




Cybersecurity

**A consolidation opportunity
in a red-hot market**

October 2021

kpmg.com/uk



A hand is shown pointing at a digital screen, which displays a blurred image of a city street at night. The background is dark with out-of-focus lights, suggesting a busy urban environment. The hand is in the foreground, and the screen is in the middle ground.

With cyberattacks on the rise and the costs of data breaches spiralling upwards, cybersecurity has become a top board-level priority for companies across geographies, sectors and size-classes. However, choosing the right provider for their needs is a real challenge, as there are literally thousands of providers offering seemingly similar, highly technical services, often with a limited track record. We believe that this fragmented state of the market offers great consolidation opportunities for investors, both strategic and financial. This paper explores the consolidation opportunity at hand and discusses some of the key challenges that a successful consolidator will need to overcome to reap its rewards.



Table of contents

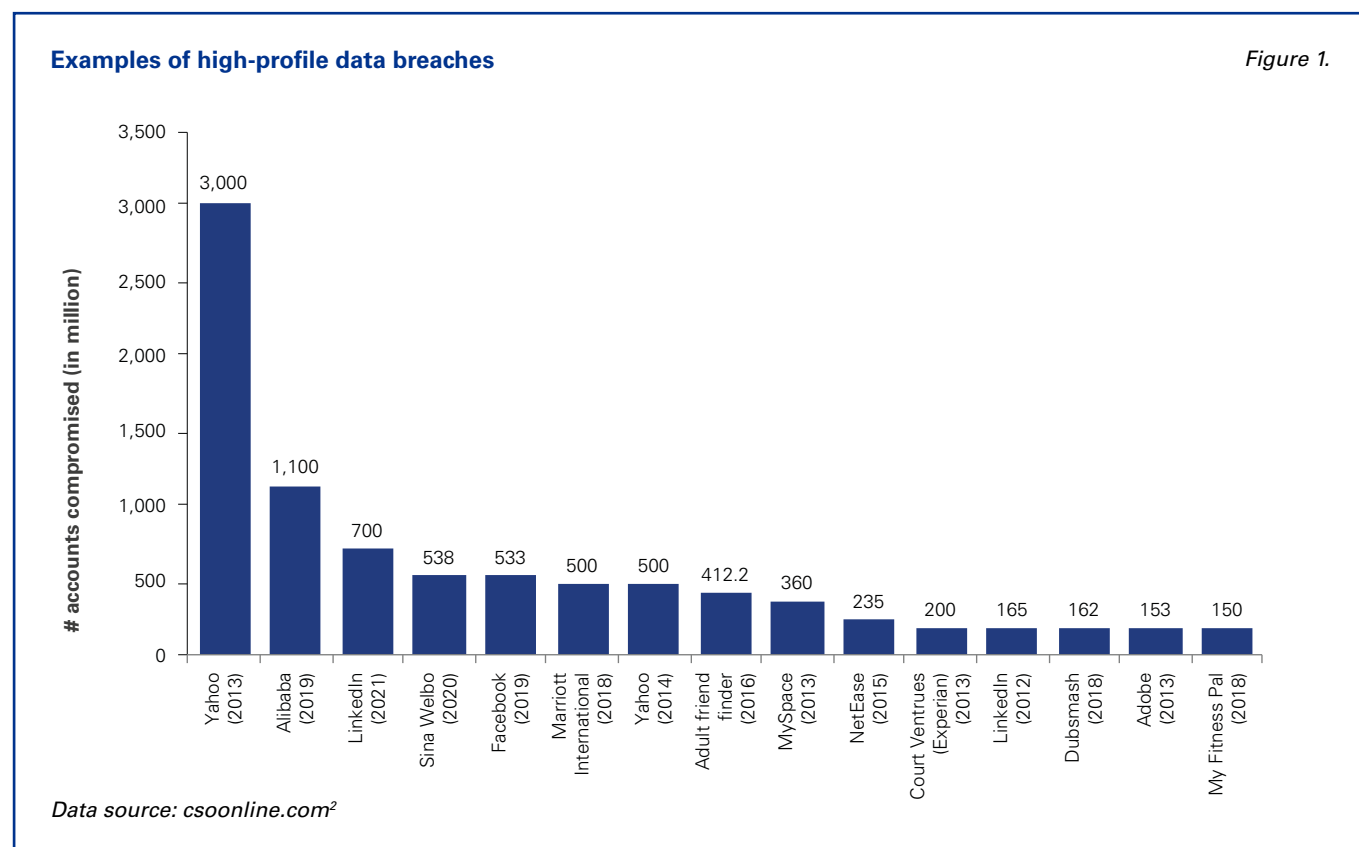
Why is cybersecurity so hot right now?	4
Who are the key players?	10
Why do we think this market will consolidate eventually?	14
What are the challenges in consolidation?	16
What does this mean for investors?	18
Authors and Contacts	19
Sources	20

Why is cybersecurity so hot right now?

In a nutshell, both the probability of being attacked and the costs in the event of a successful attack have risen significantly in recent years, driving demand for cybersecurity solutions across the board.

The number of attacks has been escalating

Cyberattacks have occasionally made headline news for some years now. For example, when Yahoo revealed in late 2016 that more than one billion of its user accounts had been breached – which later turned out to actually have affected more than three billion accounts and to have happened as early as in 2013 – the story made headline news¹. Similarly, the public took the occasional note when other well-known consumer companies such as Facebook, LinkedIn, Alibaba, or Marriott were breached (see Figure 1 for size and time of breaches).



However, while these individual examples may have worried the individual public reader, cybersecurity professionals are more worried by the fact that these are not isolated examples. In fact, there has been a structural trend of an increase in the number of cyberattacks for more than a decade.

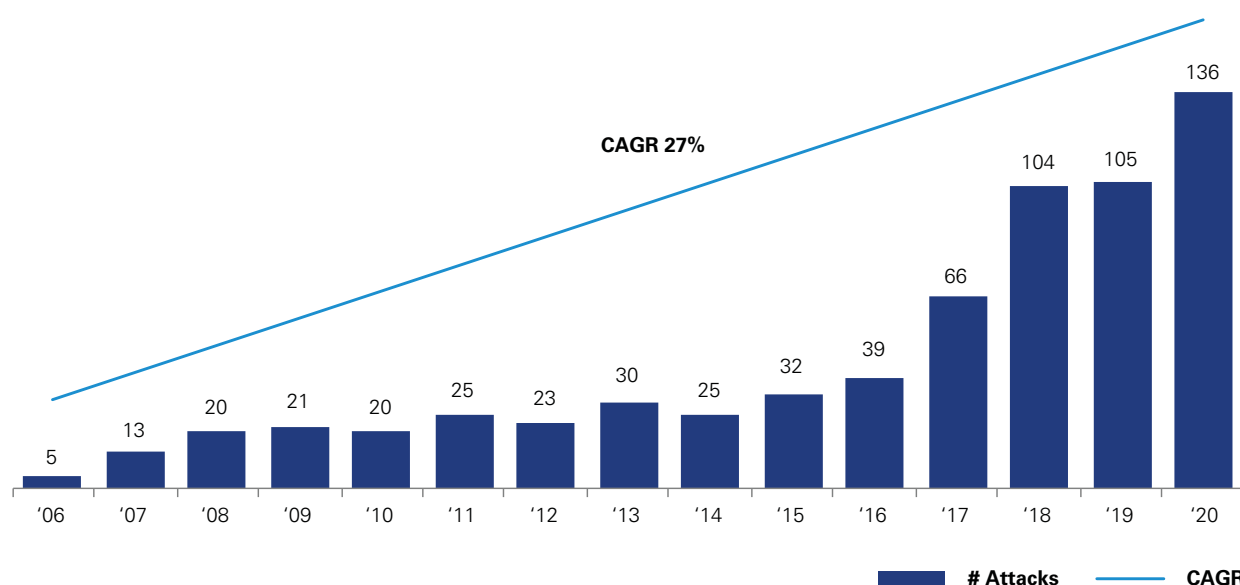
Figure 2 shows the development of the number of significant cyberattacks^a over the past 15 years. These data show two things clearly – first, the number of significant cyberattacks has grown in double digits since at least 2006. And second, their growth rate has accelerated further in the past five years.

^(a) As per the definition of the Center for Strategic and International Studies, considering attacks into a country's government agency, a defence or high-tech company, or a crime with losses of more than USD 1m

Cyber attacks with more than EUR1M reported losses

Number of attacks, 2006-2020

Figure 2.



Data source: Center for Strategic and International Studies³

The damage of attacks is increasing too

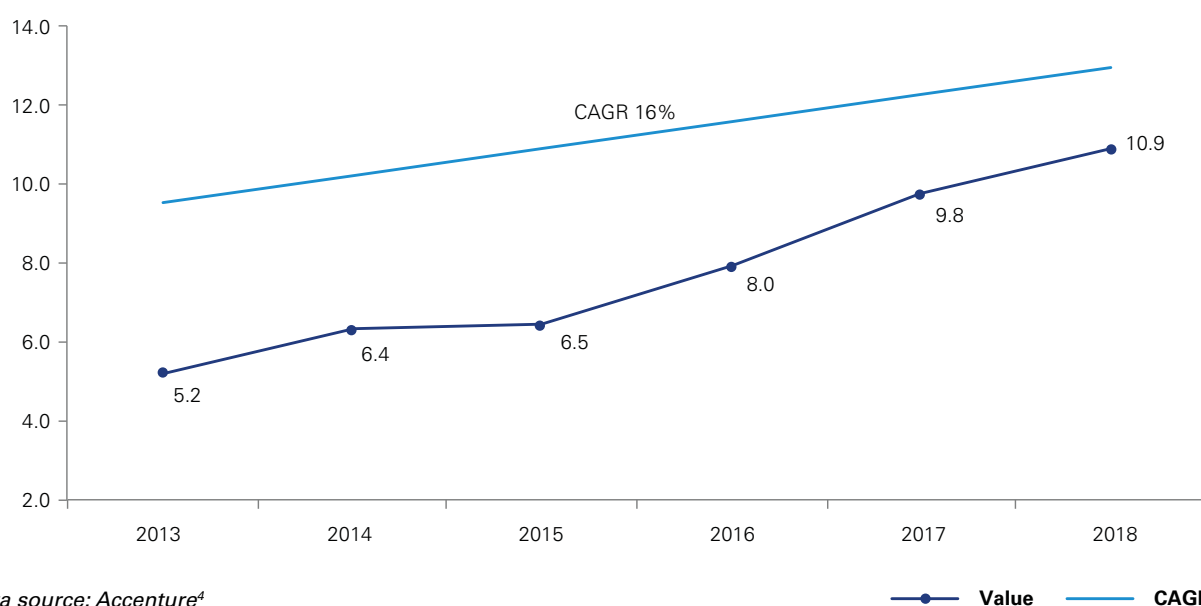
And it isn't just that cyberattacks are becoming more frequent – they are also becoming more damaging from the perspective of their victims.

Figure 3 shows the development of the global average cost of cybercrime per attack as estimated by Accenture. These costs have been growing at a CAGR of ~16%.

Global average cost of cybercrime for companies

EUR/M, 2013-2018

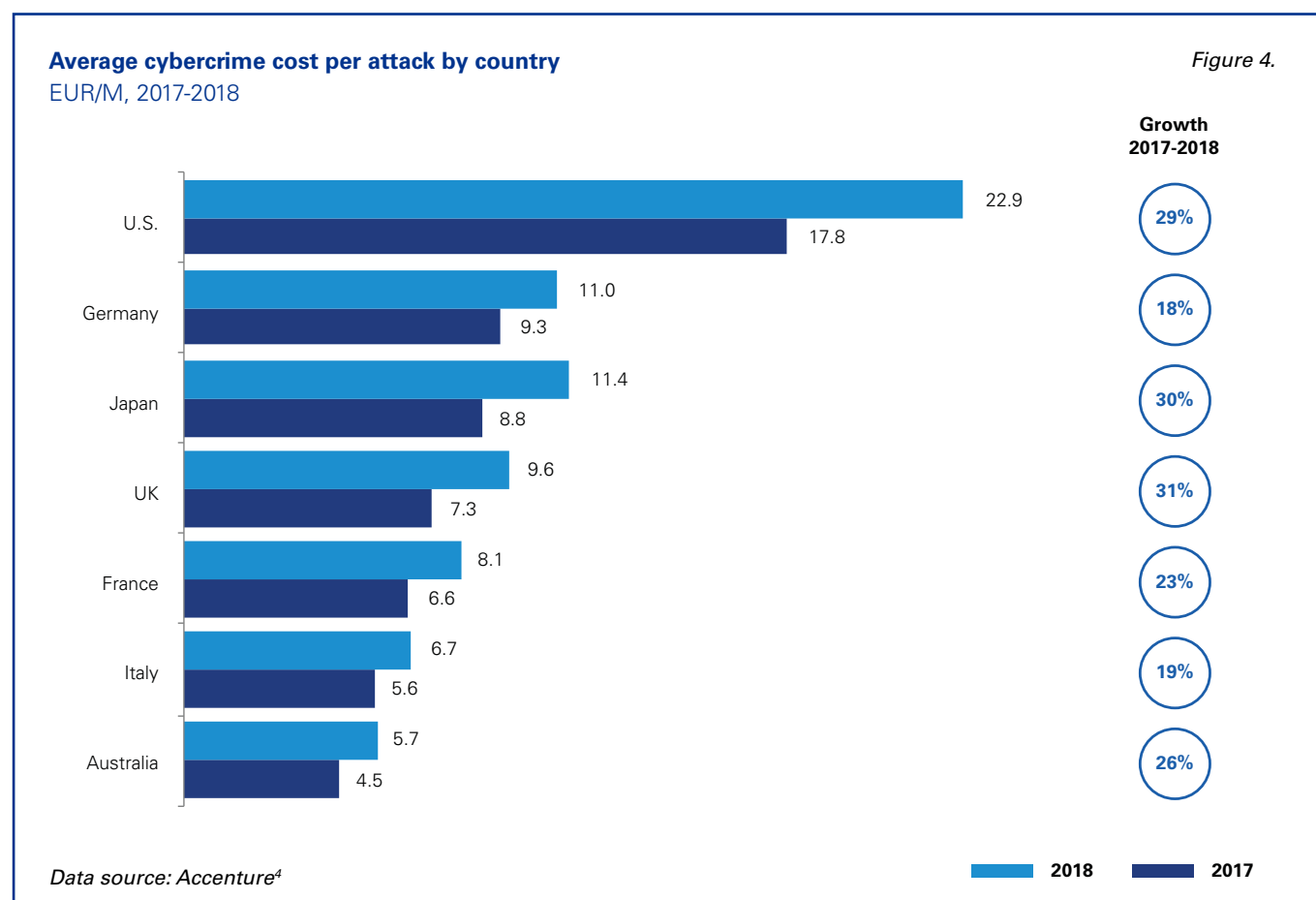
Figure 3.



Data source: Accenture⁴

^(b) CAGR = Compound annual growth rate

And this is not a pattern that is limited to a few countries. While there are significant differences in absolute cost of damage between different countries, the direction of travel is the same across the globe – attacks are becoming more expensive by the year (see Figure 4).



Both trends are slated to continue

We have spoken to dozens of cybersecurity professionals over the past months and one message that has emerged very clearly is – neither of these trends will come to a halt anytime soon.

The number of attacks is set to increase as a result of (at least) two factors:

First, due to the “digitalisation of everything,” the number of devices and the amount of potentially interesting data is increasing by the day. This is true for personal devices such as laptops and mobile phones, and also for industrial IoT devices. This factor alone is a recipe for an increasing number of attacks, as Nick Espinosa explains⁵ in his “Five Laws of Cybersecurity” – “Everything is vulnerable in some way” and “if there is a vulnerability, it will be exploited.” COVID-19 and the related shift to remote working has further accentuated this challenge.

Second, cybercrime has been going through a “wave of industrialisation,” with increasing levels of specialisation, sophistication and automation. As part of this development, something akin to a “global cybercrime ecosystem” has developed. For example, there is now “crime-as-a-service.” In the past, hackers needed to have a certain technical sophistication to pull off attacks. As of 2021, people with malicious intent and financial means find it relatively easy to find a “hacker for hire” or to purchase pre-configured attack modules on the dark web.

Similarly, there are (at least) two good reasons to believe that the average damage of attacks will also continue to rise:

First, attackers have optimised the economics of their attack. In particular, the use of ransomware attacks has been a game changer. In the words of a senior industry participant we spoke to, “In the past, these hacking groups used to go after individual personal information, such as user accounts, credit card information, etc., which they then sold for cents or dollars per record to monetise them. They had to steal millions of records to make it worth their while. Now, they have realised they can just shut down entire companies and ask for ransom in the millions at once.” From the perspective of the victims of these attacks, the increased use of ransomware by attackers implies a fundamental change of the threat landscape, because ransomware attacks cause immediate disruption to key business processes. For many companies, the negative business impact of such immediate and highly visible business disruption is more severe than the leakage of confidential data.

Second, the attackers are not resting. They are constantly changing and – unfortunately improving their modes of attack and their ways of monetising attacks. Consider the following examples:

- **Ransomware 2.0:** Attackers have recently started not only encrypting a company’s data on the target company’s servers, but also extracting a copy of the data in order to run a “double extortion” scheme. If the victim does not pay for decryption, the attackers can still revert to leaking the data⁶.
- **IT supply chain attacks:** Similarly, hackers have recently applied a new, potentially more damaging type of attack. They are now attacking individual companies in the IT supply chain to breach end users at scale. The way this works is as follows – a hacking group targets a single software provider. It hacks this provider and enters malicious code into its software product. Then, the software provider pushes this malicious software out to all its clients with its next update. Broadly speaking, this is what happened in the hacks of SolarWinds and Kaseya, two software providers in 2020 and 2021, respectively. In both cases, thousands of customers of these two software firms were affected and total damages of the SolarWinds hack have been estimated to be as high as several hundred billion dollars by some observers⁷. No wonder these new types of attacks have been referred to as “a revolution in sophistication”⁸.

Third, in recent years, the number of regulations governing data privacy have increased, and so have the regulatory penalties for breaches. In Europe, GDPR in particular has resulted in increasingly high fines (more on this in the next section).

Unfortunately, cyberattacks aren’t just a fad or an overhyped news story. They are a major challenge that is set to stay with us for the decades to come.

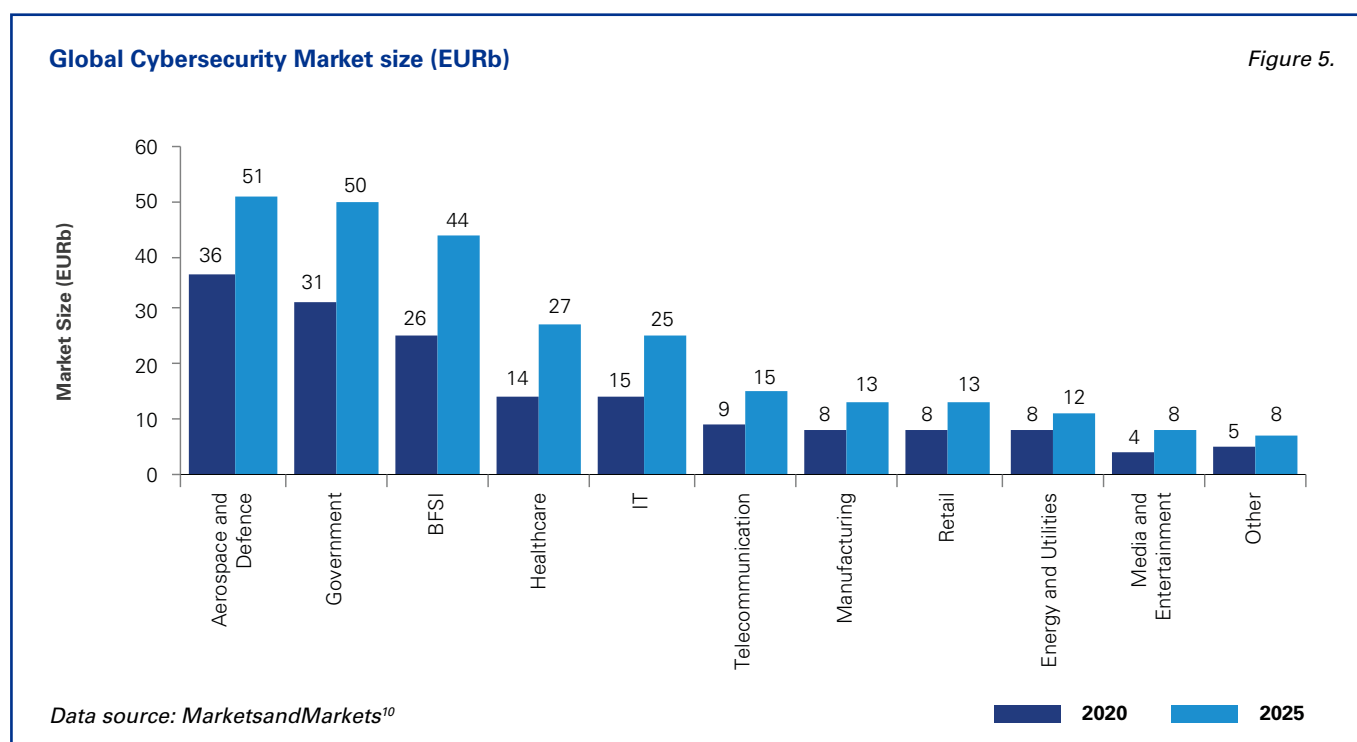
Companies across the board are becoming increasingly aware of their cyber risks

In the past, not all companies were equally aware of the threat of cyberattacks.

Traditionally, organisations with particularly sensitive data (such as aerospace and defence) or strong regulatory frameworks (such as financial services) have invested significantly in their cybersecurity capabilities. Take the example of JP Morgan, a global bank – to stay cyber-safe, it spends almost USD 600m on cybersecurity per year and employs over 3,000 people on cybersecurity matters⁹.

On the other end of the spectrum, firms with more analogue business models, less sensitive data or less stringent regulation have traditionally not invested nearly as much in cybersecurity capabilities. This is especially true for small to mid-sized businesses. In the manufacturing sector, for example, typical cybersecurity budgets are in single-digit millions, as cyber threats were perceived to be somewhat less tangible in this sector. To put it in the words of a CIO of a mid-sized European manufacturing company we spoke to – “It may sound crazy, but we would not die being out of business for a week. We also have some sensitive data, of course, but less than a bank, for example. Therefore, we felt like we could compromise a little more in terms of how much we invest in IT security.”

This type of thinking used to be – and still is in some cases – representative for industries further down the cybersecurity maturity curve (see Figure 5 for levels of maturity as proxied by cybersecurity spend).



However, this picture is changing very rapidly, as cybersecurity is becoming a board-level priority for firms in industries and size classes that were slow to warm up to the cyber threat. Figure 5 shows how cybersecurity spend is expected to increase fast across all industries in the coming years.

One of the key reasons for this awakening across different types of organisations is the introduction of increasingly stringent data protection regulation. In pre-GDPR times, companies felt accumulating pressure from consumers to some extent, as many of them voiced concerns about their loss of control over personal data. But with the formal introduction of GDPR, the stakes have now truly and tangibly increased. Companies are now required to defend themselves, at the risk of being fined if they don't do it properly. Specifically, GDPR regulation requires companies to protect data "by design and by default" (Article 25) and to consider the "security of processing" (Article 32), including "the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data." And the potential penalties for non-compliance are serious. According to Article 83, companies can be fined up to EUR 20m or 4 percent of worldwide revenues in the case of some breaches¹¹. Consider the call-out box on British Airways for a recent real-world example of a GDPR-related administrative fine in connection with a cyber attack.

Together with the increasing probability of being attacked and the increasing costs if hacked successfully that we discussed earlier in this paper, the increasing regulatory scrutiny makes for a perfect storm that calls for organisations of all sizes and types to get "cyber-ready".

GDPR fines after cyber attack: The example of British Airways

On 8 July 2019, the British Information Commissioner's Office (ICO) announced its intention to fine British Airways (BA) over GBP 183m for a GDPR infringement¹⁸.

The intention to fine BA related to an incident taking place a year earlier. Specifically, between 21 August and 5 September 2018, hackers were able to access names, addresses, e-mail addresses, and payment card details of passengers by diverting user traffic from BA's legitimate website to a fraudulent site. Overall, over 400,000 BA customers and staff were affected^{19, 20}.

The key reasons for the fine called out by the regulator were BA's failure to prevent the attack ("BA could have used numerous measures to mitigate or prevent the risk") and its "lack of awareness of the attack" until 2 months after the attack.

Since the initial notice of the ICO, BA's fine has been reduced to GBP 20m, amongst other reasons because of BA's cooperation with the authorities in investigating the breach²¹.

However, in spite of the reduced fine, this case clearly illustrates how, under GDPR, firms are now increasingly made responsible for effectively ensuring their cyber security.



And this is driving new business models

However, most organisations find it difficult, if not nearly impossible, to build complete cybersecurity operations in-house.

First and foremost, this is due to a significant shortage of qualified cybersecurity personnel in the labour market. Globally, there is currently a shortage of around 3m trained workforce¹². And multiple surveys across the globe have shown that organisations are impacted by a shortage of cyber workers^{13, 14}, that retaining their cyber staff is a challenge and that their cyber teams are generally understaffed¹⁵.

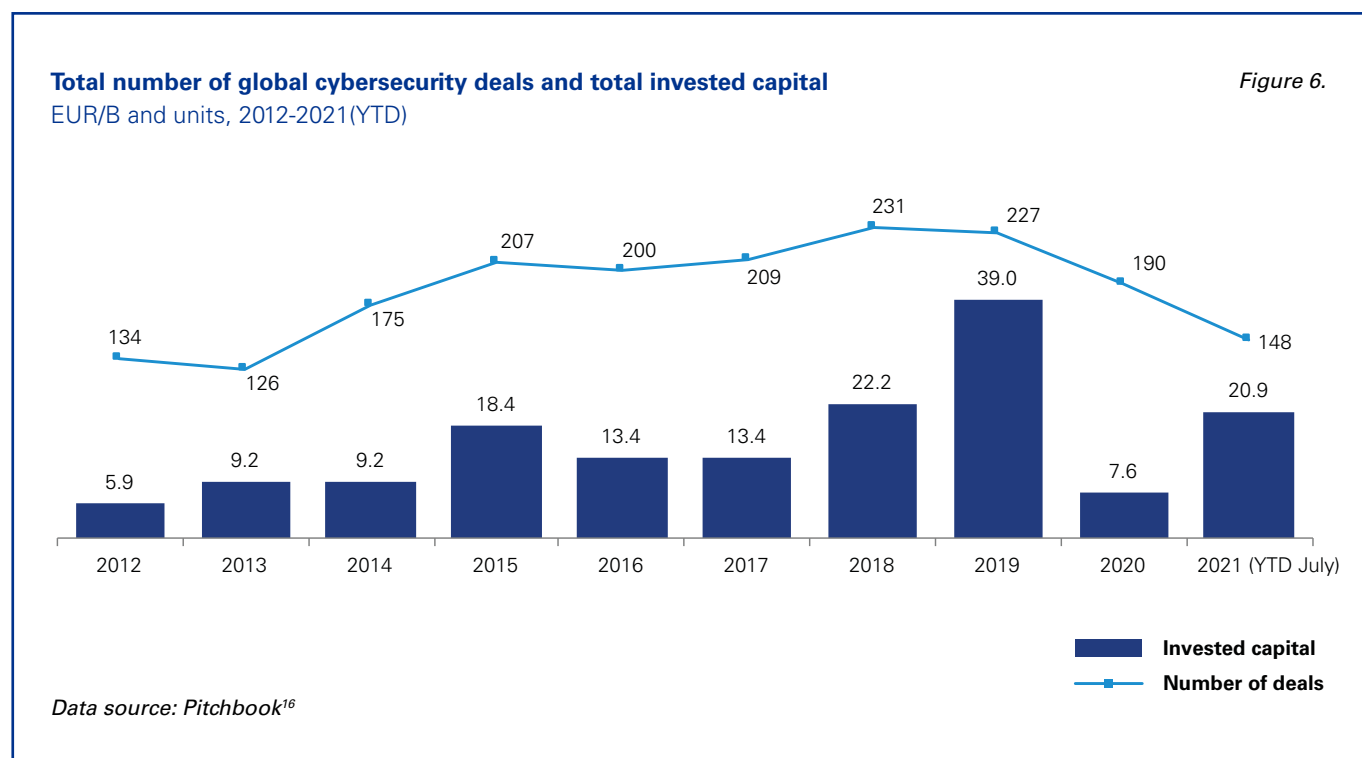
This, in turn, has led to a unique opportunity for cybersecurity companies to fill the void, primarily along two vectors; software and services.

In terms of software, companies have been developing tools that increasingly apply automation and machine learning techniques to cybersecurity tasks that used to require human handling in the past. Take the example of an endpoint detection and response (EDR) software: In the past, such software “only” logged activities of endpoint (e.g. laptop, phones) users. Human operators were then required to find potentially anomalous logs (e.g., someone logged into their laptop in New York only one minute after logging in London). If an anomalous log was confirmed as potentially dangerous, manual human intervention was required to take action (e.g., to lock the user out). In recent years, some EDR software products have developed the ability to automatically detect potentially dangerous activity and to take automated action in pre-defined cases. Similarly, some large software vendors have developed increasingly sophisticated security and information event management (SIEM) systems, which bundle and integrate previously separate cybersecurity products (such as endpoint or network detection and response software) into a single software environment, thereby enabling more convenient automation of security operations.

And while the software space is exciting, cybersecurity services may be even hotter right now. Besides high demand for traditional cybersecurity services such as penetration testing or red teaming, completely new business models are emerging. For example, an increasing number of companies are starting to offer “managed detection and response” (MDR). Such an MDR offering is essentially an outsourced security operation in which a third-party provider is plugged into a customer’s systems, monitors their activity and responds in case of incidents. This is a market that was close to non-existent a few years ago, but has grown at phenomenal rates in recent years. Basically, more and more mid-sized firms in yet relatively cyber-immature industries are starting to realise that they need proactive cybersecurity operations. However, buying cybersecurity software alone doesn’t do the trick. The company still needs to know how to configure the software, how to operate it and how to respond in case of an incident. For all these activities, human specialists are still required, driving demand for cybersecurity services.

Investors have taken notice (again)

None of this has been lost on investors. According to Pitchbook data, the total capital invested in cybersecurity deals grew at a CAGR of 30 percent per year between 2012 and 2019. In 2020, both the number and value of deals contracted heavily as a result of the overall shock to M&A caused by the global pandemic. However, as of July 2021, the cyberspace deal environment seems to be red-hot again. Globally, deals worth EUR 21bn have been struck (see Figure 6). If the remaining five months of this year continue at the same pace, 2021 might well be another year of cybersecurity deal-making records.



Who are the key players?

A very diverse set of players

There are literally thousands of cybersecurity players worldwide, spanning companies of very different backgrounds. To illustrate the differences of the firms playing in this market consider the following stylised groups:



Cyber natives

There are hundreds of “cyber native” companies that were started in the last 20 years. Some of them focus on cyber software, others on services. Examples of well-known companies in this category include firms such as CrowdStrike, FireEye, CarbonBlack, or Rapid 7. These companies are typically young, still relatively small, but valued very highly by the capital markets. See the illustrative example of CrowdStrike in the call-out box.



Global consultancies

Many global consultancies, such as Accenture and the Big 4 (EY, Deloitte, KPMG, PwC) have moved into cybersecurity services over the years – with services such as strategic cybersecurity advisory, technical consulting (penetration testing, red teaming, security architecture, etc.), incident response and in some instances even MDR services. These firms have a global footprint, brand recognition and existing C-level relationships throughout geographies and sectors, facilitating their entry in the space.



Global technology firms

The same is true for global technology firms like Microsoft, Amazon, Google, IBM, or Palo Alto, for example. These firms are active across various domains of cybersecurity, from software to services. Microsoft, for example, develops both a leading EDR software (Defender) and a leading SIEM software product (Sentinel) and utilises its strong enterprise software footprint to integrate its cybersecurity software neatly into the clients’ environments. Similarly, IBM has traditionally offered various cybersecurity software products (e.g. a well-known SIEM software called “QRadar,” amongst others) and has recently invested into expanding managed security services, including but not limited to, managed detection and response, both based on their own technology as well as 3rd-party technology suites.

CrowdStrike – example of a cyber native

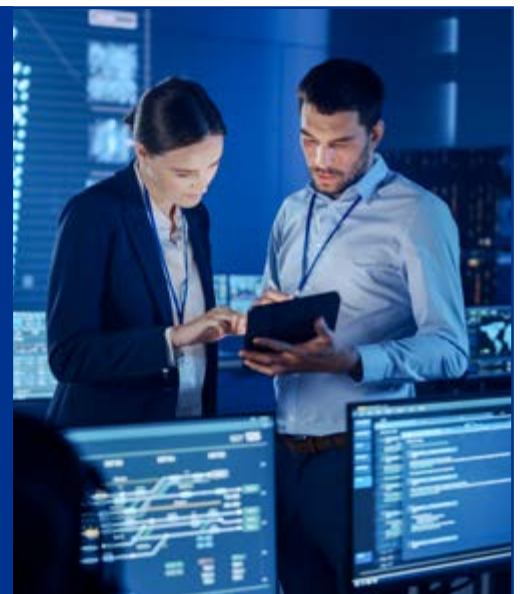
Crowdstrike is a California-based cybersecurity firm founded in 2011.

The company offers a cloud-delivered endpoint protection software product, with some services built in (e.g., 24/7 threat hunting).

The company’s latest income statement, as per its 10-K submission to the SEC, reveals how it has been able to profit from growth in cybersecurity software and services. For the fiscal year ended in January 2021, it reported revenues of USD 874m (up 82 percent from 2020).

However, the company has yet to turn in a profit for shareholders. In fiscal year 2021, it reported a net loss to shareholders of USD93m²².

This question mark on profitability notwithstanding, the capital markets are valuing the company at over USD 57bn, that is at over 65 times revenue²³.



Looking at who is investing in the cybersecurity space also yields insights as to who sees potential in the space. On this front, we have observed that there is a very broad range of active cyber-investors, ranging from the types of players mentioned above (cyber natives, consultancies, global technology firms) to professional services firms, telecom firms, engineering firms, and even defence companies.

Clearly, these are very different types of firms with different strengths, weaknesses, and resources at their disposal. And a detailed discussion of their competitive profiles goes beyond the scope of this paper. Nonetheless, it is worth pointing out that the competitive dynamics of this industry are still taking shape as we write this paper. Having spoken to multiple market participants on the matter, some of the key areas to watch in the competitive arena are discussed below.

Will European players hold their ground as American companies expand to Europe?

Many market participants we spoke to have referred to the U.S. as the most mature cybersecurity market in the world. They considered the U.K. to lag some “two-three years behind the U.S.” with continental Europe following further behind, although there is large heterogeneity in terms of cybersecurity maturity across different countries in continental Europe. As U.S. firms increasingly eye expansion in Europe – initially through the U.K. – it will be interesting to watch whether European leaders will be able to hold their ground.

While the scale and financial resources of American cybersecurity leaders speak in their favour, there are also multiple structural factors that might enable certain European players to carve-out a significant part of the market for themselves. For example, local language and culture in an industry where trust is a key success factor, physical proximity and corresponding reaction times in situations where fast response is critical, or legal requirements for local data storage (e.g., country-specific requirements like those typical in Swiss banks or even local interpretations of EU-level regulation such as GDPR).

How will the shift to the cloud impact the role of Microsoft, Amazon, Google, Alibaba?

Businesses are increasingly moving their data and software into the cloud. This is one of the megatrends in information technology impacting companies across geographies and sectors. It is underpinned by powerful forces, such as increased cost efficiency, ability to scale up and down flexibly and an increased ability to collaborate remotely.

One of the consequences of this shift to the cloud is that an increasing proportion of corporate network activity will not take place on network devices operated by companies on their own premises anymore, but on servers hosted by cloud infrastructure (IaaS) and platform (PaaS) providers such as Microsoft, Amazon, Google and Alibaba, or by cloud software (SaaS) providers such as Salesforce and the like. This, in turn, requires such cloud companies to provide cybersecurity solutions for the traffic taking place on their network devices.

Moreover, all of these firms are digital natives with outstanding machine learning and cyber defence capabilities. Also, needless to say, they are well funded and they have a unique ability to attract and retain scarce talent. As a consequence, these cloud giants have all the ingredients required to become major players in the cybersecurity software and services space.

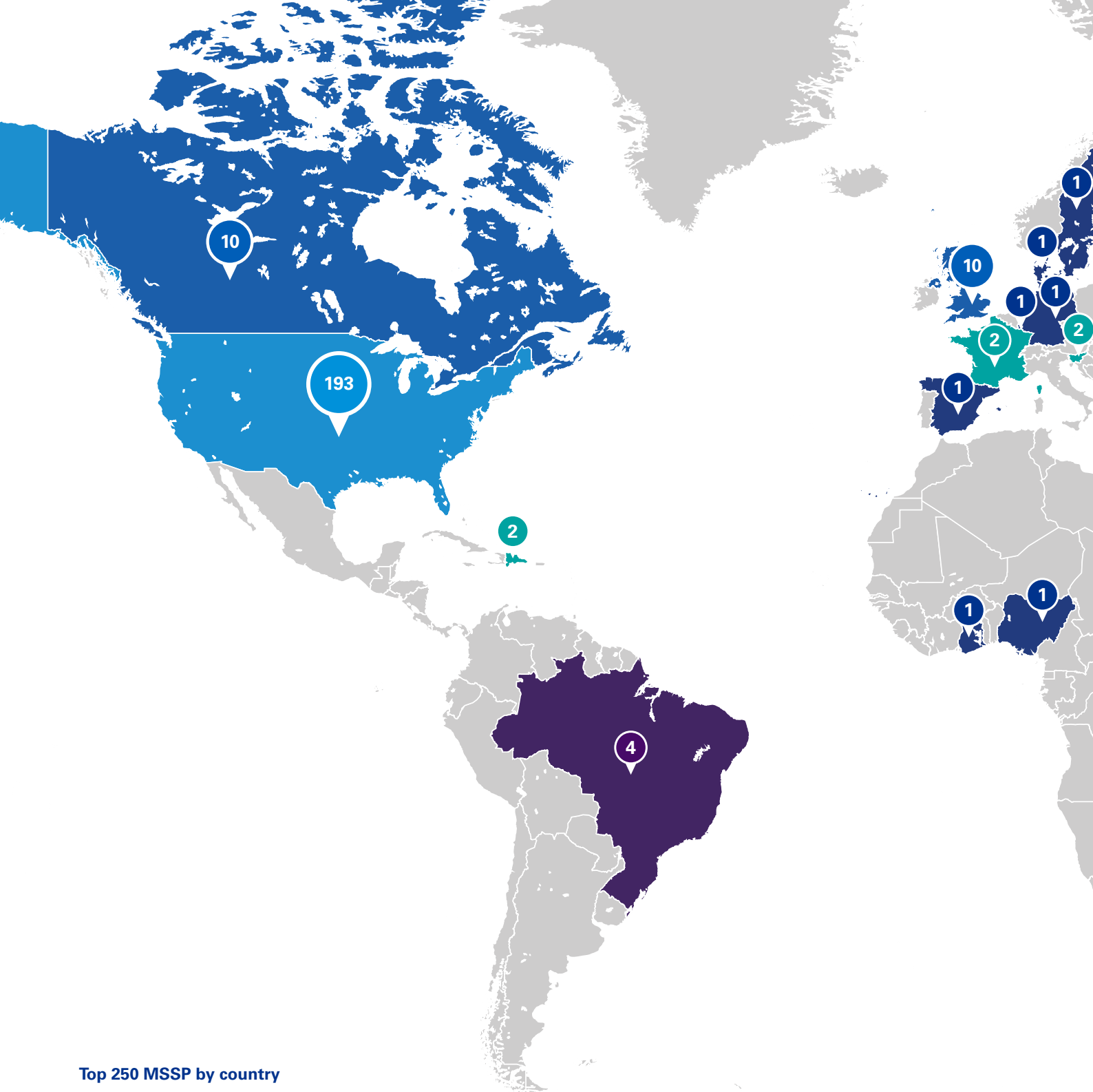
This being said, there are also potential challenges, in particular, in the area of cybersecurity services. For example, multiple market participants we spoke to expressed no interest in certain cybersecurity services such as managed monitoring, detection and response being provided by the cloud giants due to a perceived lack of independence. They would rather hire an independent service provider. And for services in particular, there is the question whether the cloud giants would want to enter a service business, given that services are harder to scale than hardware and software, which they currently excel at.

In summary, therefore, it seems clear that the cloud giants have all the capabilities it takes to be successful cyber players – but to what extent will they “want” to be cyber players themselves, in particular for services, as opposed to partnering with specialists in that space?

How disconnected will the West and the East be?

Having spoken to market experts in Europe and North America, we were surprised to find how seldom Asian cybersecurity firms were mentioned. To put some numbers to this, consider the latest ranking of the Top 250 managed security service providers (MSSPs) as published by After Nines¹⁷. According to the ranking, only 13 of these Top 250 MSSPs (i.e., 5 percent) are based in Asia¹⁷ (see Figure 7).

While some of this phenomenon may be a methodological undercount by a predominantly Western and English-speaking research community, we think the key point it illustrates is another one – there is a divide between Western and Eastern cybersecurity providers.



Top 250 MSSP by country

Not surprisingly, critical industries such as aerospace, defence and government have strong requirements to “buy local.” For example, serving American aerospace and defence companies is very difficult for non-American cybersecurity services companies. If possible at all, then only for companies headquartered in countries that are strong geopolitical allies and only under strict conditions with regard to the entity and employees that deliver the service.

But even outside of such critical industries, we have heard of similar sentiments. Many of the European cybersecurity customers we spoke to indicated that while they would be willing to consider a cybersecurity services company from another European country or perhaps the U.S., they would be less willing to consider a provider from other areas outside of the “Western bloc.”

Given the increasingly confrontational relationship between the U.S. and China, which has resulted in ongoing technology decoupling in general and specific mutual cybercrime-related allegations, it is unlikely that this divide between the West and the East will diminish anytime soon.

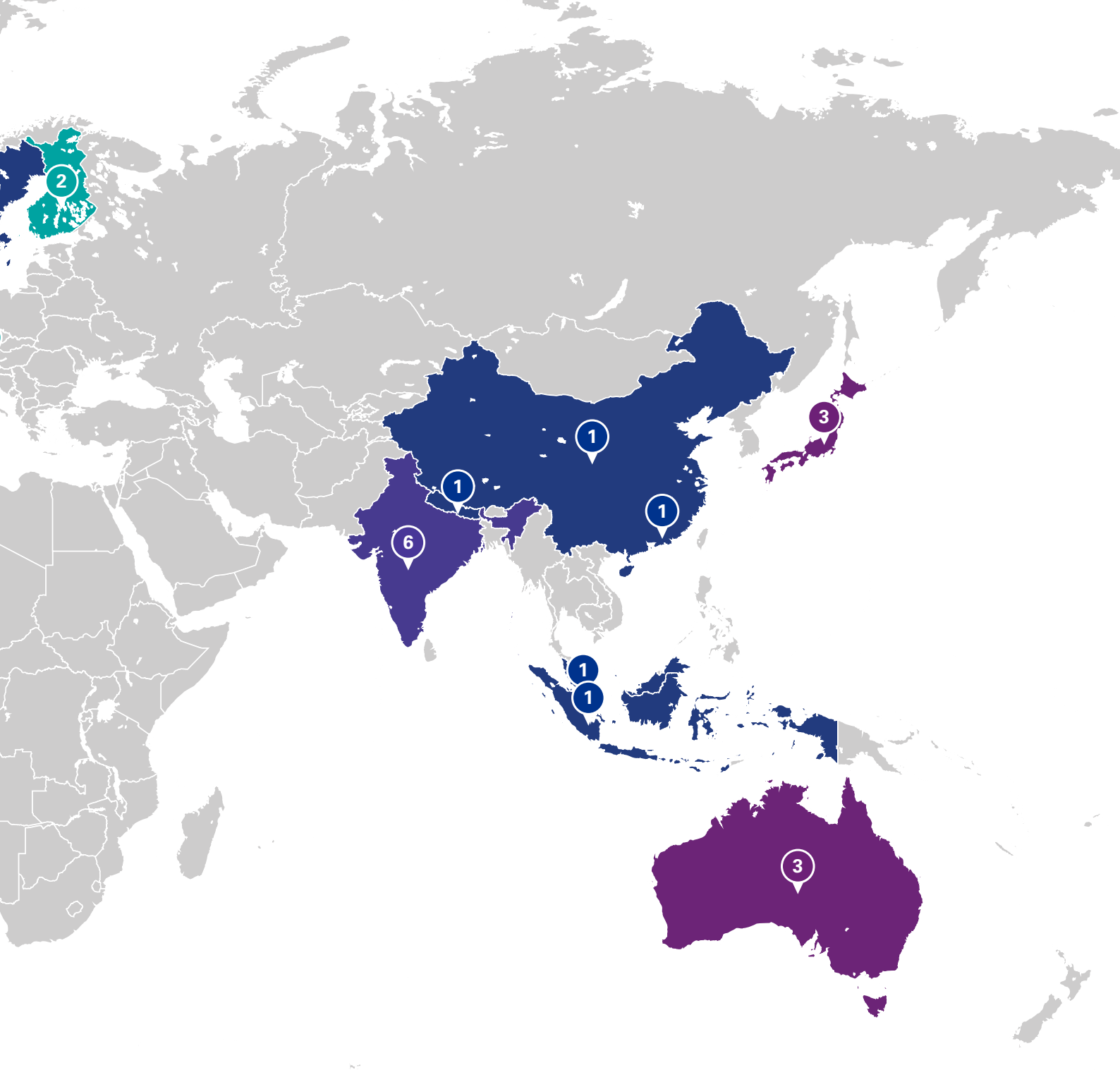


Figure 7.

These difficulties in the Chinese-American relationship notwithstanding, cybercrime remains a global problem. Attackers can attack from a physical hideout thousands of kilometres away. And non-state cybercriminals do not care much about whether they successfully attack an American, a European or a Chinese target – as long as they can monetise their attack.

Therefore, in spite of the current divide and the lack of trust between these regions, there will continue to be a need for cooperation across these regions. Cybersecurity companies which can collect actionable threat intelligence from different regions, which can apply the learnings of an attack in one region on potentially simultaneous, similar attacks in another region, will have an edge.

It will be interesting to watch over the coming years which of these forces will prevail and whether any truly global cyber champions will emerge.



Why do we think this market will consolidate eventually?

The economics of some markets dictate that they be fragmented. However, in cybersecurity, we do not believe that this is the case.

Cybersecurity software is a clear case, in our view. Software is an inherently suitable product category for scalability and market concentration – due to the nature of the product (once the software has been written, low marginal cost per additional sale), due to the prevalence of network effects and due to functional requirements on the client side (preference for a “single pane of glass”). We expect those companies that have a significant software development budget and the best ability to integrate within enterprise customers’ existing systems to act as consolidators.

But even in cybersecurity services, a category that is typically more difficult to scale, we see at least five forces that should lead to consolidation in the cybersecurity market over time.

Economies of scale and scope

First, cybersecurity services are a business with economies of scale and scope. Take MDR service as an example. There is a minimum size of cyber security analysts that are required to run a third-party security operation 24/7 (usually three shifts) and to have a base capacity for emergency incident response. However, as an MDR provider grows to attract more and more customers, this base capacity does not need to be grown linearly – resulting in lower unit costs per additional unit of revenue as the business grows (economies of scale). Similarly, an MDR business also gets better as the business takes on more customers – by learning from how Customer A is attacked, an MSSP can apply these learnings onto Customer B (economies of scope). All else being equal, these forces should benefit the large companies in the sector, putting them in a position as potential consolidators.

Need for global partners

Second, large customers are looking for regional (or even global) partners. In the current MSSP landscape, only a few firms can offer truly global support. This means there is a market opportunity to be reaped by a potential consolidator in terms of winning large, global accounts.



Need for stability (as proxied by size)

Third, security operations are a “business of trust”. Once firms get to the maturity stage where they realise the criticality of cyber defence, they do not feel comfortable hiring a small, just-about-to-turn-profitable cyber MSSP that might go under if an incident occurs. Instead, firms attach value to partners that appear to be stable (and financially large enough to absorb the impact of an incident). Again, all else being equal, this means the firms that manage to gain size first may benefit from disproportional market wins.

Consolidation of IT vendors

Fourth, in many large firms, there is a strong overall drive to reduce the number of IT vendors to a few strategic ones. While this may start in areas other than cybersecurity (such as office suite, communications technologies, etc.), we have seen first hand how this drive towards consolidation of vendors has started to include cybersecurity. From the perspective of cybersecurity providers, this implies that there will be market benefits from having a broad offering, as providers with a narrower offering will increasingly find themselves locked out. All else being equal, this should favour consolidation.

The big ones will win the war for talent

And fifth and finally, there is the cyber talent gap we discussed earlier. This gap has the direct consequence that talented cyber professionals can basically “choose where to work, how much to work, and what they want to earn” (quote of an industry participant). In such a hot talent market, the truly dedicated (and best) cyber professionals tend to prefer roles at leading cyber expert firms to in-house cybersecurity roles, as they prefer working on cutting edge cases globally to “sitting on the bench” waiting for a potential incident. As a result, cybersecurity service providers who gain scale and attract lots of interesting work, will be in pole position to win the war for talent, thereby further solidifying their position.

For these reasons, we believe that eventually, there will be consolidation in what is currently a very fragmented cybersecurity market.



What are the challenges in consolidation?

However, consolidation in cybersecurity is not an easy feat, in particular, on the service side. We have worked with investors who are considering acting as a consolidator, both on the strategic and on the financial side. The following are five challenges we have observed in practice.

Challenge 1: Maturity of potential targets

Since cybersecurity is still a relatively young market, many potential targets are still relatively small. In many of the European countries, in particular, there are only a handful of security services providers with profits in millions. As a consequence, we see buyers execute M&A in this space slightly earlier in maturity than in traditional IT services – which implies a need for investors both to be well connected to early-stage cybersecurity companies (not to miss opportunities) and to have the ability to lead deal conversations with companies that are slightly less mature than is the norm in other industries (in order to bring promising deals to a close).

Challenge 2: Technical diligence

Cybersecurity products and services are highly technical by nature. In all of the cybersecurity deals we have been involved in, targets have claimed that their product or service is unique because of some technical feature that others cannot replicate, that their solution integrates neatly into the typical software stacks on the client side and that they have some above-average track record of successfully detecting and avoiding cyberattacks. Similarly, most companies claim that their product is close to being fully developed, with limited further investments required in the future but lots of future sales potential.

While these claims may be true for some rare pearls, reality is often more subtle. And these degrees of subtlety only become evident upon conducting appropriate technical diligence.

In our experience, it is important that technical due diligence is allocated sufficient time and resources, as well as an appropriate forum for discussion. Conversely to discussions on commercial due diligence, for example, technical diligence should likely not take place at the C-level, but at the technical level – that is, between the people in charge of technical

developments on the sell-side and the knowledgeable cybersecurity tech experts on the buy-side, in the absence of (potentially intimidating) C-level stakeholders.

Of course, findings from technical diligence then need to be elevated to the commercial level in a second step and at that point, they may well become a C-level priority – but first, they need to be uncovered in tech-to-tech meetings and reviews.

Challenge 3: Technical integration

There are many reasons to acquire a cybersecurity target – such as geographic expansion, expansion of service offering, or realising cost efficiencies through economies of scale. However, the latter goal in particular, can be a challenge to achieve due to technical difficulties in integration.

Take the example of 3rd party providers of MDR: All these service providers work with certain software suites (either 3rd-party software such as Microsoft Sentinel or the CrowdStrike Falcon platform, for example or with their own in-house tools to monitor endpoint and network activities of their clients). Moreover, they have their own decision rules (i.e. which sort of activity to flag as potentially dangerous) based on years of experience. And many 3rd-party providers have linked their decision rules and their software through automation in order to make their services more efficient.

Therefore, if an investor buys two such service providers in order to reap economies of scale in operations, the first challenge the investor will face is that staff will not be able to cross-operate on each other's existing systems and processes – thereby making it difficult to reap such economies of scale. As a consequence, technical integration will become a priority. However, such technical integration usually takes place in the form where one set of systems and processes (presumably the superior one) replaces another (presumably the inferior one) – which, in turn, may trigger other challenges such as the retention of key employees (see below).

Challenge 4: Retaining the key employees

Many cybersecurity firms that are up for sale are still small-to-medium-sized and they tend to be run by their founders. And these founders tend to be technical evangelists, who were personally involved in designing the piece of technology or cybersecurity service their company advocates for. Below the founders too, there is a considerable degree of self-selection of employees into certain technical approaches, as cyber talent essentially has the choice of where to work.

Consequently, replacing one technology by another in order to presumably tap into economies of scale, as described above, is complicated by the fact that employees of the company whose technology is replaced might decide to leave the firm as a result. In a labour market that is as competitive as cyber, such an exodus of employees can be a company's death spell.

Once again, this puts pre-signing diligence front and centre; both from a technical perspective and from a commercial perspective. Key questions investors should be able to answer before signing include: Does my investment case require technical integration, or can I make the desired return “only” by continuing to sell the existing services into new customer segments? If it requires technical integration, are there any fundamental differences in the technological architecture and key processes between the two companies I am looking to integrate? And if so, are there any key employees we are likely to alienate by integrating these processes?

Challenge 5: Off-limit sectors or geographies

Some sectors and geographies are harder to tap into organically than others. As discussed earlier, in many countries, only local firms are allowed to serve customers in certain sensitive industries. As a result, it might be tempting to acquire a local target in order to gain the legitimacy needed to serve such clients.

While this might be a viable strategy in some countries and industries, it is not without potential pitfalls. For example, certain jurisdictions have local data residency requirements by law, which may limit a potential international MSSP's ability to operate truly internationally. Moreover, even in countries where few such restrictions exist, there may well be hesitancy among customers to work with a cybersecurity service provider from another geography. For example, in talking to European cybersecurity customers, we encountered a certain degree of hesitancy to acquire U.S. cybersecurity services even if the servers of these U.S. providers are located in Europe. In other words, actual purchasing behaviour is not only determined by formal market restrictions.

The upshot of this situation for investors is to conduct an appropriate level of commercial due diligence, aimed at answering questions such as: Does my investment hypothesis require the successful cross-sale into new sectors/geographies? If so, what are the typical purchasing criteria of customers in those spaces and how does my solution stack up against them?

What does this mean for investors?

The overall market case for cybersecurity in general is compelling. As we showed in chapter one, the market fundamentals could hardly be stronger, even if for the unfortunate reason of a rise in cybercrime.

In terms of competitive landscape, this is still a nascent and fragmented market that is taking shape, with little clarity on the emerging winners. This is both a positive (the lead is still up for grabs) as well as a potential negative (competitive dynamics are difficult to predict).

However, there are a number of strong forces that will push the market towards consolidation over time and only a few reasons why the market should remain as fragmented as it currently is. As a result, there are potentially large gains for investors who can successfully bring about this consolidation.

Successful consolidators will need to overcome a set of very cybersecurity-specific challenges, in particular, from a technical and commercial perspective. This makes a number of considerations of utmost importance for interested investors throughout the deal cycle:

- **Deal origination:** Given the fragmentation of the market and the fact that many potential targets are still relatively small, local start-ups, deal origination can be a challenge. Therefore, investors interested in the cybersecurity space should ensure to tap into well-connected local deal sources that have existing relationships to the local cybersecurity scene in order to tell the targets with substance from those without.
- **Pre-signing due diligence:** As discussed earlier, due to the technical nature of cybersecurity products and services, technical product details have important direct commercial implications. Moreover, since cybersecurity businesses are growth businesses, sellers generally strive for a valuation on the basis of a forward-looking business plan. In consequence, this makes both technical and commercial due diligence absolutely critical activities along the cybersecurity deal cycle.
- **Target operating model / integration:** As discussed earlier, there are some pitfalls to typical “buy-and-build” strategies in cybersecurity, in particular, the challenges of technical integration, retaining key employees in a dry labour market and clarity on focus sectors for growth post-transaction. This implies that investors should consider the specifics of their post-deal target operating model and the potential integration of their target(s) early – ideally, at a time when a deal can still be aborted in case of red flags.

Having worked with multiple investors (strategic and financial) across cybersecurity deals in various segments (software and services) and geographies, we strongly believe in the importance of integrated buy-side deal teams comprising technical, commercial and financial experts side-by-side. Only with such integrated teams is it possible to go to the technical depths required in a sector where technical aspects of the product are critical, while connecting these insights with their commercial and financial implications that will make or break a deal.

If you are interested in learning more about our experience in this space and how KPMG can help, don't hesitate to contact one of the authors listed below.



Authors and Contacts

■ Strategy & Deal Advisory

Alfonso Marone

Partner, Deal Advisory
Strategy & Value Creation
Technology, Media, Telecoms Lead
KPMG in the U.K.

E: alfonso.marone@kpmg.co.uk

Florian Bornhauser

Senior Manager, Deal Advisory
Global Strategy Group (GSG)
KPMG in Switzerland

E: fbornhauser@kpmg.com

Daniel Walters

Associate Director, Deal Advisory
Corporate Finance
KPMG in the U.K.

E: daniel.walters2@kpmg.co.uk

■ Cybersecurity consulting

Martin Tyley

Partner, Cybersecurity Consulting
KPMG in the U.K.

E: martin.tyley@kpmg.co.uk

Mark Tomlin

Senior Manager, Cybersecurity Consulting
KPMG in the U.K.

E: mark.tomlin@kpmg.co.uk

Dr. Matthias Bossardt

Partner,
Head of Cyber and Digital Risk Consulting
KPMG in Switzerland

E: mbossardt@kpmg.com

Ali Yaqoob

Director, Risk and Cyber Security Advisory
KPMG in Denmark

E: aliyaqoob@kpmg.com

Sources

1 For example, see Matthews, L. (2021, June 29). Details On 700 Million LinkedIn Users For Sale On Notorious Hacking Forum.

Retrieved from forbes.com:

<https://www.forbes.com/sites/leemathews/2021/06/29/details-on-700-million-linkedin-users-for-sale-on-notorious-hacking-forum/?sh=5760aad634a4>

2 Hill, M., & Swinhoe, D. (2021, July 16). The 15 biggest data breaches of the 21st century.

Retrieved from csoonline.com:

<https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>

3 Center for Strategic and International Studies (CSIS). (2021). Significant Cyber Incidents.

Retrieved from csis.org:

<https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>

4 Accenture. (2019). Unlocking the value of improved cybersecurity protection .

Retrieved from accenture.com:

https://www.accenture.com/_acnmedia/pdf-98/accenture-9thcostofcybercrime-study-france.pdf

5 Espinosa, N. (2018, September 7). The Five Laws of Cybersecurity.

Retrieved from youtube.com:

<https://www.youtube.com/watch?v=nVq7f26-Uo>

6 KPMG International. (2021, March). The changing shape of ransomware: How to defend against and respond to ransomware attacks.

Retrieved from assets.kpmg.com:

<https://assets.kpmg/content/dam/kpmg/xx/pdf/2021/03/the-changing-shape-of-ransomware.pdf>

7 Ratnam, G. (2021, January 11). Cleaning up SolarWinds hack may cost as much as \$100 billion.

Retrieved from rollcall.com:

<https://www.rollcall.com/2021/01/11/cleaning-up-solarwinds-hack-may-cost-as-much-as-100-billion/>

8 Marks, J. (2021, July 8). The Cybersecurity 202: The Kaseya attack is a revolution in sophistication for ransomware hackers.

Retrieved from washingtonpost.com:

<https://www.washingtonpost.com/politics/2021/07/08/cybersecurity-202-kaseya-attack-is-revolution-sophistication-ransomware-hackers/>

9 Dimon, J. (2018). CEO Letter to Shareholders.

Retrieved from jpmorganchase.com:

<https://www.jpmorganchase.com/content/dam/jpmc/jpmorgan-chase-and-co/investor-relations/documents/ceo-letter-to-shareholders-2018.pdf>

10 MarketsandMarkets. (2021). Cybersecurity market with Covid-19 impact analysis - global forecast to 2026. MarketsandMarkets.

11 European Union. (n.d.). General Data Protection Regulation.

Retrieved from:

<https://gdpr-info.eu/>: <https://gdpr-info.eu/art-32-gdpr/>

12 Business World. (2021, April). More than 3.1 Million vacancies unfilled in Cybersecurity positions all across the world: Report.

Retrieved from BWPeople.in:

<http://bwpeople.businessworld.in/article/More-than-3-1-Million-vacancies-unfilled-in-Cybersecurity-positions-all-across-the-world-Report/17-04-2021-386848/>

13 ISC2. (2020). Cybersecurity Professionals Stand up to a Pandemic.

14 Oltsik, J. (2020, August). The Life and Times of Cybersecurity. The Enterprise Strategy Group.

Retrieved from CSO:

<https://www.csoonline.com/article/3571734/the-cybersecurity-skills-shortage-is-getting-worse.html>

15 Tripwire. (2020). Cybersecurity Skills Gap Report.

Retrieved from tripwire.com:

<https://www.tripwire.com/-/media/tripwiredotcom/files/white-paper/tripwire-dimensional-research-skills-gap-report.pdf?rev=ade9d15473a24842a060d3297d1a7834>

16 Pitchbook. (2021).

17 After Nines Inc. (2020). Top 250 MSSPs 2020 Edition.

Retrieved from:

www.AfterNines.Com.

18 Information Commissioner's Office. (2019, July 8). Intention to fine British Airways £183.39m under GDPR for data breach.

Retrieved from ico.org.uk:

<https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/>

19 Information Commissioner's Office. (2020, October 16). ICO fines British Airways £20m for data breach affecting more than 400,000 customers.

Retrieved from ico.org.uk:

<https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/>

20 Newman, L. H. (2018, November 9). How Hackers Slipped by British Airways' Defenses.

Retrieved from wired.com:

<https://www.wired.com/story/british-airways-hack-details/>

21 The National Law Review. (2020, October 23). British Airways Faces Significantly Reduced £20M Fine for GDPR Breach.

Retrieved from The National Law Review:

<https://www.natlawreview.com/article/british-airways-faces-significantly-reduced-20m-fine-gdpr-breach>

22 United States Securities and Exchange Commission. (2021). Form 10-K: CrowdStrike Holdings, Inc.

Retrieved from:

<https://ir.crowdstrike.com/static-files/e51971cb-2889-42a1-92be-83982fdbb68f>

23 Yahoo Finance. (2021, August 2). CrowdStrike Holdings, Inc. (CRWD).

Retrieved from finance.yahoo.com:

https://finance.yahoo.com/quote/CRWD/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlMmNvbS8&guce_referrer_sig=AQAAAFPoIS_KzTj8PD

kpmg.com/uk



© 2021 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

Designed by **CREATE** | October 2021 | CRT137721A