TEMATICA RESEARCH

Rize etf

Vol /01

A Whitepaper on Cybersecurity and Privacy

A Whitepaper on Cybersecurity and Privacy

Prepared November, 2019

TEMATICA RESEARCH, LLC
research@tematicaresearch.com

TEMATICARESEARCH®

A Whitepaper on Cybersecurity and Privacy

TABBLE OF CONTENTS

EXECUTIVE SUMMARY

The Tematica Research® Cybersecurity & Data Privacy investment theme looks to benefit from the pain points generated by the ever-growing threat of cyber-attacks, pervasive data privacy violations and the impact of the evolving regulatory environment. We have already seen significant growth in global investment in cybersecurity, which is defined as the practice of defending systems, networks, programs, devices and data from malicious cyber-attacks. Cyber-attacks are usually aimed at accessing (and selling), changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

In today's increasingly digitized world, the amount of data accessed, utilized and shared continues to grow across a growing array of connected devices. The dark side of this robust growth in connectivity is the pronounced increase in cyber vulnerabilities and privacy violations. In the case of individuals, this digitized connectivity removes transactional friction and allows for a multitude of conveniences. In the case of businesses and institutions, it is used to drive efficiency, reduce costs and build data-driven businesses that are better suited for the modern world. The issue is a rather simple one in that as digital adoption happens, individuals, businesses move into the cyber-attack zone.

In addition to investments to combat cyber-attacks themselves, enterprises are spending heavily on IT security measures that help respond to new privacy regulations, such as Europe's General Data Protection Regulation (GDPR). The issue of cyber-attacks and privacy violations will be further compounded by new technologies, such as cloud computing, artificial intelligence, IoT and 5G. These technologies will collectively open up new points of vulnerability and allow for new forms of attacks. Like many aspects of the 21st century what we are doing essentially hasn't changed. How we are doing these things, however, is where it gets interesting and oftentimes complicated.

> *Like many aspects of the 21st century what we are doing essentially hasn't changed. How we are doing these things, however, is where it gets interesting and oftentimes complicated.*

There is little question that cybersecurity is a growth market with individuals, companies and other institutions looking to ward off future attacks, shore up their existing cyber defenses, assess attack and intrusion analytics and become more secure.

This all translates to one thing: security spending. Cybersecurity is of course rooted in security. The following is a primer on the basic elements of security.

A BRIEF HISTORY OF SECURITY

For over a millennia humans have been trying to improve how to safeguard goods and information, including secure delivery and verified receipt. Clay, and later wax, seals have been in use globally from at least 7,000 B.C. up until the 19th century[1] as a means to ensure that documents were original, untampered with and received by the intended recipient (via sealed return receipt of course). A key aspect to this evolution included not only a means to secure the information, but also to increase the speed of delivery as well.

Enter the electric telegraph.

Although initially conceived in the 18th century, the electric telegraph was commercialized and came into wide use only in the 19th century[2]. On the face of it, communicating via telegraph was as fast as one could communicate, and being a wired network, it offered the security of direct, end-to-end communication. However, intercepting messages was as simple as physically tapping into the cable and setting up another receiving station.

In the early 20th century, as Guglielmo Marconi was demonstrating his wireless telegraph, saboteurs hijacked the frequency used in the demonstration and managed to broadcast their own message, essentially insulting Marconi (figuratively and literally) with his own creation[3]. Further into the 20th century, while the telephone established itself as the next step in the evolution of communication technology, it unfortunately still shared the same security issues as its predecessors. Intercepting phone calls was as easy as finding any point along the miles and miles of cable and connecting a listening device to it in order to capture all the traffic along the route.

Fast forward to today, and wireless communication security can be just as easily be compromised by simply setting up a receiving station and identifying what frequency to monitor. Indeed

A publicity photo of Italian radio pioneer Guglielmo Marconi posing in front of his early wireless telegraph

modern communication presents a host of security issues, and users have increasingly turned to another age-old means of securing communications — cryptography.

Cryptography relies on the use of a cypher to decrypt an encoded message. Implementing cryptographic solution can be as simple as the childhood "code" of speaking in "Pig Latin" — the cypher being to move the first letter of a word to the end of that word and add an "ay" sound, or, as one would say, speaking "Ig-pay Atin-lay". A cypher can also be as complicated as a modern-day 128-bit key, which has approximately 3.4e+38 keys or 340 billion billion billion billion possible solutions![4]

AUTHENTIFICATION – IS DIGITAL MORE SECURE?

Historically, authenticating the recipient of a message was fairly straightforward, as important messages would be hand-delivered or at least delivery would follow some chain of custody protocol.

In 1993, The New Yorker published a now famous cartoon of two dogs in an office with one dog sitting at a desk, paw on a keyboard, explaining to the other dog that, "On the internet, nobody knows you're a dog."[5] While this may be true of the users of the internet, authentication technology with regards to access rights to systems and information ensures that the appropriate user (human, dog, or otherwise) has approved access.

Today, authentication involves not only confirming the user account has access rights to the information, but that the device they are using has rights to the network where the information is stored and further, that the user himself/herself is the approved account user. This becomes important as we think about data privacy in the modern world.

HOW COMMUNICATION HAS EVOLVED

As the methods of communication have evolved over time, so has the information we are communicating. Up until approximately 50 years ago, messages were generally limited to actionable information including directions, instructions, forecasts and the like. Since then, the proliferation of digital data has meant that "messages" today include almost anything ranging from preferences, photos, movies, transactions, health records to other personal information.

Regarding more traditional messages, it wasn't too long ago that publicly available information was somewhat limited, at least by current standards. One could find a person's address and phone number only if you could get a copy of the local telephone directory. If the person you were looking for had a common name, you would have fun dialing your way through the *n* similarly named entries in the phone book to find the person you were looking for.

As for private and personal data, bank records were in one of three places:

- Your bank
- Your home if you held on to your statements
- In the local landfill if you threw the statements in the trash.

State or local government identification could be found at the appropriate records office or in your wallet/purse. Similarly, medical data could be found at your doctor's office and, if you requested a copy, your home. Other personal information, such as when and where you might go for your morning run, your taste in music, taste in movies or television programs, frequented restaurants, and other items could only be determined by interviewing the person or interviewing witnesses (if you could find them).

While libraries have long been a source for information about individual interests, the advent of search engines from Infoseek to Yahoo to Alta Vista to Google allowed companies and, by extension, governments to have records of every topic searched by every user, including the time that it happened and with some extrapolation, the place where it happened. As much as search engines are a means to discern what individuals may or may not be contemplating, social media companies have taken this thing to a whole other level. What's more incredible is that all of this information has been provided on a purely voluntary basis.

The point is that as our lives become increasingly digitized, more and more information about "us" — some of it quite personal — exists in cyberspace where it is potentially accessible by those with nefarious intent.

> *As our lives become increasingly digitized, more and more information about "us" exists in cyberspace where it is potentially accessible by those with nefarious intent.*

FROM COMMUNICATION TO DATA GATHERING / SURVEILLANCE

Another aspect of modern-day digitization is that, up until the turn of the century, spontaneous and autonomous generation of data was generally limited to commercial ventures like manufacturing sensors used to monitor production environments or positional data used to facilitate the proper functioning of communication networks. Systems and sensors that in the past would record limited amounts of commercially critical data now capture huge amounts of data that up until the turn of the century was considered ephemeral.

New age systems include the launch of Facebook in 2004[6], Twitter in 2006[7], Instagram in 2010[8], Snapchat in 2011.[9] New age sensors include devices like Fitbit (2007), Amazon Alexa (2014) and all of their subsequent imitators. Straddling the line between systems and sensors lies the "smartphone". While cellphones have long had the ability to provide locational information, it wasn't until the launch of the first iPhone in 2008 that consumers, companies and governments started to understand the potential of all the data that was being generated by smartphones.

The digital transformation of our society — or the digitalization of everything by way of the internet of things (IoT) as it is referred to — spans beyond the individual. Several industries, including but not limited to aerospace, manufacturing, and healthcare, have used digitalization to enhance their operations and customer responsiveness to gain a variety of operational advantages. We are also seeing technology companies and their businesses bleed over into other industries such as financial services and healthcare. In both cases, the growing pervasiveness of digitization gives rise to a growing number of attack vectors and threats that have the potential to disrupt and compromise individuals, companies, governments as well as other institutions.

THE WORLD IS WAKING UP TO THE SECURITY PROBLEM

In today's increasingly digitized world, the amount of data accessed, utilized and shared continues to grow across a growing array of connected devices. In this evolving world, consumers are increasingly concerned about the privacy of their personal data given the growing adoption of online accounts with financial providers such as a bank, utility, or service provider. Consumers are also concerned about their own vulnerability and that of the companies that house their private information. They are also concerned about threats to government institutions and cities as well.[10] This is giving rise to data security and data privacy initiatives across individuals, companies, government and other institutions to ward off cyber-attacks.

CYBERSECURITY

As stated earlier, cybersecurity is defined as the practice of defending systems, networks, programs, devices and data from malicious cyber-attacks. In light of our historical conversation we can say that cybersecurity concerns itself with:

- Securing communications infrastructure, physical or otherwise;
- Securing the contents of communications; and
- Authentication of approved recipients of those communications.

Let's now take a look at the main types of attacks:

Attacks on Infrastructure

- **Denial-of-Service (DoS) Attack** – In a Denial-of-Service (DoS) attack, an attacker floods systems, servers or networks with traffic that exhausts resources and bandwidth, resulting in a breakdown of service (or service denial). In a Distributed Denial-of-Services (DDoS) attack, which is equally common, the attack is launched from a large number of host machines that have been infected by malicious software that is being controlled by the attacker. Unlike with other types of attacks, DoS and DDoS attacks do not provide direct benefits to the attacker, outside of the pleasure of denying service. However, they have been seen to be used in business-to-business 'competition warfare' where one company is trying to get an upper edge over another.
- **Man-in-the-Middle (MitM) Attack** – A Man-in-the-Middle (MitM) attack occurs when an attacker inserts him or herself between a two-party communication. Once the attacker interrupts the traffic, they can filter and steal data. The most common point of entry for a MitM attack is an unsecure public Wi-Fi network. An attacker will set up a Wi-Fi connection with a legitimate-sounding name and all they need to do is to wait for someone to connect. Once that connection is made, the attacker will get instant access to the connected device.

Attacks on Message Contents

- **SQL Injection** – A SQL Injection, or a Structured Query Language injection, occurs when an attacker inserts malicious code into a server that uses SQL (a domain-specific language) and forces the server to reveal information it normally would not. [4] SQL injections are only successful when a security vulnerability exists in an application's software.
- **Malware** – Malware is a term used to describe malicious software such as ransomware, spyware, adware, viruses, infectors and worms. Malware attacks use a code that is made to stealthily affect a compromised computer system without the consent or knowledge of the user. Typically, these attacks breach a network through some vulnerability, such as when a user clicks on a dangerous link or email attachments, which then installs malicious software.
- **Drive-By Attack** – Drive-By Attacks target users through their internet browser, installing malware on their computer as soon as they land on an infected webpage. These attacks can also occur where a user visits a legitimate webpage that has been compromised, either by infecting the user directly or by redirecting them to another, legitimate-looking webpage that has been compromised.
- **Ransomware** – Ransomware is the most common type of malware. It is found in 39% of malware-related data breaches, according to Verizon's 2018 Data Breach Investigations Report.[1] The report also highlights that ransomware has become so commonplace that would-be criminals now have access to off-the-shelf toolkits that allow them to create and deploy ransomware in a matter of minutes.

Attacks on Authentication:

- **Phishing** – Phishing is the practice of sending fraudulent communications that appear to be coming from a reputable source, generally via email. The attacker's objective is to steal sensitive data such as login credentials and credit card numbers, or to install malware on the victim's machine.
- **Social Engineering** – In the age of passwords, personal information is often the key to deciphering passwords. To that end seemingly innocuous items like information about family, pets, hobbies, travel, etc. provide opportunities to figure out how a person may think or prioritize when creating passwords.
- **User Error** – While not an attack *per se* user error, sometimes referred to in technology circles as "ID-10.T" errors, can be responsible for the inadvertent public release of restricted information. Examples include users leaving written passwords out in the open, leaving sensitive systems unsecured, losing prototype devices, discussing sensitive information in public areas. The list is seemingly endless.

EXAMPLES OF RECENT CYBER-ATTACKS

In October 2012, then Defense Secretary Leon E. Panetta warned that the US was facing the possibility of a "Cyber Pearl Harbor". He emphasized the country's increasing vulnerability to foreign hackers who have the ability to dismantle the nation's power grid, transportation system, financial networks and even the government[11]. Little did Secretary Panetta realize the extent to which cyber-attacks would become commonplace in the years ahead, as businesses, governments and other institutions moved increasingly into the digital world.

- In May 2017, the infamous "WannaCry" ransomware spread like wildfire across the globe in what was dubbed the worst cyber-attack in history. The attack targeted computers running Microsoft Windows, by infecting and encrypting files on the PC's hard drive (in turn making them impossible to access), and then demanding a ransom payment (in bitcoins!) in order to decrypt them.[12]
- Nearly a quarter of Americans, 23%, say that they or someone in their household had their personal, credit card or financial information stolen by computer hackers in 2018.[13]
- In 2018, Singapore suffered an unprecedented attack on its public healthcare IT systems that compromised the data of about 160,000 patients. The attack followed similar data exfiltration efforts in other countries across the region, including the massive data breach that hit Malaysian telecommunications in 2017.[14]
- In the spring of 2018, the city of Atlanta, Georgia suffered a ransomware attack at the hands of SamSam, crypto malware that according to the US Department of Justice caused $30 million in losses to US hospitals, municipalities, institutions, and other victims. The cyber-attack affected more than a third of the 424 computer applications used by Atlanta and thus prevented the city government from delivering a host of public services.[15]

> *Before September 11, 2001, the warning signs were there. We weren't organized. We weren't ready and we suffered terribly for that lack of attention. We cannot let that happen again. This is a pre-9/11 moment.*

Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City, October 11, 2012

- In June 2019, hackers launched a ransomware cyber-attack in Lake City, Florida, that disabled the city's computer systems.[16] The attack persisted for several days until city leaders called an emergency meeting and approved paying the hackers the ransom they demanded: 42 Bitcoin, worth approximately $460,000 at the time. That was the second such reported attack in as many weeks — the prior week, Rivera Beach, Florida signed off on an extraordinary $600,000 payment, also in Bitcoin.[17]
- More recently, meal delivery service provider Door Dash was breached, resulting in information related to 4.9 million customers, delivery executives and restaurants potentially being leaked.[18]

GREATER CONNECTIVITY MEANS GREATER VULNERABILITY

At the start of the 21st Century, there were less than 250 million global internet users. In the following 20 years, that user base exploded to 4.5 billion by June 2019, roughly 59% of the global population according to data published by Internet World Stats.[19] Over the last two decades, consumers and businesses have flocked to the internet to transact, shop, stream, communicate and digest information and other content. The current Cisco Visual Networking Index (VNI), which measures and projects IP traffic volume growth, calls for global IP traffic to nearly triple between 2017 to 2022.[20]

A key driver in this growth will be the exponentially rising number of connected devices per household and per person. By 2022, the number of networked devices and connections per person is forecasted to reach 3.6, up from 2.4 in 2017.[21]

Each year, various new devices in different form factors with increased capabilities and intelligence are introduced and adopted by the market. A growing number of Machine to Machine (M2M) applications, such as smart meters, video surveillance, healthcare monitoring, transportation, and package or asset tracking, are contributing in a major way to the growth in devices and connections. By 2022, M2M connections will be 51% of total devices and connections.[22]

The dark side of this robust growth in connectivity is the pronounced increase in cyber vulnerabilities and privacy violations. In the case of individuals, this digitized connectivity removes transactional friction and allows for a multitude of conveniences. In the case of businesses and institutions, it is used to drive efficiency, reduce costs and build data-driven businesses that are better suited for the modern world. The issue is a rather simple one in that as digital adoption happens, individuals, businesses move into the cyber-attack zone. These security and privacy concerns are some of the reasons why 22% of UK broadband users haven't yet installed a smart home device and don't plan to purchase one either, according to Park Associates.[23]

> *The dark side of this robust growth in connectivity is the pronounced increase in cyber vulnerabilities and privacy violations.*

DATA PRIVACY: THE NEXT FOCUS AREA FOR CYBER SPENDING

Spending in the consumer category of cybersecurity includes:

- Personal identity theft protection services.
- Computer and mobile phone repair services specific to malware and virus removal.
- Installation of antivirus and malware protection software.
- Post-breach services including data recovery, and user education on best practices for personal cyber defense.

Data privacy concerns have become a key factor for consumers and are expected to drive the global privacy management software market to $1.6 billion by 2027, up from $521 million in 2018, according to research published by ResearchAndMarkets. [24]

Research published by Statista recently found that 53% of online users worldwide are concerned about their online privacy.[25] According to the new Deloitte US Consumer Data Privacy study, nearly half of US consumers (47%) feel they have little to no control over their personal data, and one in three has had their data compromised. Perhaps it's not therefore surprising that the vast majority (86%) of consumers feel they should have the ability to opt-out of selling their data.[26]

> *According to the new Deloitte US Consumer Data Privacy study, nearly half of US consumers (47%) feel they have little to no control over their personal data, and one in three has had their data compromised.*

PRIVACY REGULATIONS SPUR CYBER SPENDING

In addition to investments to combat cyber-attacks themselves, enterprises are spending heavily on IT security measures that help respond to new privacy regulations, such as Europe's General Data Protection Regulation (GDPR). A recent Spiceworks survey showed that IT leaders agreed with a recent survey published by Gartner that found the top two factors driving IT budgets were increased security concerns and changes in regulation.

Other data, including some published by Proofpoint, an enterprise cybersecurity firm, showed that while 56% of companies reported having increased security concerns, 37% were busy focusing on complying with changes in regulations.[27] Recent findings from Cisco Systems, another major cybersecurity company, also point to the fact that executives are increasingly viewing regulations and compliance as key drivers for cybersecurity spending going forward.[28]

. . . while 56% of companies reported having increased security concerns, 37% were busy focusing on complying with changes in regulations.

Because GDPR regulations cover any company doing business in the EU, they affect companies around the globe and hold them responsible for the improper handling of people's personal information. In recent years, there have been scores of massive data breaches, including millions of Yahoo!, LinkedIn, and MySpace account details. Under GDPR, the "destruction, loss, alteration, unauthorized disclosure of, or access to" people's data has to be reported to a country's data protection regulator.

The most talked about aspects of GDPR is the ability for regulators to fine businesses that fail to comply with the regulations. If an organization doesn't safeguard or process an individual's data correctly, it can be fined. If it's required to, and an organization doesn't have a data protection officer, it can be fined. If there's a security breach, it can be fined. GDPR fines (administrative fines) can be as high as €20 million or 4% of annual global turnover, whichever is highest. Before GDPR's enforcement, the maximum fine for any data protection violation was £500,000 ($624,000) – as Facebook experienced when it was fined that amount in July 2018.[29]

GDPR fines (administrative fines) can be as high as €20 million or 4% of annual global turnover, whichever is highest.

So far there have been several high profile GDPR fines awarded. British Airways faced a record $230 million fine after its website failure compromised the personal account details of roughly 500,000 customers.[30] That $230 million fine is roughly 1.5% of British Airways' annual revenue. Separately, Marriott International was slapped with a fine of just over $124 million for exposing a variety of personal data in 339 million guest records globally.[31]

MORE PRIVACY REGULATION IS COMING, GLOBALLY

In the United States, a similar regulation has been passed in the California Consumer Privacy Act (CCPA). A draft is undergoing a public consultation period, including several public hearings, with submissions open until December 6, 2019. The CCPA is set to go into effect on January 1, 2020 with final guidelines expected by July 1, 2020.[32]

The CCPA law will require an "opt-out" button on every page of every website, allowing consumers to easily tell companies that they don't want any of their data to be harvested, managed and/or sold.

The CCPA is bringing with it a host of new regulations that will significantly restrict how brands collect and manage the consumer data that has fueled the growth in digital advertising. The law will require an "opt-out" button on every page of every website, allowing consumers to easily tell companies that they don't want any of their data to be harvested, managed and/or sold. Consumers can also tell tech companies, publishers or brands to delete their data. People may also opt-out of a company's terms of service without losing access to its offerings. Companies are also barred from selling data on anyone under the age of 16 without explicit consent.

In terms of fines for those found violating these and other associated regulations, the CCPA sets out a per user fine of $100 - $750 or actual damages (whichever is larger) for even an unintentional breach. What this means is a relatively small web service with 1 million accounts could be fined $100 - $750 million, a sum that could put them out of business.

And as the CCPA marches toward finalization and implementation, additional American legislation is winding its way through various statehouses in the US. The next state to watch will be New York with its Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) that goes into effect in March 2020.[33] The SHIELD Act expands the definition of "personal information." Before the SHIELD Act, personal information included "any information concerning a natural person which, because of name, number, personal mark, or other identifiers, can be used to identify such natural person." The SHIELD Act's expanded definition includes personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted or is encrypted with an encryption key that has also been accessed or acquired:

- Social security number;
- Driver's license number or non-driver identification card number;
- Account number, credit or debit card number, in combination with any required security code, access code, password or other information that would permit access to an individual's financial account; account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password;
- Biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity; or
- A username or e-mail address in combination with a password or security question and answer that would permit access to an online account.[34]

The state of New York isn't the only state to expand the definition of "private information." Illinois, Oregon, and Rhode Island have also expanded their definitions to include not only medical information but also certain health insurance identifiers. [35]

We are in the early stages of what looks to be far more reaching regulatory requirements that will drive robust demand for security and privacy products, as companies try to counter increasingly sophisticated attacks and protect data from breaches that could lead to steep penalties.

CYBERSECURITY WILL CONTINUE TO GROW

What this means is that cybersecurity spending is set to grow. We are in the middle of a cyber-boom as new attack vectors emerge, and new countermeasures are developed. We see this reflected in forecasts that suggest cybercrime will cost $6 trillion annually by 2021, up from $3 trillion in 2015, according to Cybersecurity Ventures.[36] That forecast includes costs associated with the damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption, forensic investigation, restoration of hacked data and systems, as well as reputational harm.

The issue of cyber-attacks and privacy violations will be further compounded by new technologies, such as cloud computing, artificial intelligence, IoT and 5G. These technologies will collectively open up new points of vulnerability and allow for new forms of attacks.

In terms of potential vulnerabilities, the IoT market alone, which includes connected devices ranging from cars and factory assembly lines to baby monitors and traffic lights as well as smart appliances, smoke alarms and other smart devices connected to the internet, is expected to reach 25 billion devices by 2021, according to data compiled by Gartner.[37] To put some perspective around that, Cybersecurity Ventures expects a business will fall victim to a ransomware attack every 11 seconds by 2021, up from one every 14 seconds in 2019, and one every 40 seconds in 2016.[38]

The issue of cyber-attacks and privacy violations will be further compounded by new technologies, such as cloud computing, artificial intelligence, IoT and 5G.

That offers some context for why cyber-attacks were named the leading risk by business executives in the US, Canada, and Europe, according to a survey of business leaders published by the World Economic Forum, in partnership with Zurich Insurance Group and Marsh & McLennan.[39]

It comes as little surprise that decision-makers include cybersecurity among their top considerations when it comes to digital transformation. We see this sentiment reflected in several cybersecurity spending forecasts:

- Gartner expects worldwide, IT security spending in 2019 to have grown 8.7% to $124 billion vs. 2018. Gartner also sees security services accounting for 50% of cybersecurity budgets by 2020, with key investment areas security services, infrastructure protection, and network security equipment.[40]
- Worldwide spending on information security (a subset of the broader cybersecurity market) products and services exceeded $114 billion in 2018, and according to Gartner that market will $170.4 billion in 2022.[41]
- Global spending on security awareness training and phishing simulation programs for employees – one of the fastest-growing categories in the cybersecurity industry – is predicted to reach $10 billion by 2027, up from around $1 billion in 2014.[42]
- MarketsandMarkets forecasts the cybersecurity market will hit $248.3 billion by 2023, growing at a 10% CAGR during the 2018–2023 period.[43]
- Cybersecurity Ventures predicted that global cybersecurity spending will exceed $1 trillion cumulatively from 2017 to 2021.[44]
- According to an updated forecast from the International Data Corporation (IDC) Worldwide Semiannual Security Spending Guide, worldwide spending on security-related hardware, software, and services will rise 10.7% in 2019 to $106.6 billion and will continue growing, reaching $151.2 billion in 2023.[45]

According to IDC, worldwide spending on security-related hardware, software, and services will rise 10.7% in 2019 to $106.6 billion and will continue growing, reaching $151.2 billion in 2023.

CONCLUSION

In our view, there is little question that cybersecurity is a growth market with individuals, companies and other institutions looking to ward off future attacks, shore up their existing cyber defenses, assess attack and intrusion analytics and become more secure.

This all translates to one thing: security spending. While the actual dollar amounts may vary, what all of these forecasts have in common is an upward vector and accelerating velocity with cybersecurity spending accounting for more of the overall IT spending budget. Per Gartner, general IT spending is slated to grow by 3.2% in 2019 compared to 8.7% for cybersecurity.[46]

Those trajectories point to continued cyber spending growth given that cybersecurity is an arms race with bad actors looking to exploit new vulnerabilities with newfound forms of attacks. History would suggest however that industry spending forecasts have been too conservative. For example, in 2017, Gartner forecast that spending would increase to $93 billion in 2018. In mid-2018, Gartner revised that spending forecast to $114 billion for all of 2018.[47] Data per Gartner shows that even that upward revision fell modestly below the $114.1 billion that was spent during 2018. All of this bodes rather well for Tematica Research's Cybersecurity & Data Privacy investing theme.

Important Disclosures and Certifications

Analyst Certification - The author certifies that this research report accurately states his/her personal views about the subject securities, which are reflected in the ratings as well as in the substance of this report. The author certifies that no part of his/ her compensation was, is, or will be directly or indirectly related to the specific recommendations or views contained in this research report. Investment opinions are based on each stock's 6-12 month return potential. Our ratings are not based on formal price targets, however, our analysts will discuss fair value and/or target price ranges in research reports. Decisions to buy or sell a stock should be based on the investor's investment objectives and risk tolerance and should not rely solely on the rating. Investors should read carefully the entire research report, which provides a more complete discussion of the analyst's views. This research report is provided for informational purposes only and shall in no event be construed as an offer to sell or a solicitation of an offer to buy any securities. The information described herein is taken from sources, which we believe to be reliable, but the accuracy and completeness of such information is not guaranteed by us. The opinions expressed herein may be given only such weight as opinions warrant. This firm, its officers, directors, employees, third party data providers or members of their families may have positions in the securities mentioned and may make purchases or sales of such securities from time to time in the open market.

Endnotes

[1] Collon (ed.), Dominique (1997). 7000 Years of Seals. London: British Museum Press, p225

[2] E.A. Marland, Early Electrical Communication, Abelard-Schuman Ltd, London 1964, pp17-19

[3] "The Great Wireless Hack 1903" Available at https://www.theatlantic.com/technology/archive/2011/12/the-great-wireless-hack-of-1903/250665/

[4] "128-Bit Encryption" Available at https://www.techopedia.com/definition/29708/128-bit-encryption

[5] The New Yorker cartoon by Peter Steiner, 1993

[6] "From Alibaba to Google, here are the 10 biggest tech IPOs of all time" Available at https://yourstory.com/2018/02/biggest-tech-ipo-of-all-time/

[7] ibid

[8] "Our story" Available at https://instagram-press.com/our-story/

[9] "From Alibaba to Google, here are the 10 biggest tech IPOs of all time" Available at https://yourstory.com/2018/02/biggest-tech-ipo-of-all-time/

[10] ZDNet, "Most consumers have cybersecurity concerns, but a fraction take action", 2018. Available at https://www.zdnet.com/article/most-consumers-have-cyber-security-concerns-but-a-fraction-take-action/

[11] The New York Times, "Panetta Warns of Dire Threat of Cyberattack on U.S.", 2012. Available at https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html

[12] CSO, "The 6 biggest ransomware attacks of the last 5 years", 2019. Available at https://www.csoonline.com/article/3212260/the-5-biggest-ransomware-attacks-of-the-last-5-years.html

[13] Gallup, "One in Four Americans Have Experienced Cybercrime", 2018. Available at https://news.gallup.com/poll/245336/one-four-americans-experienced-cybercrime.aspx

[14] The Straits Times, "Info on 1.5m SingHealth patients stolen in worst cyber attack", 2018. Available at https://www.straitstimes.com/singapore/info-on-15m-singhealth-patients-stolen-in-worst-cyber-attack

[15] The New York Times, "A Cyberattack Hobbles Atlanta, and Security Experts Shudder", 2019. Available at https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html

[16] The Hacker News, "Two Florida Cities Paid $1.1 Million to Ransomware Hackers This Month", 2019. Available at https://thehackernews.com/2019/06/florida-ransomware-attack.html

[17] IBID

[18] CNBC, "DoorDash hack leaks data of 4.9 million customers, restaurants", 2019. Available at https://www.cnbc.com/2019/09/27/doordash-hack-leaks-data-of-4point9-million-customers-restaurants.html

[19] Internet World Stats. Available at https://www.internetworldstats.com

[20] Cisco Systems, "Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper"

Available at https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html

[21] IBID

[22] Cisco Systems, "Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper" Available at https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html

[23] Park Associates, "U.K. smart home adoption lagging compared to the U.S.", 2018. Available at https://www.parksassociates.com/newsletter/article/ca-nov18

[24] ResearchAndMakets, "Privacy Management Software Market to 2027", 2019. Available at https://www.researchandmarkets.com/reports/4762324/privacy-management-software-market-to-2027#pos-0

[25] Statista, "Online privacy - Statistics & Facts", 2109. Available at https://www.statista.com/topics/2476/online-privacy/

[26] Chain Store Age, "Deloitte: Consumers seek control of personal data", 2019. Available at https://chainstoreage.com/deloitte-consumers-seek-control-personal-data

[27] Proofpoint, "Understanding Email Fraud". Available at https://www.proofpoint.com/sites/default/files/pfpt-us-tr-survey-of-understanding-email-fraud-180315.pdf

[28] Cisco System, "Maximizing the value of your data privacy investments", 2019. Available at https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/dpbs-2019.pdf

[29] The Guardian, "UK fines Facebook £500,000 for failing to protect user data", 2018. Available at https://www.theguardian.com/technology/2018/oct/25/facebook-fined-uk-privacy-access-user-data-cambridge-analytica

[30] CNN, "British Airways faces $230 million fine. It would be a record under Europe's tough data privacy law", 2019. Available at https://www.cnn.com/2019/07/08/tech/british-airways-gdpr-fine/index.html

[31] Compliance Week, "Marriott reveals $124M GDPR fine for data breach", 2019. Available at https://www.complianceweek.com/data-privacy/marriott-reveals-124m-gdpr-fine-for-data-breach/27373.article

[32] CNBC, "California AG tells businesses like Facebook and Google how they must comply with the state's new landmark privacy law", 2019. Available at https://www.cnbc.com/2019/10/11/california-attorney-general-outlines-rules-for-state-privacy-law-ccpa.html

[33] JD Supra, "SHIELD Act Overhauls New York's Data Privacy Framework", 2019. Available at https://www.jdsupra.com/legalnews/shield-act-overhauls-new-york-s-data-33724/

[34] Workplace Privacy, Data Management & Security Report, "New York Enacts the SHIELD Act", 2019. Available at https://www.workplaceprivacyreport.com/2019/07/articles/data-breach-notification/new-york-enacts-the-shield-act/

[35] IBID

[36] Cybersecurity Ventures, "Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021", 2018. Available at https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[37] Network World, "Gartner's top 10 IoT trends for 2019 and beyond", 2018. Available at https://www.networkworld.com/article/3322517/a-critical-look-at-gartners-top-10-iot-trends.html

[38] Cybersecurity Ventures, "Global Cybercrime Damages Predicted To Reach $6 Trillion Annually

By 2021", 2018. Available at https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

39 Insurance Journal, "Cyber-Attacks Named as Top Business Risk in U.S., Canada and Europe, by WEF Survey", 2019. Available at https://www.insurancejournal.com/news/international/2019/10/01/541672.htm

40 Security Intelligence, "11 Trends to Inform Your 2020 Cybersecurity Budget", 2019. Available at https://securityintelligence.com/articles/11-stats-on-ciso-spending-to-inform-your-2020-cybersecurity-budget/

41 Cybersecurity Ventures, "Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021", 2018. Available at https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

42 IBID

43 MarketsandMarkets, "Cybersecurity Market worth $248.3 billion by 2023", 2019. Available at https://www.marketsandmarkets.com/PressReleases/cyber-security.asp

44 Cybersecurity Ventures, "Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021", 2018. Available at https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

45 IDC, "New IDC Spending Guide Sees Solid Growth Ahead for Security Products and Services", 2019. Available at https://www.idc.com/getdoc.jsp?containerId=prUS45591619

46 Gartner, "Gartner Says Global IT Spending to Grow 3.2 Percent in 2019", 2019. Available at https://www.gartner.com/en/newsroom/press-releases/2018-10-17-gartner-says-global-it-spending-to-grow-3-2-percent-in-2019

47 IBID