Industry Outlook

Cybersecurity

ITIC

Table of Contents

Summary

In the past years, technology has grown in numbers we could never think of, making the digitalization of that much data a reality, such as precious information of organizations, their decisions, strategies, and so much more are available digitally.

This has brought up a problem, how do we keep all that safe from our competitors and from people who might make our plans fail? Gladly cybersecurity is here, helping with the maintenance and safety of our files, protecting them from outsiders.

In the past years, technology has grown in numbers we could never think of, making the digitalization of much data a reality, such as precious information of organizations, their decisions, strategies, and so much more are available digitally.

This has brought up a problem, how do we keep all that safe from our competitors and from people who might make our plans fail? Gladly cybersecurity is here, helping with the maintenance and safety of our files, protecting them from outsiders.

Due to the current pandemic situation, our lives have been more and more digital, we have been working through web conference apps and websites, sending files to other people through multiple platforms, and that has raised even more awareness to the cybersecurity industry, due to the people and companies growing concerned for the safety of their data.

With this industry outlook, we aim to inform our readers about this growing industry, which many people only started seeing its value since the Covid-19 pandemic, having become one of the industries that benefited more from this happening.

Ana Ratão, Research Analyst

Environmental Analysis

Political factors

Ali Aljundi

Asset Management Department

	Political		
	Regulations	**Political Instability**	**Foreign Trade Restrictions**
Duration of Impact	Long term	Medium term	Medium term
Type of change	Positive	Negative	Negative
The factor's rate	Increasing	Decreasing	Decreasing
Importance	Critical	Important	Important

In places such as the United States and Europe, governments are beginning to pay much more attention to people and organizations' need for security while online on the web. This has led to regulations and major laws being put into place. An example of this is the National Cybersecurity Protection Act of 2014 done by the Department of Homeland Security (DHS) in the USA. This law states that the DHS, along with all the associated entities and individuals must regularly adapt and maintain their Cybersecurity interface. Much of these types of laws and regulations regarding cybersecurity are seen in Europe under the General Data Protection Regulation (GDPR).

Economic Factors

	Economic		
	Economic growth	**Recession**	**Low Interest rate**
Duration of Impact	Long term	Long term	Medium term
Type of change	Positive	Negative	Positive
The factor's rate	Decreasing	Increasing	Neutral
Importance	Critical	Critical	Important

Economic growth suggests that many companies are also growing and thriving with greater revenues. This is a critical factor in many industries including cybersecurity, due to the fact in a recession companies are more focused on their main activities and survival and are less likely to be interested in buying cybersecurity solutions.

Social Factors

	Social		
	Labor Quality	**Labor Quantity**	**Lifestyle (remote working)**
Duration of Impact	Long term	Short term	Long term
Type of change	Negative	Negative	Positive
The factor's rate	Decreasing	Decreasing	Increasing
Importance	Critical	Critical	Critical

With the current state of the pandemic, remote work has been a must for many organizations as a way to keep operations going. With that in mind, much more information and data are now online and possibly at risk. This is positive for the industry since the demand for cybersecurity increases much more and companies within the industry are able to provide a solution to this increasing problem that is now becoming more prevalent.

Technological Factors

	Technology		
	Tech incentives	**Tech innovation**	**Awareness and uses**
Duration of Impact	Long term	Long term	Long term
Type of change	Positive	Positive	Positive
The factor's rate	Increasing	Increasing	Increasing
Importance	Critical	Critical	Important

Advances and development in technology are critical for this industry and have a positive impact since this allows for innovation of cyber protection products to take place. The latest advancements which are currently happening include the use of blockchain technology and Artificial intelligence. The implementation of Blockchain technology will potentially allow for decentralization and no human errors in the cybersecurity products. In addition, Artificial intelligence will aid in responding to cyberattacks more effectively by identifying and preventing threats much faster than traditionally.

Legal Factors

	LEGAL	
	SEC legislation	**Health Law**
Duration of Impact	Medium term	Medium term
Type of change	Positive	Positive
The factor's rate	Increasing	Increasing
Importance	Important	Important

The Securities and Exchange Commission (SEC) regulations are put in place to oversee the cybersecurity of financial entities such as brokers, investment companies, and investment advisors. The many regulations and policies set by SEC require for many companies in the financial field to implement cybersecurity solutions to guard against cyber-breaches that would affect many stakeholders.

Healthcare regulations have been put in place with the aims of maintaining confidentiality, protecting information, and preventing online cyberattacks. An example of these regulations is the Health Insurance Portability and Accountability Act of 1996. This regulation requires health departments in the US to adopt national standards for health care information transactions that take place electronically, one of the standards is that there must be online security implemented.

Environmental Factors

	Environment
	COVID-19
Duration of Impact	Short term
Type of change	Negative
The factor's rate	Increasing
Importance	Critical

Covid-19 has majorly impacted many companies negatively. A lot of the company's revenues have decreased, and operations have changed. Due to this factor, the world economy has also been negatively impacted by this. With that said, many companies have mainly been focusing on survival and how to adapt to the current environment. This can have a negative effect on the cybersecurity industry due to companies only focusing on staying afloat in times like this instead of looking for cybersecurity solutions. On the other hand, however, this pandemic has caused many things to become digital as mentioned previously, which has raised more awareness of cybersecurity.

Industry Competitiveness

Carolina Marques

Research Department

Porter 5 Forces

The Threat of New Entrants

- **Moderately strong competitive force;**
- Upon entering the market it's hard for new companies to gain customers, since it's an industry highly dependent on trust, taking a long-term commitment to developing a range of strategic abilities. Taking that into account, big companies who already have a "name" in the market end up absorbing or monopolize the small businesses with potential;

- Many companies still struggle to recognize the necessity for high-quality security, lacking in their budgets the financial resources needed. This makes it especially hard for new companies to enter the market with high-end products, as many don't recognize their value.

Competitive Rivalry Within the industry

- **Strong competitive force;**
- The cybersecurity market is highly competitive due to its fragmentation, having several global and regional players;
- Rapid product Innovation makes it hard for companies to achieve sustained sales and growth over time, as the market is changing rapidly, and new products are launched daily;
- New areas like Big Data and IoT are changing security trends and rising the firm concentration ratio, as the major players in the market grip about 30-35% share due to their portfolio and large customer base.

The Threat of Substitute Products

- **Moderately strong competitive force;**
- The perceived level of product differentiation is still very low;
- Various products/services that serve the same need make it easier for customers to buy different company's products;
- Some operative system providers like Microsoft already include anti-malware tools and equipment in their products.

Bargaining Power of Suppliers

- **Moderately Low competitive force;**
- The market is very fragmented making up for a lot of players;
- Very complicated for suppliers to gather valuable IT security developers, as many lack sufficient training and knowledge in analytics, forensic investigations, and cloud computing security;

- Shortage of players with security solutions to meet the upwards trend in IoT, BYOD, Artificial Intelligence, and Machine Learning in Cybersecurity;
- Great Dependency on traditional authentication methods and low preparedness for unexpected cyber-attacks;
- The need for security solutions is rising as constant new threats appear.

Bargaining Power of Buyers

- **Moderately strong competitive force;**
- The high number of players and different options available in the market, make buyers have an advantage when it comes to their choices;
- Governments and big companies gain a lot of negotiation power due to their size and influence, which lowers the product/service providers in the industry the capacity to meet their needs;
- Agencies to charities—to strengthen their cyber defenses. The growing security needs of these organizations are expected to underpin the rapid growth and evolution of the global cybersecurity industry over the next decade.

SWOT Analysis

Ana Ratão

Research Department

Strengths	Weaknesses
S1. Importance regarding remote working S2. Growing importance of the sector in the current world S3. Always developing, there is always new work S4. Work can be done remotely	W1. Can be costly W2. There are not many people in this area, due to the difficulty associated with it W3. The value of services can be hard to be perceived by customers

Opportunities	Threats
O1. Growing awareness of it at the current time O2. Growing need for cybersecurity in a growingly technological world O3. Increase on investors O4. Increase in perceived value by stakeholders O5. Increase in tech usage O6. Increase of important info available online	T1. Whenever a solution is found, someone finds a way to break through it T2. Lack of regulations

W3&O6: ***The value of keeping our files secure***

Nowadays people tend to value more the value of services provided by cybersecurity since most of their life is now digital, making it important to keep it safe. While it is still hard to define a value, customers are tending to see the importance of cybersecurity and understanding more its need to exist.

Due to the pandemic many people started working from home, using their computers, either personal or from work and many realized the risk of having such important info on their computers that could potentially be stolen or corrupted, therefore people have begun to see the value of cybersecurity.

W1&O3: ***Costs are easier to cover***

While some years ago not many people believed that this market was important, due to our current situation and the ongoing digitalization of our world, investors have now started to bet on this market, making its costly investments less difficult for companies, since now they have options beyond credit. It also contributes to the constant development of this sector since due to its specificities it needs constant update and training.

S4&O1: *Covid-19 and remote work*

Since the start of the pandemic remote working is not new for anyone, therefore for cybersecurity we have the best of both worlds, now people need their data as safe as possible and cybersecurity services can many times be done remotely, which is perfect in these times of social distancing and quarantine.

The protection of a server, for example, can be done by a worker of a cybersecurity firm from the comfort of their own home by remotely accessing the server and making the necessary adjustments.

The Big Players

TrendMicro

Carolina Marques

Research Department

Description

Trend Micro Incorporated is a multinational company, headquartered in Tokyo, Japan that develops and sells security-related software for businesses, data centers, cloud environments, networks, and endpoints. The company offers solutions regarding collective attacks like viruses, spam, phishing, spyware, botnets, and data-stealing malware. It runs a global network of data centers, along with an automated and manual threat correlation system that offers its customers round-the-clock feedback and protection. Furthermore, the company provides solutions for more than 500,000 customers such as enterprises, small and medium businesses, individuals, service providers, and OEM partners.

Strategy

The main goal for Trend Micro is making exchanging digital information a safe activity for all users of its products. The strategy of the company has been focused on safeguarding quality cloud security to its customers by offering a differentiated approach that is" cross-

platform, cross-operating system and cross-people". To be able to attain this position, they have been investing in threat research and innovative core technologies that work for a multitude of devices and platforms, this way customers can enjoy safe use, no matter the platform they're using. The company has a worldwide network of about fifteen threat research centers, which monitor potential security issues and come up with quick solutions to major problems, responding faster and efficiently to customer's requests. As new vulnerabilities are always appearing, Trend Micro provides the global security reach with the personalized local touch that enables customers to be secure when operating online.

Potential Projects

Interpol Partnership to combat Covid-19 Threats: As the pandemic started, organizations around the globe were forced to adapt to mass remote working, which put great pressure on IT security teams and remote access infrastructures since new scams and threats were emerging every day. In order to protect organizations and their workers, Interpol partnered up with TrendMicro to counsel and secure the newly distributed workforce. They improved their password security, 2FA for work accounts, automatic software updates, regular back-ups, remote user training, and restricted use of VPNs along with six months free use of its flagship Trend Micro Maximum Security for home workers.

ZDI (Zero Day Initiative) was created to promote the reporting of 0-day vulnerabilities privately to the affected vendors by financially rewarding researchers. Although it's not a new initiative as it was created in 2005, this year the project celebrated 15 years of existence. By incorporating the global community of independent researchers with their internal research organizations the company was able to become the world's main vendor-agnostic bug bounty program.

Financials

The company's revenues have been growing consistently over the years, reaching about $1.52 billion in 2019, reflecting a rise in demand for Trend Micro's products and services considering the current favorable market conditions. The ROA has been stagnant in the last few years, being around 8%, however, in the 1st quarter of 2020, this value was slightly higher

at 8.77%. Following the same trend, ROE has averaged at 14.5% but at the end of the 1st quarter was at 17.27% making up for positive results when considering the company's profitability.

In terms of liquidity, the company shows a solid financial ability to cover short-term liabilities since the current ratio at the end of the 2nd quarter of 2020 was situated at 2.12 and the quick ratio at 2.09. However, and by analyzing Trend Micro's Debt-to-Equity(D/E) ratio it can be concluded that the company relies mostly on loans and borrowed capital since in the 2nd quarter of 2020 it was registered at 0.93.

At the end of 2019, the stock (TMICY) closed at $51.1 compared with the $55.73 registered as of 27th November 2020, making up for a 9% growth. Even though Trend Micro's stock price has increased, it isn't showing an outstanding evolution, as it's growing at a slow pace.

CyberArk

Fernando Rangel
Research Department

Description

CyberArk is an American Cybersecurity company created in 1999 by Udi Mokady (current CEO) and Alon N. Cohen. The company became publicly traded in 2013 and is currently listed on the NASDAQ with a current market cap of over $4.05B. CyberArk focuses on privileged access management (PAM); This refers to the numerous systems that are put in place to keep important accounts that have access to highly confidential and corporate resources secure from any potential hackers and cybercriminals.

This company is currently one of the global leaders in this area of cybersecurity with offices in 14 countries around the world.

Strategy

CyberArk has a mass-market business model, not focusing their products on any niche market but to organizations in all industries. However, CyberArk's security solutions are

mainly be used by organizations that deal with critical information such as governments, financial services, and healthcare.

The product that the company provides to other firms is Privileged Access Management. This product has three main features, which are to monitor, keep secure, and manage a company's online platform, databases, network devices, operating systems, etc. These features can all be used in combination or individually depending on the package that is selected. That said, CyberArk allows potential customers to have a free trial of 30 days so that they get to try the product and see if it fulfills their needs.

Financials

By analyzing some of the key ratios, it is seen that overall, CyberArk has a moderate financial performance.

Over the past years, the company's revenues have been on the rise. In December 2018 revenues were $343m, a year later revenues increased 26.53% to $434m and as of now, September 2020 revenues are at $450m. As seen, the revenues have been steadily increasing every year with annual gross profit also increasing alongside.

At the end of 2018, CyberArk's ROA was at 7.16%. Then at the end of 2019, it decreased to 6.68% and further decreased even lower to 0.21% in September 2020. This ratio is currently under the industry's average of 1.75%. The company's ROE also followed a similar route going from 10.94% at the end of 2018, increasing a little bit to 11.31% the following year but sharply decreasing to 0.46% in September 2020. This ratio is also under the industry average of 4.83. Both the ROA and ROE are currently on the decline as of recently.

In terms of liquidity, the company's current ratio was mainly around 3.30-3.60 from 2017 to mid-2019. However, the ratio increased by more than 80% to 6.25 earlier this year in March but has declined to 4.47 in September. Although the ratio has declined, it still is well above the industry average of 1.85. CyberArk currently has a quick ratio of 4.47 which is also currently above the industry average of 1.74. This indicates the company has very good short term financial strength

The debt to equity ratio (D/E) in 2019 was at 0.78 and had a minor decrease to 0.74 in September this year. This ratio is currently below the industry average of 0.22.

The stock (CYBR) price is currently at $113 (11/27/2020), this year's stock high was $142 at the beginning of the year and the stock low was 72.78 in March. Price on the yearly chart is currently consolidating with no clear trend at the moment.

Fortinet

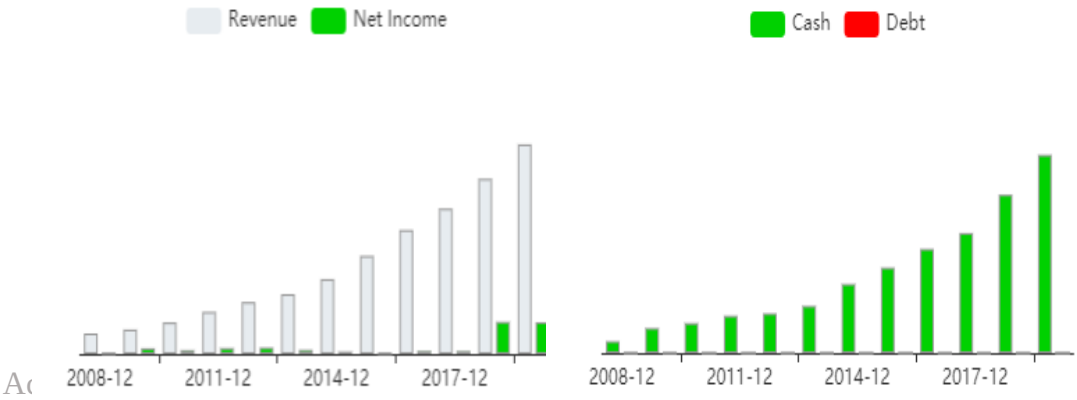
Ali Aljundi

Asset Management Department

Fortinet is one of the most considerable companies in the cybersecurity industry. It is an American universal firm headquartered in Sunnyvale, California, and it is traded in Nasdaq with a ticker FTNT.

It operates through different fields and develops numerous products such as network security; infrastructure security; cloud security; and endpoint protection, internet of things (IoT), and operational technology.

The 20 years old company that went public in 2009 just nine years after its establishment, now possesses $3.89B in assets and its revenues have been growing for the last five years where it achieved $2.16B in 2019. Furthermore, despite the high COGS, its net income skyrocketed dramatically in 2019 to reach $326.5M from $7.99M in 2015. It is critical to mention that Fortinet is creating value because ROIC (21.41%) is higher than WACC (6.88%).



Additionally, Fortinet manifested that it is financially strong because it is significantly funded by equity since the debt to equity, debt to capital, and debt to assets recorded 0.035, 0.034, and 0.012, respectively. Hence it is for granted that it is a safe debtor from a long-term creditor perspective. Whereas from a short-term perspective its current ratio, quick ratio, and cash ratio emphasized that the firm is trustworthy where they scored 1.88, 1.8, and 1.4, respectively.

Besides, the Altman- Z score of Fortinet is 5.27>3 which indicates that it is in the safe zone and far from bankruptcy.

Moving to valuation, the firm's market cap in 2019 boosted to $18.33B, and its enterprise value was $16.39B. The company's financial multiples are higher than its index which may indicate that it is overvalued.

This table shows the corporation's financial multiples and its index:

The multiple	The company	The index
P/S price to sales	9.12	2.4
P/E price to earnings	47.27	25.77
P/C price to cash flow	23.43	14.57
P/B price to book value	28.18	3.39
EV/EBITDA	44.12	20.23

Conclusion

The usage of online platforms is ever increasing, especially with the current ongoing Covid-19 outbreak that has majorly amplified the need for countless organizations to go online and implement remote work. With that said, as online usage increases, so does the prevalence of cyber criminals, who have the ability to use technology for malicious intent; such as breach of critical data, Identity theft, and phishing scams to name a few.

In spite of this, the cybersecurity industry is due to be valued much more than its current value of about $161 billion in the near future as cybersecurity products increase in adoption as more people become aware of the importance of having security on the web and not only it is limited to the big organization since anyone can be a victim of a cybercriminal anywhere, at any time, within minutes.

This industry is here to stay and has much more potential for growth in the future. along with the companies currently operating in it, such as the ones mentioned in this report.

Fernando Rangel, Editor-in-Chief

Industry Outlook Team

Editor-in-Chief: Fernando Rangel

Revision: Fernando Rangel, Tânia Caria

Design: Inês Martins

Analysts: Ana Ratão, Carolina Marques, Fernando Rangel, Ali Aljundi

Our Club

ISCTE Trading & Investment Club (ITIC) is a non-profit student organization of ISCTE Business School, who promotes training and research in Finance and Investment. The club intends to train the best professionals in the industry and promote its analysts by their commitment to producing useful and truthful information and analysis based on excellence.

Find out more content at: **www.itic-iscte.com**