July 21, 2021

Cybersecurity: Increasingly Indispensable

Soner Kistak and Jade Bajai

With so many facets of our daily lives dependent upon digital infrastructures, cybercrime is a growing and considerable threat worldwide, affecting governments, corporations and individuals alike. As the rollout of 5G and successive mobile technologies further digitalise our lifestyles, enhanced digital defence systems will become increasingly indispensable. For investors, this means that cybersecurity may be an interesting and enduring investment theme which merits consideration in portfolios.

A Growing Threat

The first known cyberattack occurred all the way back in 1988, when what became known as the Morris Worm damaged approximately 6,000 computers, representing about 10% of the entire internet at the time. [1][2]

Cybercrime has evolved since then, becoming highly sophisticated and a lucrative source of income for cybercriminals. The umbrella term constitutes a range of activities whether it be intellectual property theft, the targeting of data systems of individuals or businesses for financial gain, the theft of sensitive information or orchestrated disruptions, simply to create panic and discord.

Common types of cybersecurity threats

Malware	A type of software designed to gain unauthorized access to or cause damage to a computer.
Phishing	The practice of sending fraudulent e-mails that resemble those from a reputable source. The aim is to steal confidential or sensitive data, such as bank details and login credentials. *German officials have warned that foreign intelligence agencies could be seeking to influence September's Bundestag election, with a spike in phishing attacks on German MPs and regional politicians.*
Ransomware	A type of software that enables digital extortion by blocking files or systems until a ransom is paid. *US Government agencies were hit with over 31,000 ransomware attacks in 2020*
Social engineering	The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

The Covid-19 pandemic and ensuing lockdowns accelerated the secular trend of digitalization, pushing millions of businesses online essentially overnight. This created fertile ground for cyber criminals to operate.

This year, news headlines have been consumed with stories of ransomware attacks.

- In the US, the Colonial pipeline, a key oil artery, fell victim to a ransomware attack,

causing fuel shortages across the east coast for days. With the assistance of the FBI, Colonial Pipeline paid the requested ransom (75 bitcoin or $4.4 million) within several hours and the hackers delivered a software application to restore their network, but it operated very slowly.

- JBS, the world's largest meat processor, had its IT systems attacked, meaning that the majority of its plants in the US, Canada and Australia were forced to close for around three days, raising alarm about food security. The company paid a ransom of roughly $11m to end the attack.
- Conti ransomware group reportedly asked the Irish health service for $20m (£14m) to restore services after a "catastrophic hack". In the end the Irish government said it did not pay and the systems were restored.
- Computer systems of several companies across the world, including 800 physical grocery stores of Sweden's Coop, were attacked by REvil ransomware with hackers demanding $70 million to restore the data.

More recently, a scandal broke involving Pegasus spy technology which was used to intercept the phones of prominent figures and media personnel. This event shows the vulnerability of our systems and importance of cybersecurity not only against cyberattacks but also for privacy and in countering espionage.

In acknowledging the seriousness of the threat posed by cyberattacks, the US Navy is attempting to bring back celestial navigation techniques alongside modern electronic navigational systems. [3] But broadly, digitalisation will not retreat. Rather, individuals, companies and countries must become well-versed in cybersecurity. They must shift away from reactionary defence mechanisms in that they are perpetually on guard and secured.

Indeed, while the threat from cybersecurity swells, the ecosystem of protective measures is rapidly expanding in tandem. This includes firewalls to keep unauthorized users from accessing private data, the rise of forensic firms that monitor traffic for intrusions and audit systems for weakness, antivirus programs that block malware and viruses, data protection through evolving forms of authentication (encryption, digital signatures, biometrics...), and so on...

More investment flows into advanced cybersecurity systems and innovation is expected as the issue rises to the top of government agendas. Policymakers are becoming increasingly concerned that critical infrastructure such as power plants and hospitals risk being compromised by hackers and are aware that securing critical national infrastructure is essential to keeping society functioning.

Recognising the potential threat, NATO leaders are seeking to modernise their alliance and toughen their response to new high-tech threats.

In May, the US President Biden issued an Executive Order to improve the cybersecurity of federal computer networks with assistance from the private sector. The 18-page document sets

deadlines for named agencies to develop requirements, standards, or guidelines on specific cybersecurity areas with emphasis on identifying, deterring, protecting against, and responding to cybercrime.

"INCREMENTAL IMPROVEMENTS WILL NOT GIVE US THE SECURITY WE NEED; INSTEAD, THE FEDERAL GOVERNMENT NEEDS TO MAKE BOLD CHANGES AND SIGNIFICANT INVESTMENTS IN ORDER TO DEFEND THE VITAL INSTITUTIONS THAT UNDERPIN THE AMERICAN WAY OF LIFE." – EXTRACT FROM BIDEN'S EXECUTIVE ORDER

Here in Europe, the European Commission recently announced a "Joint Cyber Unit," which would allow member states hit by cyberattacks to ask other countries and the EU for assistance, including through rapid response teams that can swoop in and fight off the threat in real time. The plan aims to help countries fight back against increasingly sophisticated attacks by pooling national governments' cybersecurity resources.

As governments race to outsmart hackers, we could see new tailwinds for the industry and a new wave of public-private partnerships and innovation.

Investment Case

Cybersecurity threats are real and they affect everyone. As we try to build up defences, the International Data Corporation (IDC), believes that worldwide spending on security-related hardware, software and services will continue to grow, reaching an estimated $151.2 billion in 2023.

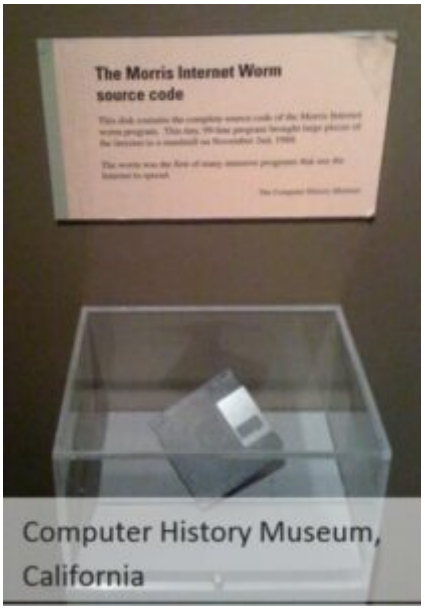
Cybersecurity piggy-backs on the unstoppable trend of digitalization and demand for cybersecurity products looks to accelerate further as new technologies, such as cloud computing, AI, the IoT and 5G proliferate.

While the theme could represent a very interesting opportunity for investors, selecting an optimal way to play it is key. Within the broad theme, you will find a number of traditional companies that are adapting their business models as well as new entrants (there is a vibrant start-up industry in this field), then you have pure plays and companies that are only dipping their toes in this realm. Investors must approach the theme in a way that fits their own individual risk tolerances and preferences.

References

[1]
https://www.nasdaq.com/articles/how-the-pandemic-has-increased-the-need-for-cybersecurity-2020-10-29

[2]



[3]
https://www.npr.org/2016/02/22/467210492/u-s-navy-brings-back-navigation-by-the-stars-for-officers?t=1626772083919

Disclaimer

All financial data and/or economic information released by this Publication (the "Publication"); (the "Data" or the "Financial data and/or economic information"), are provided for information purposes only, without warranty of any kind, including without limitation the warranties of merchantability, fitness for a particular purpose or warranties and non-infringement of any patent, intellectual property or proprietary rights of any party, and are not intended for trading purposes. Banque Internationale à Luxembourg SA (the "Bank") does not guarantee expressly or impliedly, the sequence, accuracy, adequacy, legality, completeness, reliability, usefulness or timeless of any Data. All Financial data and/or economic information provided may be delayed or may contain errors or be incomplete. This disclaimer applies to both isolated and aggregate uses of the Data. All Data is provided on an "as is" basis. None of the Financial data and/or economic information contained on this Publication constitutes a solicitation, offer, opinion, or recommendation, a guarantee of results, nor a solicitation by the Bank of an offer to buy or sell any security, products and services mentioned into it or to make investments. Moreover, none of the Financial data and/or economic information contained on this Publication provides legal, tax accounting, financial or investment advice or services regarding the profitability or suitability of any security or investment. This Publication has not been prepared with the aim to take an investor's particular investment objectives, financial position or needs into account. It is up to the investor himself to consider whether the Data contained herein this Publication is appropriate to his needs, financial position and objectives or to seek professional independent advice before making an investment decision based upon the Data. No investment decision whatsoever may result from solely reading this document. In order to read and understand the Financial data and/or economic information included in this document, you will need to have knowledge and experience of financial markets. If this is not the case, please contact your relationship manager. This Publication is prepared by the Bank and is based on data available to the public and upon information from sources believed to be reliable and accurate, taken from stock exchanges and third parties. The Bank, including its parent,- subsidiary or affiliate entities, agents, directors, officers, employees, representatives or suppliers, shall not, directly or indirectly, be liable, in any way, for any: inaccuracies or errors in or omissions from the Financial data and/or economic information, including but not limited to financial data regardless of the cause of such or for any investment decision made, action taken, or action not taken of whatever nature in reliance upon any Data provided herein, nor for any loss or damage, direct or indirect, special or consequential, arising from any use of this Publication or of its content. This Publication is only valid at the moment of its editing, unless otherwise specified. All Financial data and/or economic information contained herein can also quickly become out-of- date. All Data is subject to change without notice and may not be incorporated in any new version of this Publication. The Bank has no obligation to update this Publication upon the availability of new data, the occurrence of new events and/or other evolutions. Before making an investment decision, the investor must read carefully the terms and conditions of the documentation relating to the specific products or services. Past performance is no guarantee of future performance. Products or services described in this Publication may not be available in all countries and may be subject to restrictions in some persons or in some countries. No part of this Publication may be reproduced, distributed, modified, linked to or used for any public or commercial purpose without the prior written consent of the Bank. In any case, all Financial data and/or economic information provided on this Publication are not intended for use by, or distribution to, any person or entity in any jurisdiction or country where such use or distribution would be contrary to law and/or regulation. If you have obtained this Publication from a source other than the Bank website, be aware that electronic documentation can be altered subsequent to original distribution.

As economic conditions are subject to change, the information and opinions presented in this outlook are current only as of the date indicated in the matrix or the publication date. This publication is based on data available to the public and upon information that is considered as reliable. Even if particular attention has been paid to its content, no guarantee, warranty or representation is given to the accuracy or completeness thereof. Banque Internationale à Luxembourg cannot be held liable or responsible with respect to the information expressed herein. This document has been prepared only for information purposes and does not constitute an offer or invitation to make investments. It is up to investors themselves to consider whether the information contained herein is appropriate to their needs and objectives or to seek advice before making an investment decision based upon this information. Banque Internationale à Luxembourg accepts no liability whatsoever for any investment decisions of whatever nature by the user of this publication, which are in any way based on this publication, nor for any loss or damage arising from any use of this publication or its content. This publication, prepared by Banque Internationale à Luxembourg (BIL), may not be copied or duplicated in any form whatsoever or redistributed without the prior written consent of BIL 69, route d'Esch ı L-2953 Luxembourg ı RCS Luxembourg B-6307 ı Tel. +352 4590 6699 ı www.bil.com.