering a favourable research rating or specific price target, or offering to change a rating or price target, as consideration or inducement for the receipt of business or for compensation.

BASIS OF PRESENTATION

References herein to “Stifel” collectively refer to Stifel, Nicolaus & Company, Incorporated, Stifel Nicolaus Europe Limited (“SNEL”), Stifel Europe AG (“STEA”), Stifel Europe Advisory GmbH, Stifel Nicolaus Canada Incorporated, Bryan Garnier & Co Limited, Bryan Garnier Securities SAS, Bryan Garnier & Co GmbH, Bryan Garnier & Co AS and other affiliated broker-dealer subsidiaries of Stifel Financial Corp. SNEL and STEA also trade as Keefe, Bruyette & Woods (“KBW”)). For a list of Stifel affiliates and associated local regulatory authorisations please see here: www.stifel.com/disclosures/emaildisclaimers. References herein to “Stifel Financial” refer to Stifel Financial Corp. (NYSE: SF), the parent holding company of Stifel and such other affiliated broker-dealer subsidiaries. Unless otherwise indicated, information presented herein with respect to the experience of Stifel also includes transactions effected and matters conducted by companies acquired by Stifel (including pending acquisitions publicly announced by Stifel), or by Stifel personnel while at prior employers.

If you no longer wish to receive these marketing communications, please e-mail StifelEurope.GDPR@stifel.com and we will arrange to have you taken off the relevant mailing list(s).

www.StifelEurope.com

STIFEL | IRIS

INTELLIGENCE • RESEARCH • INSIGHTS • SERVICE

LONDON, UNITED KINGDOM

Stifel Nicolaus Europe Limited
150 Cheapside
London, EC2V 6ET

T: +44 20 7710 7600

FRANKFURT, GERMANY

Stifel Europe AG
Kennedyallee 76
60596 Frankfurt am Main

T: +49 69 788080

LONDON, UNITED KINGDOM

Bryan Garnier & Co Limited
Michelin House 81 Fulham Road
London, SW3 6RD
Tel: +44 20 7332 2500

T: +49 89 2422 62 11

PARIS, FRANCE

Bryan Garnier Securities SAS
26 avenue des Champs-Elysées
75008 Paris

T: +33 1 56 68 75 00

PARIS, FRANCE

Stifel Europe AG – Paris Branch
80 Avenue de la Grande Armée
75017 Paris

T: +33 1 7098 3940

FRANKFURT, GERMANY

Stifel Europe Advisory GmbH
Bockenheimer Landstrasse 24
60323 Frankfurt am Main

T: +49 69 247 4140

MUNICH, GERMANY

Stifel Europe AG – Munich Branch
Maffeistrasse 4
80333 Munich

T: +49 89 9992 9820
T: +49 89 2154 6000

MUNICH, GERMANY

Bryan Garnier & Co GmbH
Königinstraße 9
80539 Munich

T: +49 89 242 262 11

MILAN, ITALY

Stifel Europe AG – Milan Branch
Via Privata Maria Teresa, 8
20123 Milan

T: +39 02 85465761

OSLO, NORWAY

Bryan Garnier & Co AS
Haakon VIIs Gate 1, 2nd Floor
0161 Oslo
Postbox: 0117 Oslo

T: +47 908 45 025

ZURICH, SWITZERLAND

Stifel Schweiz AG
Tessinerplatz 7
8002 Zurich

T: +41 43 888 6100

GENEVA, SWITZERLAND

Stifel Schweiz AG – Geneva Office
Place de la Fusterie 12
1204 Geneva

T: +41 22 994 0610

Stifel Nicolaus Europe Limited | Authorized and regulated by the Financial Conduct Authority | Member LSE | www.stifeleurope.com