2019 EDITION

INVESTING IN CYBERSECURITY

MCM ISRAELI IT CYBERSECURITY FUND

MIGDAL
CAPITAL MARKETS

2018 RANKED NO. 1 MORNINGSTAR

Nov. 2018 RANKED NO. 1 CITYWIRE

2019 EDITION

INVESTING IN CYBERSECURITY

MIGDAL
CAPITAL MARKETS

GENERAL OVERVIEW

The year 2018 will be remembered in the cybersecurity industry as the year of data breaches, as more than 700 million records were exposed in the ten largest data breaches. The total number of compromised data by the end of the second quarter of 2018 had already crossed the total number of breaches recorded in the whole of 2017. These data breaches were all from listed companies such as Marriott and Under Armour.

While data breach is the current issue, the number of cyber-attacks is growing exponentially, targeting countries and organisations. These attacks are much more sophisticated and cause heavy damage. According to the U.S. Council of Economic Advisers, malicious cyber activity cost the U.S. economy between $57–$109 billion and cyberattacks against critical infrastructure sectors could be highly damaging.

We can highlight three important trends that are likely to continue in 2019:

- From Hacking to Influencing: As cyber-attacks evolve, the attacks have shifted from stealing data and causing damages to having influential effects (e.g. fake news).
- E-Privacy: The responsibility to secure private data has shifted to the companies themselves and is driven internally by the companies and by regulators.
- Consolidation: As cybersecurity becomes more competitive, several M&A transactions have been made in 2018 (Imperva, Dome9, and so on). There are two main reasons for this: Improving technology and diversifying the number of products.

General Data Protection Regulation (GDPR), cyber insurance and other privacy protection regulations increase the demand for cyber protection and allow some of the cybersecurity stocks to gain from these trends.

In this overview, we will analyse these factors and market trends, their growth potential and their effect on the cybersecurity equity sector.

2018 TRENDS IN CYBERATTACKS

DATA BREACHES

In 2018, the estimation of the number of identity thefts exceeds more the 1 billion records. These records include private medical data, payment card numbers, social security numbers, billing information, health insurance information, physical addresses and phone numbers. According to Ponemon Institute, the average cost of a data breach per compromised record was $148, and it took organisations 196 days, on average, to detect a breach. They also found that the average total cost of a breach ranges from $2.2 million for incidents with fewer than 10,000 compromised records to $6.9 million for incidents with more than 50,000 compromised records.

Figure 1 demonstrates that the listed companies that reported a data breach suffered from a decline in stock price on the day of the announcement, and most of them continue to suffer from a negative trend in the following days.

1B
Identity thefts

148$
Average cost of data breach per compromised records

196
Averages days to detect data breach

2.2-6.9M$
Average cost per breach incident

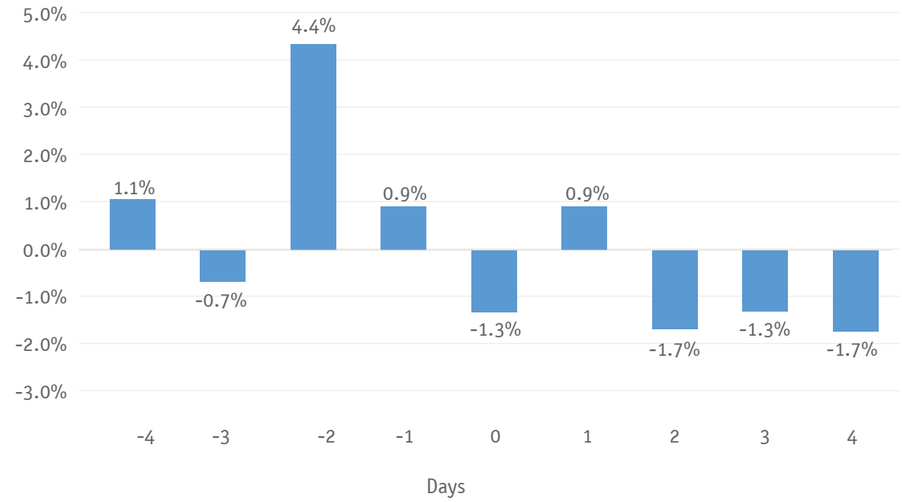
RANSOMWARE

While massive ransomware attacks were limited in 2017 (WannaCry, NotPetya and so on), it seems that ransomware has become a normal occurrence. In 2018, the largest known ransomware attacks locked down the City of Atlanta's digital systems and destabilised municipal operations, which took months to recover.

Cybersecurity Ventures estimates that ransomware attacks a business every 14 seconds, and the total costs in 2018 exceeded 8 billion USD and are expected to by 50% in 2019.

The ransomware attackers focused mainly on SMB, where the probability of obtaining a ransom is higher because of the lack of backup systems. In mid-2018, the FBI warned of increasing ransomware, and suggested that organisations should not support the attackers by paying them, because paying a ransom does not guarantee that the organisation will regain access to their data.

FIGURE 1: Large companies' data breach announcement's average effect on their performance in 2018. Day 0 refers to the day of the announcement.



Source: Bloomberg. The companies were the following: T-Mobile, Air Canada, Facebook, Marriot and HSBC.

DDoS

In 2018, distributed denial of service (DDoS) attacks increased by more than 100%, with more than 60,000 recorded attacks. The preferred days for the attackers were Friday and Sunday. During 2018, the bandwidth peaks continued to rise during the attacks. According to Corero Network Security, the estimated average cost for organisations due to such attacks was 50,000 USD in 2018. Beyond the costs of handling the attack, the main effect is the loss of customer trust.

In February 2018, the largest DDoS ever recorded hit the GitHub website. The attack took the site offline for five minutes. In order to solve the problem, GitHub decided to move the traffic to Akamai, who could help provide additional edge network capacity (Figure 2).

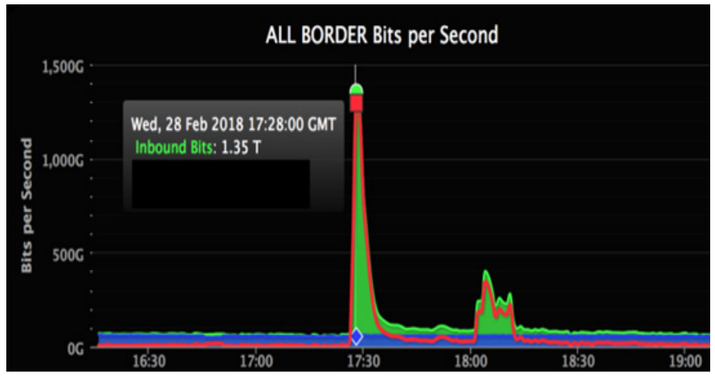


Figure 2: GitHub's inbound traffic skyrocketed during the attack. Source: Akamai

CLOUD

As cloud adoption continued to grow rapidly in 2018, different cloud models presented different risk factors. Shifting to the cloud was considered to be more secure. In 2018, 60% of the enterprises that implemented appropriate cloud visibility and control tools experienced one-third fewer security failures. Most of the data breaches in the cloud were related to human error (e.g. cloud storage misconfiguration). In 2018, one of the largest breaches occurred at GoDaddy, the world's largest domain name registrar, which exposed high-level configuration information for tens of thousands of systems in Amazon AWS.

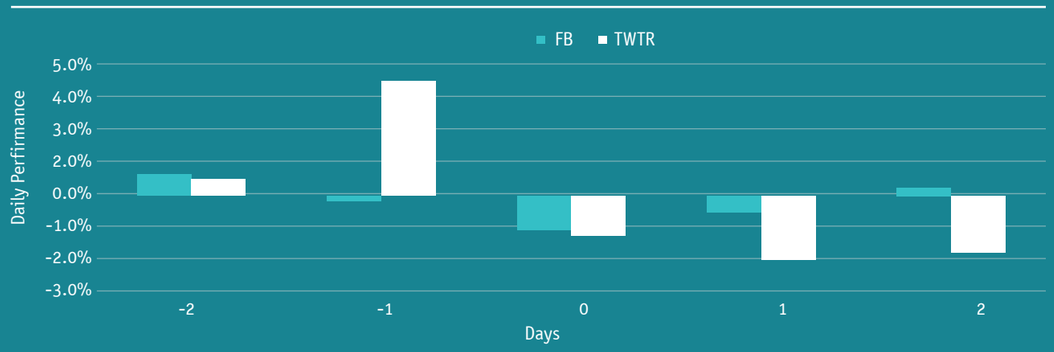
MOBILE AND INTERNET OF THINGS (IoT) ATTACKS

The number of Internet of Things (IoT) attacks tripled in 2018. IoT attacks are considered to be one of the fastest growing, mainly because of insufficient protection against them. These attacks have become more sophisticated in terms of stealing from, spying on and blackmailing users. In addition, in the 2nd half of 2018, much more sophisticated attempts were made to target infrastructure such as airports, power grids, etc.

INFLUENCE OF CYBER-ATTACKS

Governments, organisations and individuals attempt to use cyberattack techniques targeting social media as a news resource in order to ffect influence by creating fake news to affect public opinion (e.g. elections, branding). In May 2018, Facebook deleted 583 million fake accounts in Q1 that comprised more than a quarter of its 2.2 billion monthly active users. In July 2018, Twitter suspended more than 70 million fake accounts. Figure 3 shows the effect of the announcements on the stock price of Facebook and Twitter.

FIGURE 3: Twitter and Facebook announcement's average effect on their performance. Day 0 refers to the day of the announcement.



Source: Bloomberg.

TREND IN REGULATION AND CYBER INSURANCE

IMPLEMENTATION OF GDPR – GDPR FINES ARE LIKELY TO BE LEVIED IN 2019

GDPR is a regulation in European Union (EU) regarding data protection and privacy for all individuals within the EU and the European Economic Area (EEA). It also addresses the export of personal data from the EU and EEA areas. GDPR aims primarily to give individuals control over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. Under GDPR, the data controller is under a legal obligation to notify the supervisory authority without undue delay unless the breach is unlikely to result in a risk to the rights and freedoms of the individuals. There is a maximum time frame of 72 hours after becoming aware of the data breach after which the report must be made. In 2019, we believe that the European Data Protection Supervisor will begin to initiate fines on data breaches.

In 2018, the Information Commissioner's Office fined Facebook £500,000 because Facebook failed to keep the personal information of its users secure by failing to make suitable checks on developers using its platform.

We assume that due to the sufficient time available to adopt the new regulation, the regulators are likely to begin to implement penalties according to GDPR, and these penalties are much higher than the penalties prior to GDPR and include a fine of up to €10 million or up to 2% of the annual worldwide turnover of the preceding financial year in the case of an enterprise, whichever is greater, if there has been an infringement of GDPR's provisions.

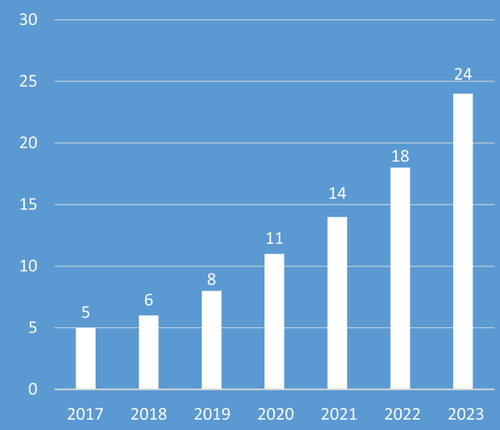
CYBER INSURANCE

The cyber insurance market was estimated at 6 billion USD in 2018, with a growth of 25% annually to 24 billion USD by 2023 (Figure 4).

The growing number of cyberattacks, such as malware and data breaches, in addition to new regulations, increases the need for organisations to protect themselves, both by appropriate solutions and by proper insurance policies that cover some of the losses. These losses include loss of business due to cyber-attacks, data restoration, event management, ransomware payments and so on. The demand for cyber insurance began with large enterprises, because their premium is considered to be relatively expensive. However, we estimate that SMB's will also buy this coverage, as some of the malwares now focus on SMB's with insufficient solutions for cybercrimes.

Currently, most of the insurance that has been underwritten has been in the U.S. (more than 85%).

FIGURE 4: Cyber insurance market (B USD)



CYBERSECURITY MARKET GROWTH POTENTIAL 2018-2022

The cybersecurity market size is estimated at 160 billion USD. There are several market segments that we estimate as having double-digit growth, ranging from 15%–25% annually.

DATA PROTECTION MARKET

The increase of data collection, both on the premises and cloud, tightens regulations such as GDPR and increases the demand in the 120 billion USD market. This market includes web filtering, social media security, messaging security as well as security assurance. We expect this demand to increase by 12% annually until 2023, mainly due to the adoption of several data protection solutions to meet cyber insurance and GDPR requirements. However, the growth will not be linear, and we expect a 20% growth in 2019 and moderate growth in 2020–2023.

ENCRYPTION SOFTWARE MARKET

As data breaches increase and the regulation is tightened, transferring encrypted data becomes crucial, even in the case of ransomware or DDoS in this 5 billion USD market. We estimate market growth in this segment of 25% annually over the next five years, mainly because our expectation for increasing the total data being transferred, including cloud

USER ACTIVITY MONITORING MARKET AND PRIVILEGED ACCOUNT MARKET

As some of the data breaches and data thefts are carried out by insiders, the monitoring activities to detect anomalous behaviours of employees has become based more on AI methods. The activity monitoring market analyzes and reports to the CISO on abnormal behaviour. Usually, these solutions are designed for large enterprises with many employees. In this market, we also include the privileged account solution. We estimate this market to be worth 10 billion USD and expect an annual growth of 20%. This estimation is based on the market assessment of historical annual growth.

DDoS PROTECTION MARKET

E-commerce and the value of customer satisfaction and trust is crucial for almost every online retailer. The increase in web traffic and the increasing number of DDoS attacks in 2018 increased the demand for DDoS solutions, mainly in terms of shifting traffic to other servers. Hence, we estimate this 3 billion USD market to grow annually by 20% in the next five years. This estimation is based on the increase of E-commerce industry sales, web traffic estimation and the expected growth of DDoS attacks.

CLOUD PROTECTION MARKET

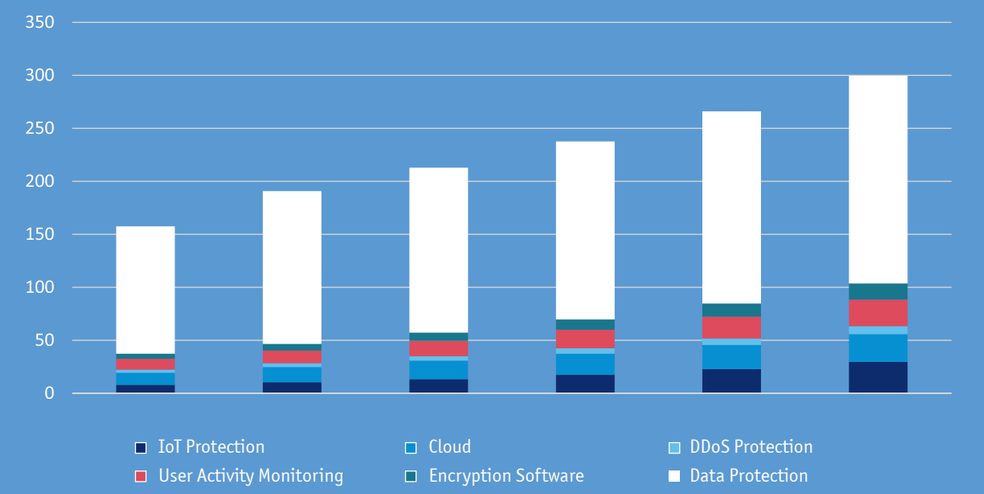
The cloud market is estimated to be worth 190 billion USD. The largest market share in terms of revenues is Cloud Application Services (SaaS) that make up 40% of revenues. A fast-growing segment is the Cloud System Infrastructure Services (IaaS), with an annual growth of more than 30%. We estimate that the adoption of the multi-cloud strategy among enterprises will increase the demand for the cloud protection market, which is estimated at 12 billion USD. We estimate an annual growth of 25% in the cloud protection market. Our estimation is based on the current pace of cloud adoption by enterprises (both IaaS and SaaS) and both private and public clouds estimated at 15%–25%, hence the growth in cloud protection, at least in the initial step of cloud adoption, will be higher mainly in order to gain customer trust.

IoT PROTECTION MARKET

The number of IoT connected devices is 7 billion, but the estimation is for accelerating growth to 22 billion devices by 2025 with an annual growth of 21%. This includes wearables, mobile phones, toys, autonomous cars, and so on. The current security market is estimated at 8 billion USD and we estimate a higher growth of 30% annually, supported by the acceleration in the number of connected devices and the accelerated number of IoT attacks in 2018.

To summarize, according to our estimation, the cyber security market will almost double over the next five years, as shown in Figure 5.

FIGURE 5: Cyber market growth estimation (B USD)

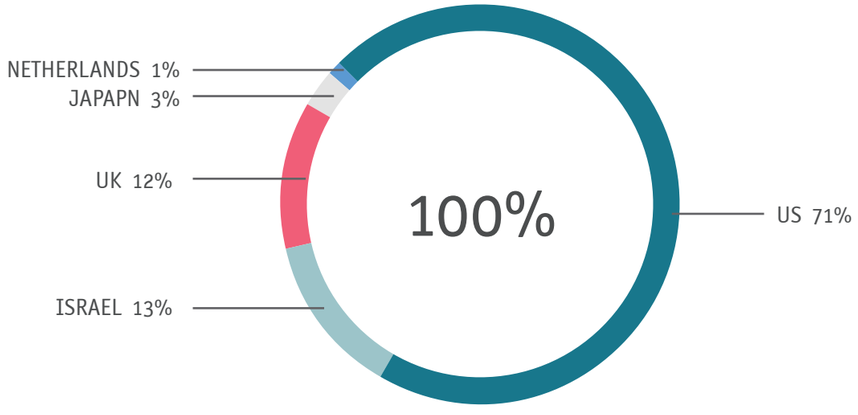


INVESTING IN CYBER SECURITY – UNIVERSE OF LISTED CYBERSECURITY COMPANIES.

The number of public cyber security companies listed globally was 58 as of the end of 2018. The total market cap of these companies as of the end of 2018 was about 360 billion USD. These companies presented an average revenue growth of 16%, 14% in EPS growth and increase of 10% in stock price in 2018.

Although Israel is considered to be a relatively small country in terms of GDP, it has the second largest portion of the cyber security in terms of public companies' market cap (Figure 6). The reason for this, besides the fact that Israel is considered to be the "start-up nation", is the fact that Israel is one of the main markets targeted by hackers, which has thus empowered Israel's cybersecurity skills. The U.S. maintained the dominant position in the cybersecurity market.

FIGURE 6: Cyber market CAP geographic allocation (B USD)



PERFORMANCE

In 2018, the cybersecurity sector continues to have a positive year, unlike the NASDAQ and other technology sectors, as can be seen in Table 1.

FIGURE 6: Cyber market CAP geographic allocation (B USD)

Year	Performance		Standard deviation		Sharpe Ratio		Var (95%)	
	CYBER EW	NASDAQ EW	CYBER EW	NASDAQ EW	CYBER EW	NASDAQ EW	CYBER EW	NASDAQ EW
2015	8.7%	2.5%	17.6%	17.1%	0.49	0.14	-1.8%	-1.7%
2016	19.2%	5.9%	19.3%	17.3%	1.00	0.34	-1.7%	-1.9%
2017	11.7%	26.0%	11.9%	9.8%	0.98	2.64	-1.2%	-0.7%
2018	9.92%	-5.99%	20.1%	19.4%	0.49	-0.31	-2.3%	-2.4%

The cybersecurity sector is considered to be relatively young. Therefore, we examined in Figure 7 the equal weight of the listed companies in the last four years and compared it with the NASDAQ equal weight.

There is a robust connection between the performance of the Cyber Equal Weight index and the google search for cybersecurity, as can be seen in Figure 8. The explanation for the connection between these two factors can be attributed to cyberattacks. It seems that in periods with massive cybercrimes, the public seeks explanations and protection and investors try to take advantage of this opportunity.

FIGURE 7: Cumulative performance of the Cyber security and NASDAQ equal weights in 2015–2018.

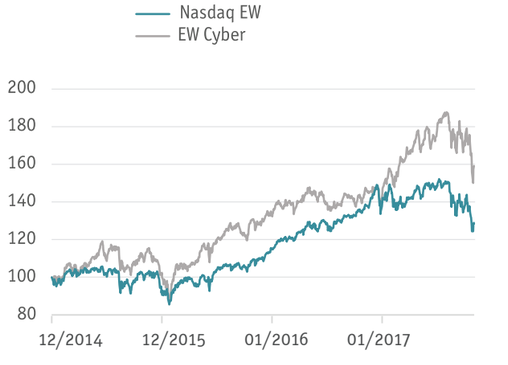
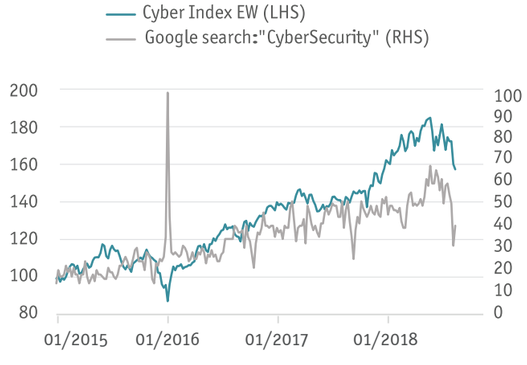


FIGURE 8: Cumulative performance of the Cyber security Equal Weight and google trend keyword "cybersecurity" in 2015–2018.



WHAT TO EXPECT IN 2019 IN THE LISTED COMPANIES?

COMPANIES' IN-LINE GUIDANCE

In 2018, most of the companies reported guidance in line with expectation and some of them even increased their guidance during the year. This guidance is crucial in the growth sector. So far, we haven't observed any company that reduced their expectation for 2019, but it seems that even if guidance is reduced, the growth rate both in terms of income and revenues will likely be more than in the case of other IT security sectors, driven by strong demand.

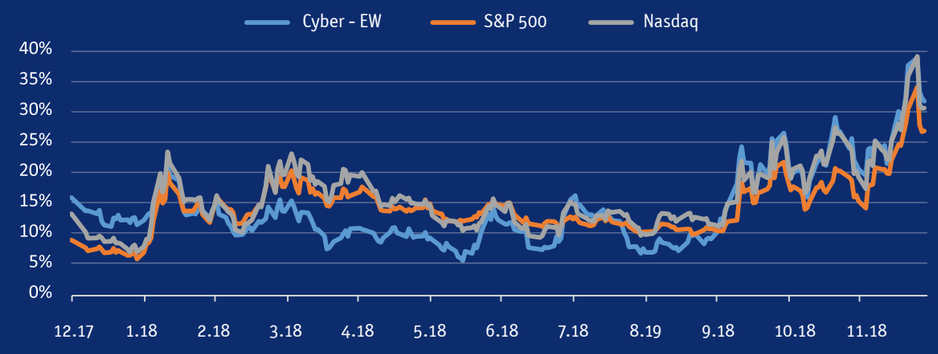
VALUATION

The cybersecurity market will probably continue to enjoy the increase in demand for cybersecurity solutions. Valuation had picked up in mid-2018 and has rebounded by 14%.

In order to compare the upside potential in the cybersecurity sector, we have taken Bloomberg Best's daily target price, which reflects bottom-up analysts' recommendations, and then divided this by the daily stock price to calculate the upside potential. We have built the Equal Weight benchmark for cybersecurity companies, covered by analysts which published the analysis. We have compared this benchmark with the S&P500 and NASDAQ upside potential (which is calculated based on the indices' weight calculation).

Figure 9 shows the daily best upside potential for the Cyber Equal Weight and also the S&P500 and NASDAQ composite in 2018.

FIGURE 9: Bottom-up upside in Cyber Equal Weights, S&P500 and NASDAQ composite



During the first half of 2018, the cyber target price was lower than S&P and NASDAQ, which indicates that the valuation was higher for the cyber sector. However, during the second half of 2018, especially in Q4, cybersecurity became more attractive in terms of valuation. As of the end of 2018, the higher upside was in the Cyber -EW 30%, which was more than NASDAQ and S&P500.

CONSOLIDATION

We believe that consolidation will continue in 2019. The consolidation will be much more important for platforms (e.g. Palo-Alto, Check Point) in order to preserve their status as market leaders. The M&A transactions will likely include start-ups and private companies when their valuation is unknown, as well as small listed companies (market cap of 1–4 billion USD) with best of breed solutions.

Informes sobre ventas/distribución:
KNG International Advisors
[Office Mex: +52 (998) 500-1627 | Office UK: +44 (207) 183-3787]
[info@ kngadvisors.co.uk | www.kngadvisors.co.uk]

MIGDAL
CAPITAL MARKETS