INDUSTRY REPORT

The Third Evolution of Cybersecurity: How Security Threats and Cyber Defenses Shifted Over the Years

SHARESPOST

Table of Contents

Contacts:

For more information on transacting in the private market:

Jennifer Phillips
Managing Director,
Private Securities Group

Email: **jphillips@SharesPost.com**
Tel: **650.492.6885**

For information on research and analysis:

Rohit Kulkarni
Managing Director,
Investment Research Group

Email: **rkulkarni@SharesPost.com**
Tel: **650.300.5128**

For important disclosures and analyst certification, please see page 20

Executive Summary

Unlike other rapidly growing industries, the cybersecurity industry already features a developed ecosystem with important public and private companies at all stages of maturity. Even as some major incumbents decline, startups rapidly grow to fill new niches. Large tech firms then swallow these upstarts just as quickly.

Over the past decade, consumers and enterprises have fundamentally changed the way they access applications and data. The ubiquity of laptops, smartphones, and other connected devices has caused a surge in the number of endpoints and ways for cybercriminals to gain access to private networks and systems. As a result, the entire cyber battlefield has grown in both complexity and scope.

> "Cybersecurity risk is uncharted territory. It's going to get worse, not better"
>
> Warren Buffett
> (Berkshire Hathaway 2018 Annual Shareholder Meeting, May 5th, 2018)

In order to understand the future of cybersecurity, we must look at the industry as a whole – both from a technological and societal standpoint. In this report, we focus on six key areas of inquiry that investors should consider so they can make intelligent investment decisions.

Understanding Cybersecurity: What is cybersecurity, and how does it relate to the broader IT security industry? Why are there so many cybersecurity companies today, and how do they serve the needs of companies across all sectors?

The Evolution of Cybersecurity: New Perspectives: How has cybersecurity changed over the years? How do innovative new companies compete against well established giants in this rapidly evolving environment?

Trends in Hacking Activity & Data Breaches: How are cyber threats today different from those of years past? How can we quantify trends in "hacks" and data breaches? What impact do cybersecurity breaches have on companies and consumers today?

Current Technical Trends in Cybersecurity: What current technical trends are likely to shape the future of cybersecurity in the immediate future and beyond? What are the underlying secular trends that continue to drive innovation in the industry?

Regulatory Trends and Concerns in Cybersecurity: What role does government play in the cybersecurity industry, and what areas are most likely to see increased regulation in the future? What are the driving forces behind the increasing regulatory scrutiny of cybersecurity practices?

Understanding the $100 Billion Dollar Cybersecurity Market: Can we accurately estimate the overall market potential for cybersecurity companies? What do current cybersecurity spending trends tell us about areas of opportunity in the future?

Understanding Cybersecurity - Industry Overview

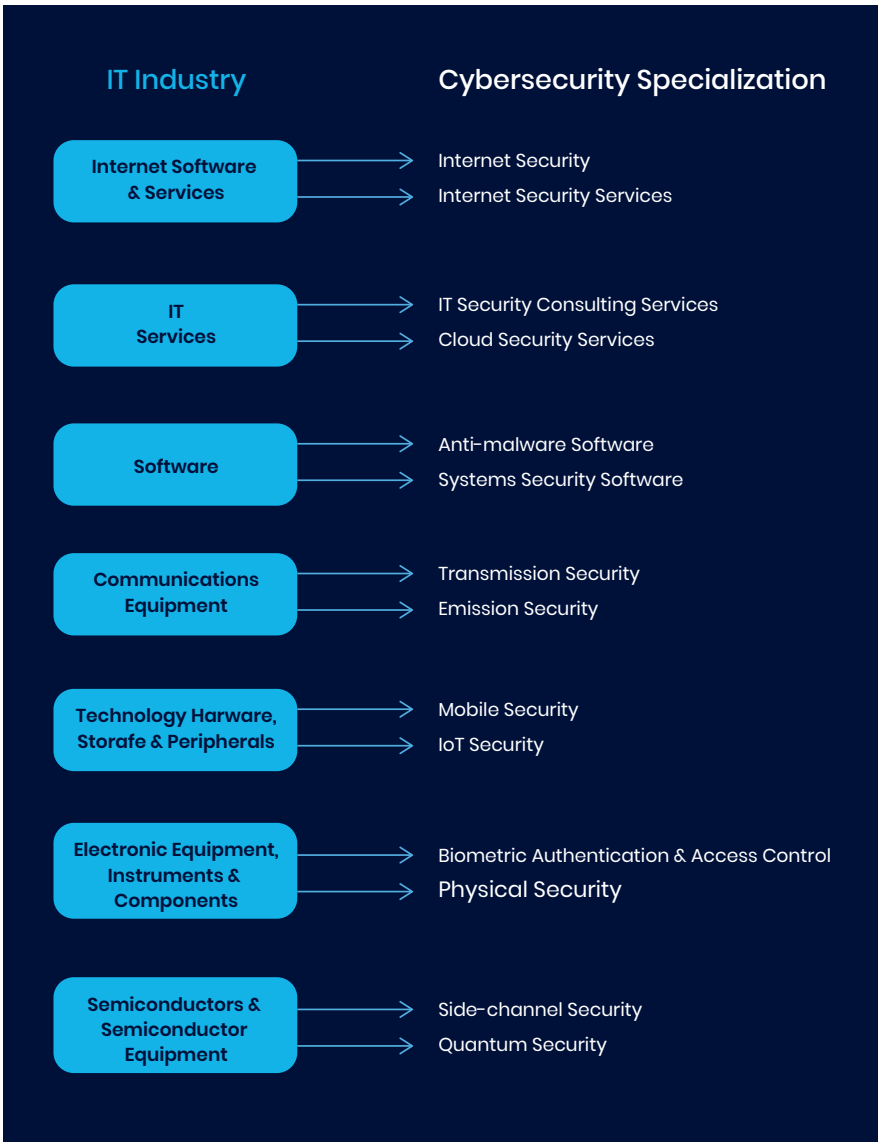
What is cybersecurity, and how does it relate to the broader IT industry? Why are there so many cybersecurity companies today, and how do they serve the needs of companies across all sectors?

Cybersecurity, also known as Information Technology (IT) security, is the set of techniques, tools, and regulations used to protect digital hardware, software and data from unwanted access, damage, or theft. As such, the cybersecurity industry is an integral part of the broader IT industry. Generally, cybersecurity is defensive in nature: it anticipates, detects, and responds to cyber threats. Sometimes, cybersecurity offers offensive capabilities in that it tracks, attacks, and eliminates digital threats.

Since cybersecurity touches nearly every aspect of IT, companies cannot be lumped into any single industry or sub-industry. Pure play cybersecurity companies exist along with dedicated cybersecurity divisions of larger corporations. Exhibit 1 shows how cybersecurity specializations relate to the corresponding IT industries defined by MSCI and Standard and Poor's Global Industry Classification Standard (GICS). Cybersecurity specializations are so varied because the IT industry itself is so varied. For example, software companies like Microsoft have very different cybersecurity needs than hardware companies such as Intel. Whereas Microsoft must secure its suite of consumer software offerings and dedicated cybersecurity software, Intel must secure its line of processors and other hardware.

Despite that cybersecurity is often implemented at the software level, recent hardware vulnerabilities such as "Meltdown" and "Spectre" highlight the importance of these other specializations.

Exhibit 1: Cybersecurity and the IT Industry [1]

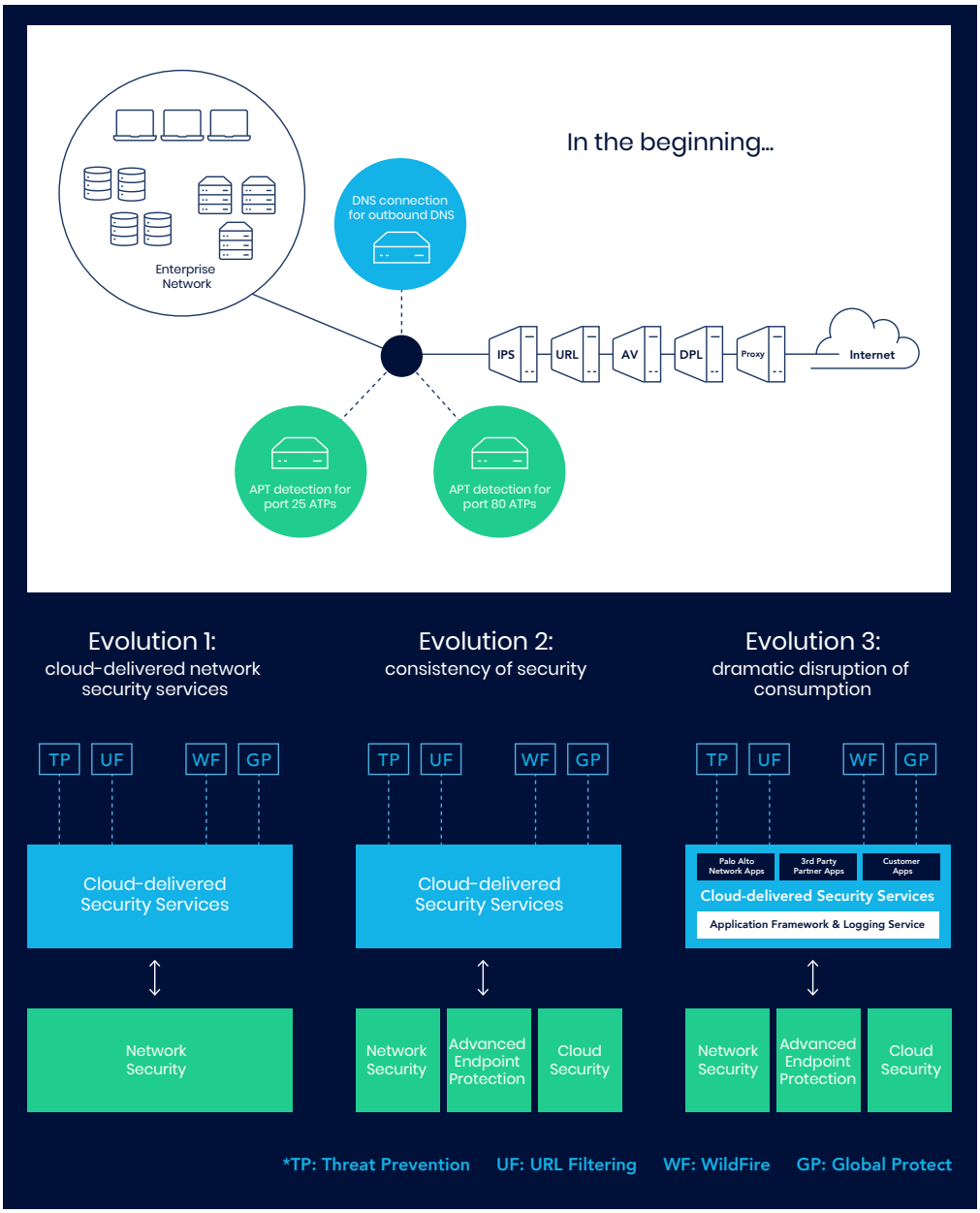


The Evolution of Cybersecurity: New Perspectives

How has cybersecurity changed over the years? How do innovative new companies compete against well established giants in this rapidly evolving environment?

Over the past decade, consumers and enterprises have fundamentally changed the way they access applications and data. The ubiquity of laptops, smartphones, and other connected devices has created a number of ways for cybercriminals to gain access to private data and systems. As a result, the entire cyber battlefield has grown in both complexity and scope. While major companies have considered cybersecurity a top priority since the 1980s, individual users and smaller enterprises across the private sector have only now started to recognize its importance. Governments are also growing increasingly worried about cyberwarfare and digital threats to key physical infrastructure such as power plants and transportation systems.

Exhibit 2: The Three Evolutions of Cybersecurity [2]



Thus, the traditional cybersecurity solutions of the past, such as signature-based antivirus programs, have grown increasingly ineffective. Companies who dominated the cybersecurity for nearly 20 years now face nimble, venture backed competitors developing cybersecurity solutions which utilize cutting-edge technologies like artificial intelligence, machine learning and behavioral detection. The time is ripe for technological and strategic innovation in cybersecurity. For example, Exhibit 2 below from PANW's (Palo Alto Networks) recent investor presentation, explains the company's perspective on the evolution of cybersecurity.

As shown, PANW outlines three steps in the evolution of cybersecurity: the adoption of cloud-delivered network security services, security consistency, and the disruption of consumption. Each of these three steps brought new complexity to cybersecurity but also provided additional benefits such as enhanced protection, improved convenience of use, and reduction in remote accessibility.

> "We are on the third evolution of cybersecurity applications, and each one starts with securing your data"
>
> Mark McLaughlin, CEO, Palo Alto Networks
> (CNBC, Feb 27th 2018)

Similarly, in Carbon Black's recent IPO filing, the company visualized the evolution of cybersecurity in terms of the changing security perimeter as shown in Exhibit 3. In the past, companies guarded the overall enterprise network. Today, the abundance of endpoints makes such a defense strategy ineffective. Instead, Carbon Black places the new security perimeter at the endpoints themselves. This approach, which addresses PANW's third evolution, highlights that such issues are common concerns among innovative cybersecurity companies.

Exhibit 3: The Evolving Security Perimeter [3]

BEFORE

The **Network** was the Perimeter

TODAY

The **Endpoint** is the new Perimeter

Finally, a recent investor presentation from Zscaler, who also recently went public, describes an industry shift from the "hub and spoke" network architecture hosted on centralized, on-premise data centers to direct-to-cloud architectures located in the public cloud or onsite in the local cloud. The decline of traditional network security described in Exhibit 4 below corresponds roughly with PANW's first evolution, reaffirming the importance of such trends to cybersecurity innovators.

Exhibit 4: The Decline of Network Security [4]

	OLD WORLD		NEW WORLD
Application Location	On-premises data center	→	Public cloud, SaaS, on-premises data center
Network Architecture	Hub-and-spoke: backhaul traffic to the on-premises data center	→	Direct-to-cloud traffic routed locally to the internet
Security Approach	"Castle and Moat" to secure the corporate network	→	Securely connect users and devices regardless of network

In order to better navigate an increasingly complex cybersecurity industry, we charted the capabilities of a variety of players (including public, pure play cybersecurity companies, VC-backed cybersecurity companies, PE-backed cybersecurity companies, and major dedicated cyber-divisions) in 18 cybersecurity specializations. The results, as shown in Exhibit 5 below, show that most well-rounded players are dedicated divisions at major tech companies like Cisco, IBM, and Microsoft, while the most focused players are VC-backed companies such as CloudFlare, Duo Security, and Crowdstrike. Overall, It is clear that major players are racing to attain comprehensive competency in emerging specializations. For further analysis on the implications of these capabilities for M&A and IPO opportunities as well as individual company profiles, stay tuned for our forthcoming report **"Hacking Secure Growth: Investment Opportunities In Cybersecurity".**

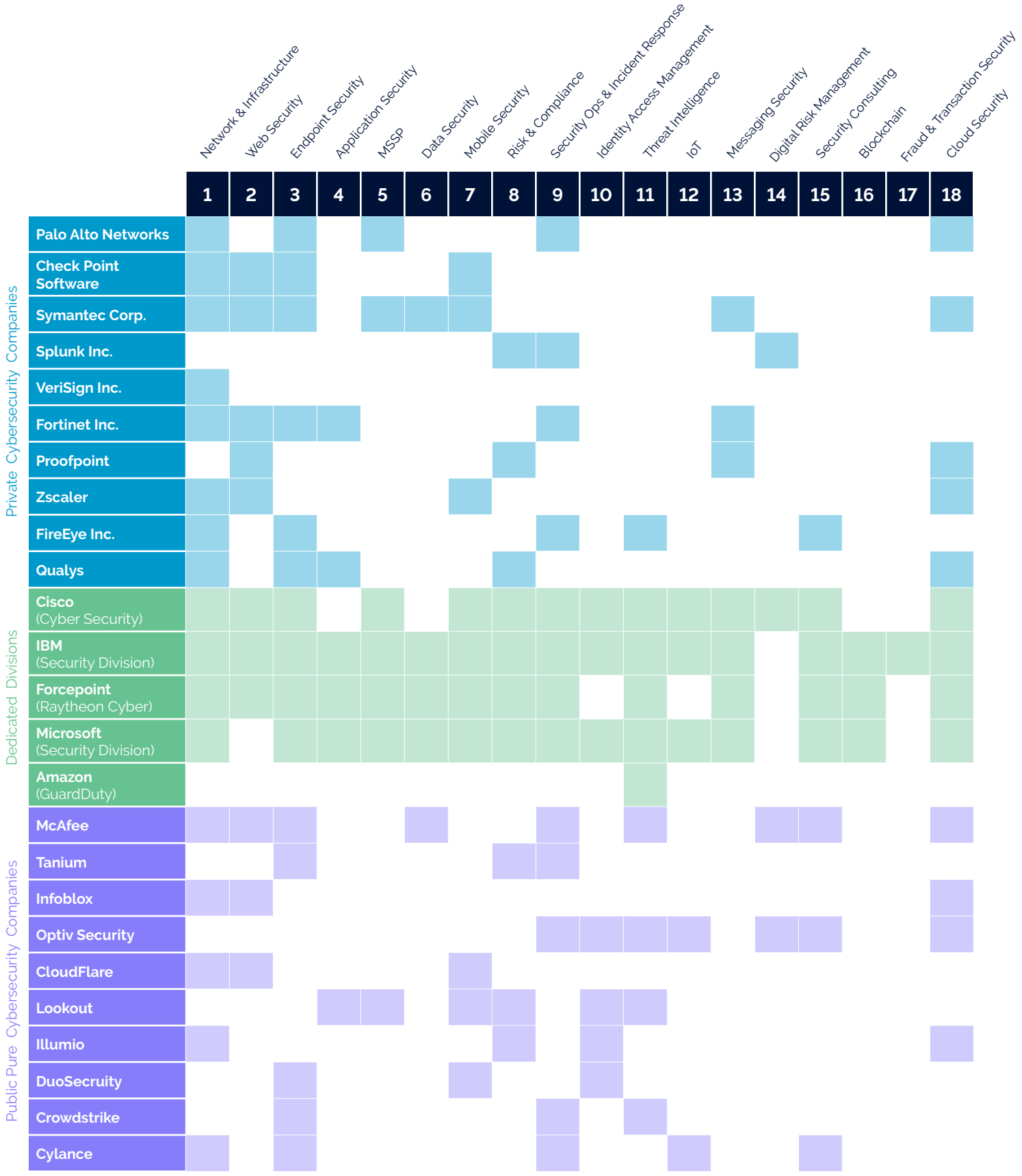


Exhibit 5: Cybersecurity Capabilities Industry Map [5]

Trends in Hacking Activity & Data Breaches

How are cyber threats today different from those of years past? How can we quantify trends in "hacks" and data breaches? What impact do cybersecurity breaches have on companies and consumers today?

Hacks and other major data breaches have been on the rise in recent years. The Yahoo hack in 2016 alone impacted a record three billion user accounts, or about one account for every three people on Earth. Last year, notorious spam sender River City Media accidentally leaked databases containing more than a billion consumer records. Exhibit 6 below lists the most prolific hacks and data breaches since 2012 (events affecting over 100 million records). Notably, the list doesn't even include previously mentioned security flaws, Meltdown and Spectre, which affect nearly every computer today, as they are not themselves hacks or data breaches.

Exhibit 6: Hacks and Data Breaches Affecting Over 100 Million Records [6]

Date Made Public	Company	Location	Total Records
14-Dec-16	Yahoo	Sunnyvale, California	**3,000,000,000**
8-Mar-17	River City Media	Portland, Oregon	**1,370,000,000**
5-Aug-14	Unknown (email/ passwords)	Unknown, Wisconsin	**1,000,000,000**
22-Sep-16	Yahoo	Sunnyvale, California	**500,000,000**
16-Nov-16	FriendFinder	Sunnyvale, California	**412,000,000**
31-May-16	MySpace	Santa Monica, California	**360,000,000**
19-Jun-17	Deep Root Analytics	Arlington, Virginia	**198,000,000**
6-Jun-12	LinkedIn.com	Mountain View, California	**167,000,000**
30-Mar-18	Under Armour	California	**150,000,000**
7-Sep-17	Equifax Corporation	Atlanta, Georgia	**145,500,000**
21-May-14	Ebay	San Jose, California	**145,000,000**
17-May-16	LinkedIn	Mountain View, California	**117,000,000**

While the scale of the incidents above is unprecedented, it is far from surprising. In fact, these incidents are merely the continuation of an almost 40-year-long upward trend in the scale and maliciousness of cyberattacks. To understand how we got to where we are today, it is important to understand the brief history of cybersecurity so far.

From 1980 to 1983, teams of hackers such as the 414s began infiltrating major institutions like National Computer Software Systems and Los Alamos National Laboratory for the first time. Though rarely malicious, these attacks drew public attention to the risks posed by unsecure computer systems.

The next evolution came in the late 1990s, when malware such as the Code Red Worm infected tens of thousands of PCs. The motive

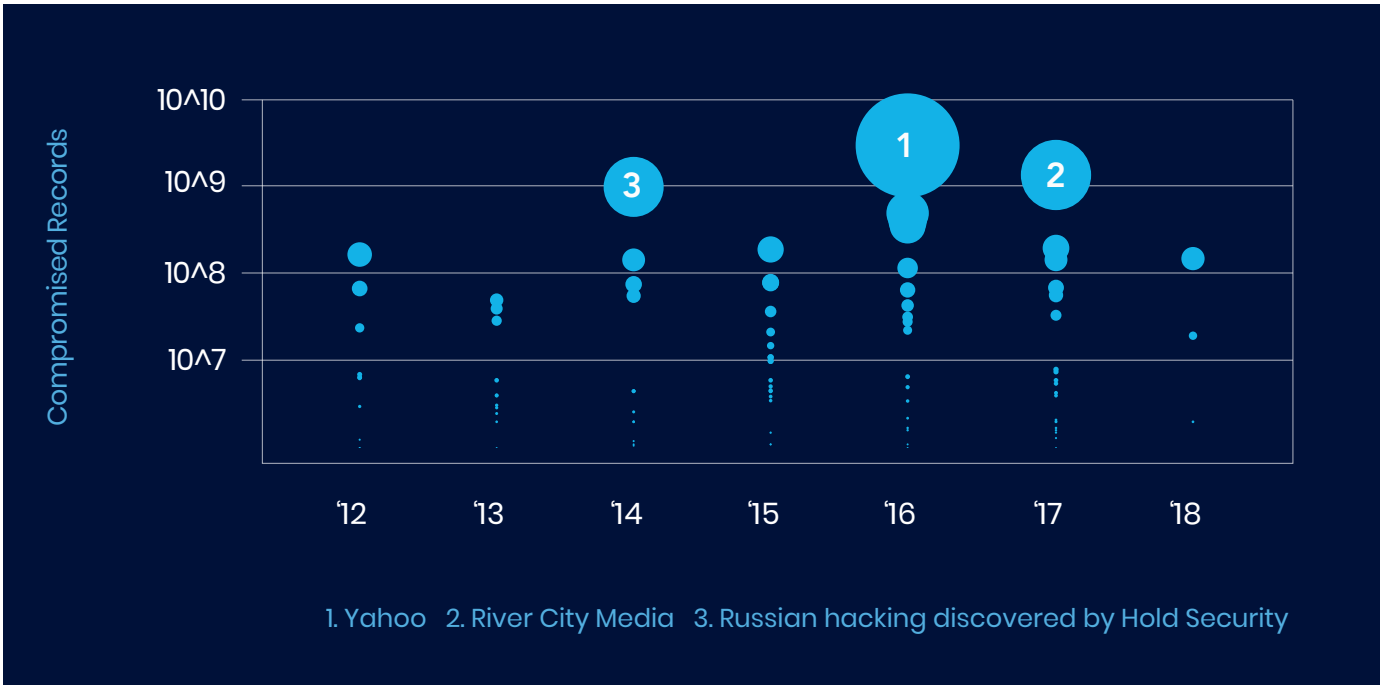
> "My primary goal of hacking was the intellectual curiosity, the seduction of adventure"
>
> Kevin Mitnick, FBI's most wanted hacker in the mid-1990s

behind such breaches, however, was not financial gain. Rather, the malware inflicted seemingly random damage to vulnerable computer systems - leading to the first mainstream adoption of software security systems.

As Internet usage exploded in the early 2000s, simple exploitation techniques such as phishing schemes became the go-to methods to target uninformed consumers. In the mid-to-late 2000s, there were two more major developments in cybersecurity. First, the mass adoption of smartphones, beginning with the iPhone in 2007, offered hackers an entirely new, nearly ubiquitous platform for cyber exploitation. Second, cyberattacks on state institutions and infrastructure around the world became more common. The Struxnet virus in particular, which was allegedly jointly developed by the United States and Israeli governments, made headlines in 2010 when it was discovered to have compromised Iranian nuclear facilities.

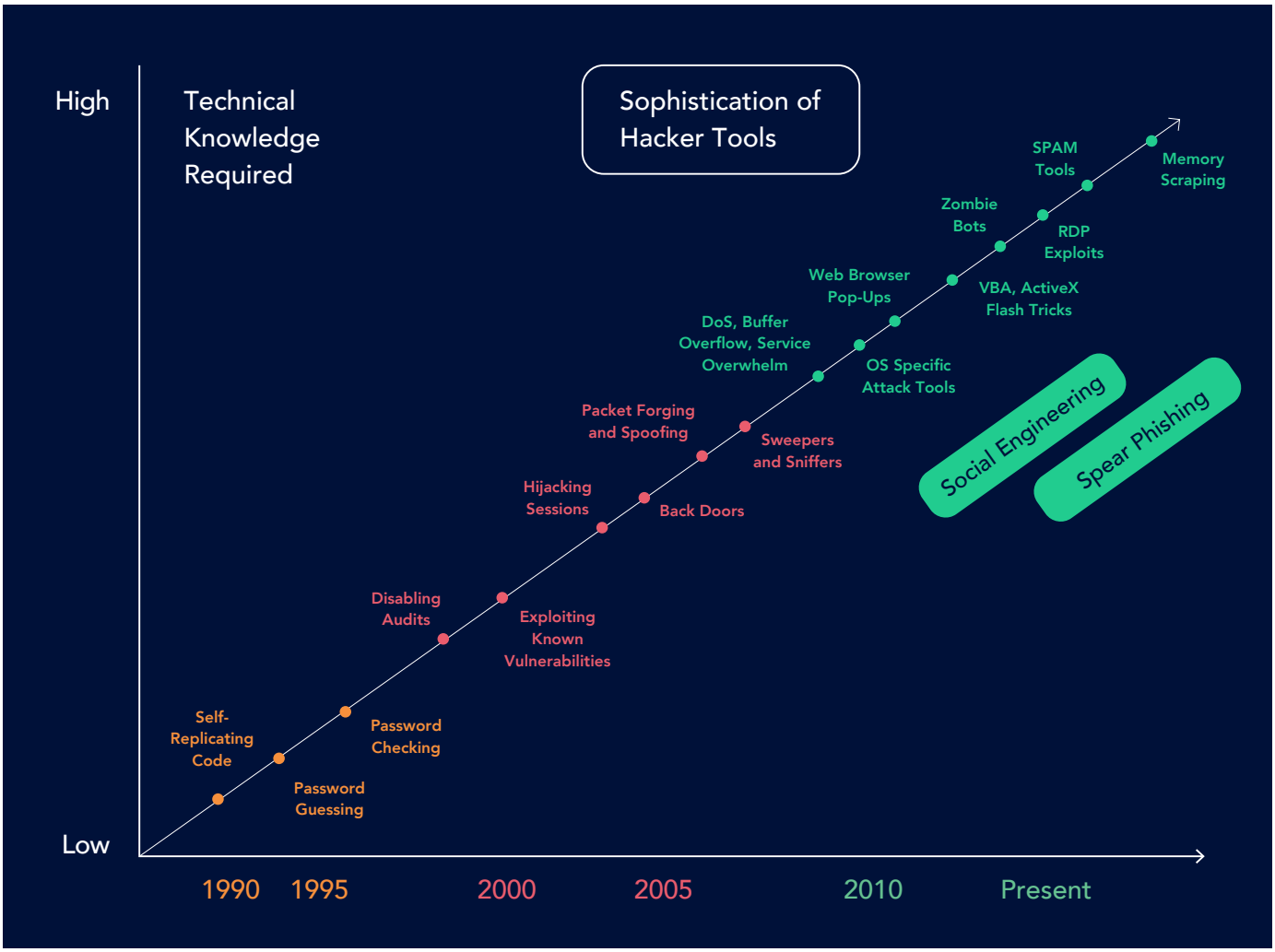
In the eight years since, the scale of cyberattacks has continued to increased. Long gone are the days when the key motivations for hacking were disruption, notoriety and the thrill of adventure. Today, individual bad actors, cybercrime syndicates, and even nation-states all commit cybercrimes for financial or political gain. Exhibit 7 below shows data for all known hacks and data breaches which affected more than one million sensitive records since 2012.

Exhibit 7: Five Years of Hacks and Data Breaches [7]



Major hacks and data breaches such as these, along with more recent ransomware attacks such as WannaCry and NotPetya are not only larger scale and more complex than previous attacks, they are a sign of the times. As shown in Exhibit 8, the sophistication and technical knowledge displayed in modern hacks has steadily increased since the 1990s as the internet and digital devices have steadily become a more integral component of our commercial and personal lives. Additionally, it is important to realize that the range of potential targets has also grown dramatically. With the digitization of company assets, intellectual property, customer records, financial statements, and more are now are now all at risk.

Exhibit 8: The Increasing Sophistication of Hacking Since 1990 [8]



We might thus understandably think only criminals or terrorists commit hacks. However, large companies now employ their own teams of hackers, such as Alphabet's Project Zero, to stress-test new systems and detect security flaws. These ethical hackers are sometimes referred to as "white hats" in contrast to "black hats," or malicious hackers. Similarly, most major governments now maintain sophisticated cyberwarfare operations that utilize hackers in the interest of national security.

Current Technical Trends in Cybersecurity

What current technical trends are likely to shape the future of cybersecurity in the immediate future and beyond? What are the underlying secular trends that continue to drive innovation in the industry?

There are several technical and commercial factors driving the evolution of the cybersecurity industry. In Exhibit 9 below, we summarize the most important technical trends in cybersecurity along with corresponding driving factors and examples of use cases for each.

Exhibit 9: The Most Influential Technical Trends in Cybersecurity and Their Drivers [9]

Technical Development	Adoption Drivers	Implementation
Cloud & Hybrid Security Solutions	Corporations increasingly host cloud applications and operate across hybrid-cloud infrastructures, introducing sensitive data to new security risks.	Cloud and hybrid security solutions serve many of the same purposes as traditional IT security, but in a more scalable, efficient way.
Analytics with Big Data	Security software often generates massive amounts of data, which is not easily understood or utilized.	Advanced data analytics can be used to draw conclusions and make predictions from security data.
ML (Machine Learning)-based Threat Detection	The malware landscape is constantly evolving and signature based approaches to threat detection are easily thwarted by determined hackers.	ML-based threat detection software can scan networks for new threats or suspicious behavior without the need for specific malware signatures.
(AI) Artificial Intelligence Managed Security Automation	Cybersecurity can be unmanageable and expensive, especially for small and medium sized business with limited IT budgets. Thus, cybersecurity is often poorly managed.	So-called AI technology can enable MSSPs (Managed Security Service Providers) to provide more affordable cybersecurity services.
Insider Threat Detection and Prevention	Insider threats pose significant risks to organizations. Inappropriate handling of data or applications, whether malicious or accidental, can lead to catastrophic incidents.	Data access protocols and automated access requisitioning can mitigate the risks posed by insiders.
Phishing Detection and Recovery	Many cyber attacks are linked to compromised login credentials for proprietary systems. Phishing remains the key means by which end users are exploited.	Phishing simulations and machine learning-based email filtering now complement traditional methods to combat phishing campaigns.
Firmware and Hardware Defense Software	Attackers exploit insecure supply chains to infect firmware and hardware that allows for siphoning data and destroying machines.	Specialized software can now be used to defend systems against firmware, hardware, and supply chain attacks.
Blockchain-based Security Protocols	Centralized networks lack transparency, and are especially vulnerable to hacking, since sensitive data is stored and processed in a single location.	Blockchain-based security protocols offer a transparent decentralized alternative for data processing and storage.
Edge Computing	The increasing amount of data transmitted by IoT and IIoT devices is vulnerable to attacks during transmission and at the centralized data storage location in the cloud.	Edge computing leverages IoT & IIoT devices for localized decision making to reduce required data transmission and limit centralized data storage.
IoT and IIoT Security Software	As the number of IoT devices grows, so does the number of vulnerable endpoints which can be exploited to gain access to private networks.	Specialized tools are used to help identify and authenticate autonomous machines for ensuring data protection, availability, and privacy.
Automotive Cybersecurity	Automobiles are becoming increasingly connected and autonomous and thus increasingly vulnerable to cyber attacks.	Automotive-specific security software to protect connected cars from cyber threats is developing currently.

While all of the trends above will likely play an important role in the evolution of cybersecurity, the three developments we see as likely to have the most widespread impact in the near-term are cloud and hybrid security solutions, advanced data analytics, and ML-based threat detection. Alternatively, we consider the last five entries to be longer-term bets on the future of cybersecurity. We offer a closer look at the more immediate trends below.

Cloud and Hybrid Security Solutions

The increasing prevalence of hybrid infrastructures and cloud-based applications for business and homes is a major secular trend driving the evolution of cybersecurity. On the one hand, this shift has created new security challenges, as cloud-based systems inherently link to potentially unsecure outside networks. Furthermore, cloud-based applications in business often introduce a host of potentially vulnerable access points to previously well-defended networks, and allow unwitting employees to easily distribute critical data in non-secure ways. However, ambitious companies like Zscaler have leveraged these technological advances to create complete, cloud-based, enterprise-level, cybersecurity solutions. These products replace complicated on-site security hardware and software with a centrally managed, continuously updated security platform. Ideally, cloud cybersecurity technology offers more efficiency and scalability than traditional IT security solutions.

Advanced Analytics with Big Data

Advanced analytics allows companies to leverage previously untapped resources. Previously, security systems often generated disorganized, cumbersome, data , which failed to offer meaningful insights about potential dangers, and even exigent cyber threats were sometimes overlooked. However, data analytics companies such as Splunk, who recently acquired cybersecurity startup Phantom Cyber for $350 million, are applying big data analytics and machine learning to cybersecurity. Companies can use this technology to predict, detect, and triage cybersecurity breaches and effectively respond to threats more efficiently than traditional methods.

Machine learning-based threat detection

Signature-based threat detection systems have been integral to cybersecurity since the first anti-virus software systems. Such systems identify infections by scanning for malware based on the digital signature of previous malware samples. Though easy to implement, these systems can only flag known malware, and can't identify new variants without first obtaining new signatures. Analyzing malware samples to produce usable signatures is also time consuming. Modern malware is fast acting and rapidly evolving, which makes it hard to obtain the right signatures before the malware has already damaged critical systems. By the time the system has analyzed a given file, the malware has likely changed its signature.

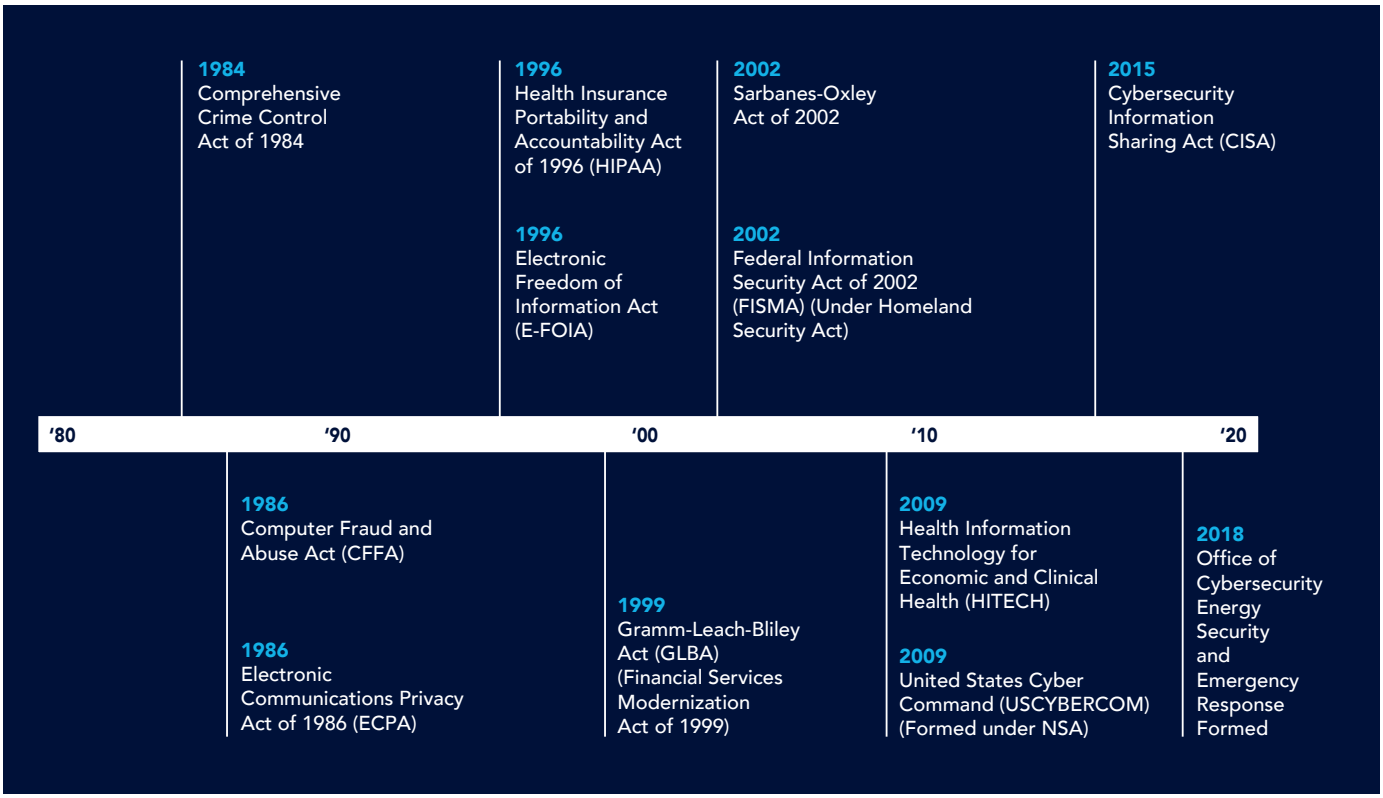
Behavior-based malware detection, by contrast, identifies potentially malicious files by their behaviors or attempted behaviors. Using dynamic sets of real files, the technology trains systems (usually based on layers of deep neural networks) to recognize potentially threatening patterns of behavior or files. While still relatively new, ML promises to help enterprises identify malware infections as they occur and even preempt them altogether. Furthermore, ML techniques have the added benefit that, aside from optimization and training procedures, security designers don't necessarily need to provide ML systems with explicit instructions to detect and combat malware.

Regulatory Trends and Concerns in Cybersecurity

What role does government play in the cybersecurity industry, and what areas are most likely to see increased regulation in the future? What are the driving forces behind the increasing regulatory scrutiny of cybersecurity practices?

As digital technology and information networks increasingly form the underpinnings of our economy and society, cybersecurity vulnerabilities multiply not only in number but also in potential impact. Today, cybersecurity is an issue not just for private software companies, but for entire countries. Governments around the world are increasingly trying to protect consumers, corporations and national security with new regulations. Exhibit 10 charts out major U.S. cybersecurity legislation and regulatory milestones to date.

Exhibit 10: Key Milestones in Cybersecurity Regulation and Legislation [10]



However, these major legislative milestones are just the tip of the iceberg. In 2017, 42 U.S. states introduced 240 bills and resolutions related to cybersecurity -- more than double the previous year. At least 27 of these states actually passed related legislation. The rising pace of state legislation poses major challenges to U.S. companies, which must also contend with federal laws. At the federal level, recent actions suggest a measure of relaxation of enforcement in areas impacting consumer information privacy and security. At the same time, the federal government has been working to ensure companies secure consumer data from cyber threats. Despite these efforts, successful cyber attacks on government systems and other major organizations still occur with some regularity.

Surprisingly, the most pressing cybersecurity regulation major U.S. companies must contend with today isn't U.S. regulation at all. The European Union's General Data Protection Regulation (GDPR) applies to all organizations who manage data from people "in the EU", including citizens, residents, and even tourists.

General Data Protection Regulation

The EU adopted GDPR on April 27, 2016, and the law went into full effect on May 25 this year. GDPR's is intended to ensure companies and organizations responsibly manage personal consumer data, streamline the handling of personal data within the bloc, and give EU citizens more control of their data. GDPR's impact is global because it applies to all organizations, that collect data from EU citizens regardless of origin. The regulation protects not only personal information like account numbers and patient data but broadens the definition of "personal data" to include identifiers associated with the economy, culture, society, genetics, psychology, and digital fingerprints like IP addresses and cookies. The law also requires companies to report data breaches to affected consumers within 72 hours. As a result, companies around the world have been scrambling to update their cybersecurity policies and infrastructure to comply with GDPR standards.

We cannot overstate the effects of GDPR. Major corporations including Facebook and Google already face lawsuits for alleged non-compliance, and cybersecurity firms have already developed dedicated offerings around automated GDPR compliance. Since GDPR fines and penalties could be potentially devastating to smaller companies, we expect such solutions will gain popularity over the near-term.

While GDPR is certainly the elephant in the room, there are also several other areas we are monitoring closely in terms of potential domestic regulations.

Healthcare IT Security

Regulators are especially interested in healthcare because providers regularly digitize, store and transmit some of consumers' most sensitive data. While existing laws like HIPAA and HITECH address cybersecurity in some fashion, the emergence of wearable IoT devices and connected medical devices raises new questions about protecting consumer data. For example, smart watches and smartphones commonly store and transmit consumer's fitness data and vital signs, including body temperature and heart rates. Similarly, the medical diagnostic tools and even surgical tools of the future are expected to become increasingly connected. It would thus be unsurprising to see increased regulation regarding the handling of certain kinds of user medical/health data.

Financial IT Security and Fraud Detection

In some ways, financial IT security and fraud detection resemble healthcare security. Breaches of sensitive financial data, which consumers increasingly store on unsecure connected devices, could potentially yield similarly catastrophic results. Furthermore, consumers increasingly conduct transactions on mobile devices, often using different payment methods or currencies. Such a shaky foundation invites further legislation to regulate digital transactions, electronic identify verification, and financial privacy.

Whether external or internal, fraud remains a key source of risk for large organizations. While laws like the Sarbanes-Oxley Act address fraud and allow some protections for whistle blowers, further bills such as the Cybersecurity System and Risks Reporting Act have been introduced that would amend the act to specifically include more cybersecurity systems provisions.

Risk Management and Cybersecurity Insurance

Cybersecurity insurance offers organizations a way to mitigate this risks presented by cybersecurity threats, which can impact profits just as severely as lawsuits or natural disasters. Cyber-insurance could become relevant from a regulatory perspective in several ways. For example, regulators could one day require banks and other critical institutions to buy cybersecurity policies to ensure risk mitigation. Alternatively, cyber-insurance could become a required component of automotive insurance plans, home-owner's insurance, or even health insurance plans, depending on future developments in autonomous vehicles and IoT technology. Admittedly, these possibilities are speculative and unlikely in the near-term, but as the cybersecurity landscape continues to evolve, cybersecurity insurance will as well.

Net Neutrality

Net neutrality regulation is a hotly debated topic among corporations, academics, and consumers. The Federal Communications Commission partially repealed net neutrality regulations at the end of 2017, but certain provisions remain. Individual states such as California now want to implement their own regulations. Ultimately, the debate largely hinges on whether regulators should classify internet services as information services or telecommunications services. This is crucial because the U.S. government requires telecommunications providers to transmit data as is and without bias toward content. Opponents of net neutrality argue that repealing these regulations will encourage competition and innovation. Supporters warn eliminating net neutrality could allow service providers to unfairly "throttle" internet traffic to competitors' websites or arbitrarily restrict access to certain content.

The end of net neutrality has many implications for cybersecurity. ISPs could transmit information how they see fit and with minimal transparency. They could collect, mine, or even alter data with minimal accountability. Without net neutrality, ISPs could also eliminate encryption by default, exposing those unwilling or unable to pay to new security risks. Some have suggested ISPs could even decrypt encrypted data at will.

Encryption Backdoors

U.S. government agencies have demonstrated full willingness to use backdoors to access encrypted devices for the purpose of law enforcement and have even obtained court orders demanding companies create such backdoors. Companies like Apple have repeatedly publicly refused such requests, arguing that such backdoors would pose significant risks to customers. In the most high-profile incident to-date, Apple was ordered to grant the FBI entrance to the iPhone of one of the San Bernadino shooters, but the request and the case were withdrawn before any higher court ruling on the matter. Thus, the question remains open as to the extent to which the courts can compel companies to comply with such requests, and it wouldn't be surprising if similar situations in the future brought the matter to a head once and for all.

Understanding the $100 Billion Dollar Cybersecurity Market

Can we accurately estimate the overall market potential for cybersecurity companies? What do current cybersecurity spending trends tell us about areas of opportunity in the future?

The IT security industry has historically been a mature and consolidated market with products like antivirus software, firewalls, and e-mail filters boasting adoption rates close to 100 percent. But the changing threat landscape and the migration of the security perimeter have created new opportunities. As the cybersecurity market develops, we expect significant growth, from both new entrants and legacy players looking to expand and diversify their business models.

Theoretically, the upper limit on cybersecurity spend is just less than the cost of the cybercrime which it can prevent. Thus, rather than considering all crime that occurs via the internet or connected devices, we are only concerned with crime that involves criminals gaining illicit access to a victim's computer or network. Though all estimates for the annual cost of cybercrime involve significant assumptions, we believe that the maximum possible cybersecurity spend is within the range of error for the total cost estimates for such crime as shown in Exhibit 11 below. Thus, we estimate that the upper limit for potential cybersecurity spend is between $495 and $650 billion a year.

Exhibit 11: The Annual Cost of Cyber Crime (Billions of Current Dollars) [11]

When compared with worldwide cybersecurity spend as shown in Exhibit 11, we can see that the cybersecurity market is far from saturated, even without significant growth in cybercrime. Total spend in 2018 is projected to be less than one fifth of the overall cost of cybercrime.

Exhibit 12: Worldwide Security Spending by Segment, 2016-2018 (Millions of Current Dollars) [12]

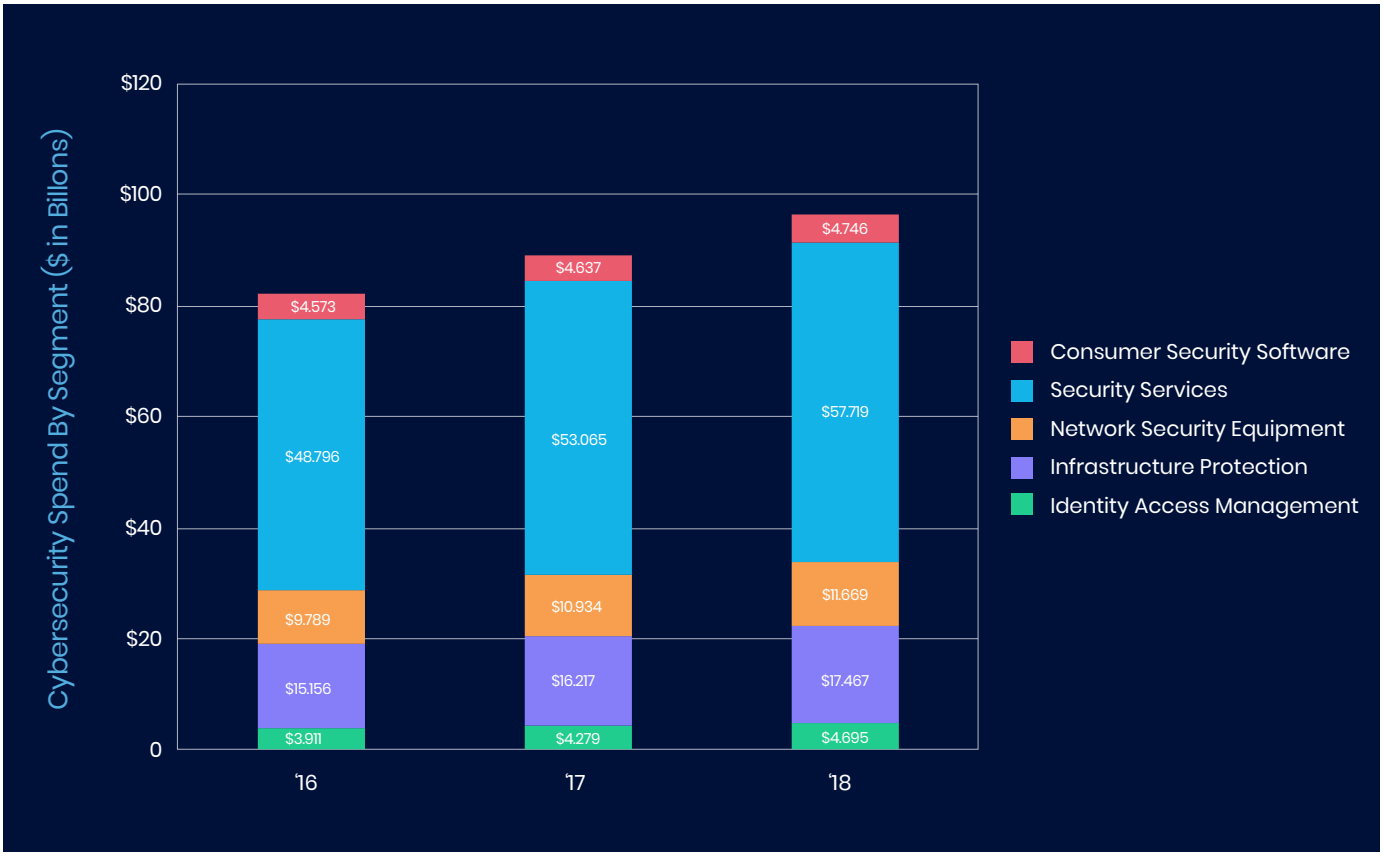


Exhibit 12 shows the breakdown of cybersecurity spend by category. Security services, which include consulting and outsourced management, represents the majority of current cybersecurity expenditures, followed distantly by infrastructure protection and network security equipment. The broad range of companies offering "security services" fill specific niches and cater to a variety of clients. Other categories such as consumer security software and identity access management are fairly narrow by comparison. Interestingly though, no one category significantly outperformed the others in terms of YoY growth. The only underperformer was consumer security software, which is unsurprising, as traditional anti-virus packages have become ever more obsolete. Overall, we believe growth in the cybersecurity market is likely to continue to outpace growth in overall IT spend. If these trends continue, we could see the overall market opportunity grow to $165 billion in 2023 from $95 billion today, a roughly 10 percent CAGR—well ahead of the mid-single-digit growth in overall IT spend.

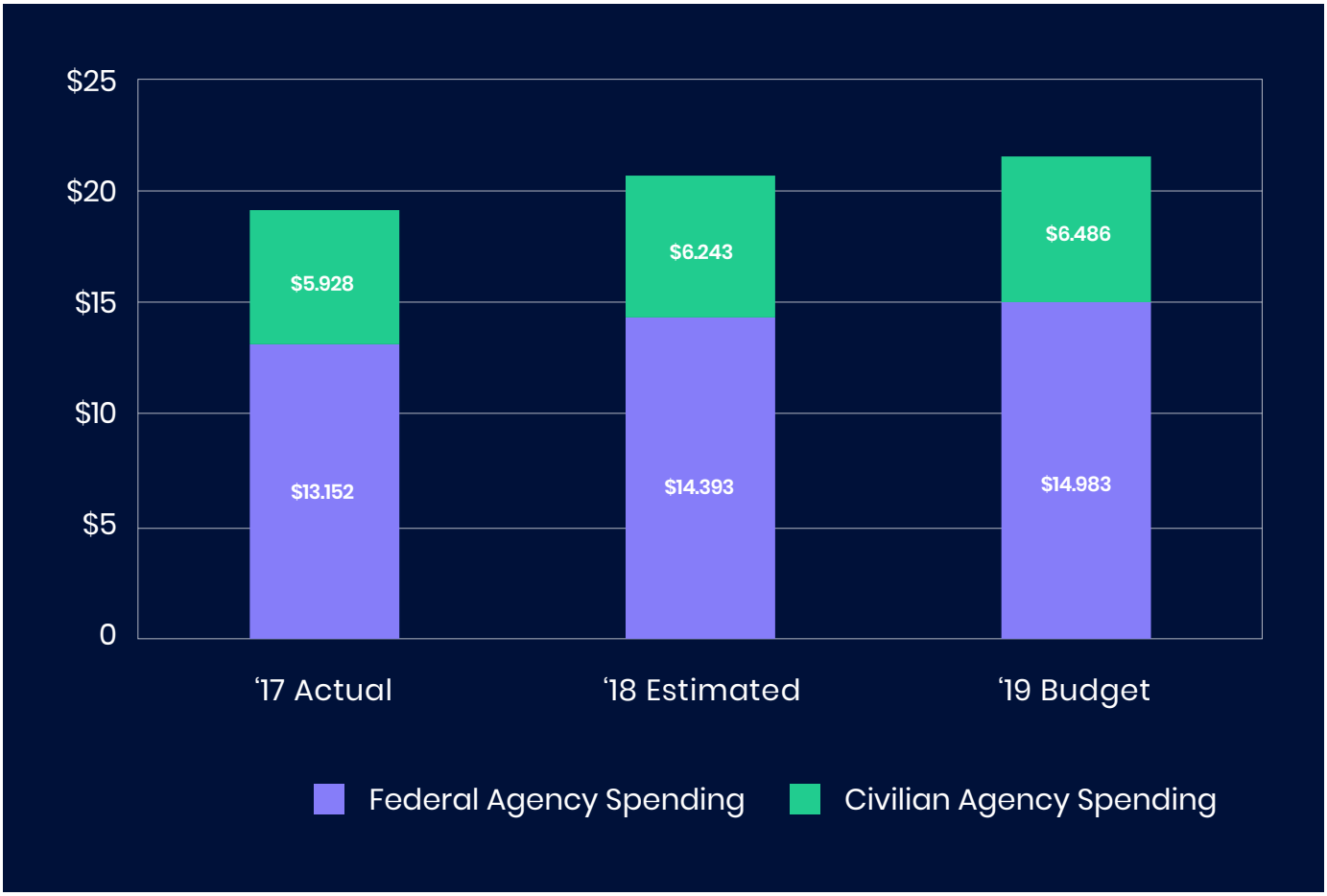
One final piece of the puzzle with the potential to drastically alter worldwide cybersecurity spending in the coming years is the role of government spending. Governments around the world are focused on strengthening cybersecurity defenses—bolstering internal security architectures, deterring malicious activities, and enhancing protection of the private sector through regulations. The ever-present threat of cyberwarfare between nations could generate outsized growth in specific market segments such as critical infrastructure defense software, given the magnitude of economic and social impact at stake.

"A cyber attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack on 9/11"

Leon E. Panetta, U.S. Secretary of Defense at the Business Executives for National Security meeting (October 11th, 2012)

Given the difficulty of tracing cybercrime and espionage to specific agencies or governments, the potential rewards of state-sponsored cyber attacks outweigh the risks. Thus, we are likely to continue to see growth in state-sponsored cyber attacks, further driving growth in related segments. The U.S. government, in particular, has identified cybersecurity as "one of the most serious economic and national security challenges we face as a nation.", and the Trump administration called for a 33% increase in cybersecurity spending in the federal budget. To better understand the impact of government dollars on cybersecurity, we examined actual historical spending, current spending estimates, and the 2019 cybersecurity budget for civilian and federal agencies. While the growth rates observed are far less than those for the overall industry, political and strategic developments could still drive additional growth beyond current estimates and budgets.

Exhibit 13: U.S. Government Spend on Cybersecurity ($ in Billions) [13]



PLEASE READ THESE IMPORTANT LEGAL NOTICES AND DISCLOSURES

CONFLICTS: This report is being published by SharesPost Research LLC, and distributed by SharesPost Financial Corporation, a member of FINRA/SIPC. SharesPost Research LLC, SharesPost Financial Corporation and SP Investments Management, LLC, an investment adviser registered with the Securities and Exchange Commission, are wholly owned subsidiaries of SharesPost, Inc. SP Investments Management is the investment manager of the SharesPost 100 Fund, a registered investment company, and other funds.

Recipients who are not market professionals or clients of SharesPost Financial Corporation should seek the advice of their own personal financial advisors before making any investment decisions based on this report. None of the information contained in this report represents an offer to buy or sell, or a solicitation of an offer to buy or sell, any security, and no buy or sell recommendation should be implied, nor shall there be any sale of these securities in any state or governmental jurisdiction in which said offer, solicitation, or sale would be unlawful under the securities laws of any such jurisdiction. This report does not constitute an offer to provide investment advice or service. Registered representatives of SharesPost Financial Corporation do not (1) advise any member on the merits or advisability of a particular investment or transaction, or (2) assist in the determination of fair value of any security or investment, or (3) provide legal, tax, or transactional advisory services.

Information regarding companies in the SharesPost 100 List available on the website has been collected from or generated from publicly available sources. The availability of company information does not indicate that such company has endorsed, supports, or otherwise participates with SharesPost. Company "thesis" is the opinion of SharesPost and is not a recommendation to buy, sell, or hold any security of such company.

Investors should be aware that the SharesPost 100 Fund (the "Fund") may or may not have an ownership interest in any of the issuers that are discussed in the report at any given point in time. Accordingly, investors should not rely on the content of this report when deciding whether to buy, hold, or sell interests in the Fund. Instead, investors are encouraged to do their own independent research. Before investing in the Fund, investors are cautioned to consider the investment objectives, risks, charges, and expenses carefully before investing. For a prospectus with this and other information about the Fund, please visit www.sharespost100fund.com. Read the prospectus carefully before investing.

ANALYST CERTIFICATION: The analyst(s) certifies that the views expressed in this report accurately reflect the personal views of such analyst(s) about any and all of the subject securities or issuers, and that no part of such analyst compensation was, is, or will be, directly or indirectly related to the specific views contained in this report.

Analyst compensation is based upon various factors, including the overall performance of SharesPost, Inc. and its subsidiaries, and the performance and productivity of such analyst, including feedback from clients of SharesPost Financial Corporation and other stakeholders in our ecosystem, the quality of such analyst's research and the analyst's contribution to the growth and development of our overall research effort. Analyst compensation is derived from all revenue sources of SharesPost, Inc., including brokerage sales.

DISCLAIMER: This report does not contain a complete analysis of every material fact regarding any issuer, industry, or security. The opinions expressed in this report reflect our judgment at this date and are subject to change. The information contained in this report has been obtained from sources we consider to be reliable; however, we cannot guarantee the accuracy of all such information.

Any securities offered are offered by SharesPost Financial Corporation, member FINRA/SIPC. SharesPost Financial Corporation and SP Investments Management are wholly owned subsidiaries of SharesPost, Inc. Certain affiliates of these entities may act as principals in such transactions.

(continued on next page)

Investing in private company securities is not suitable for all investors. An investment in private company securities is highly speculative and involves a high degree of risk. It should only be considered as a long-term investment. You must be prepared to withstand a total loss of your investment. Private company securities are also highly illiquid and there is no guarantee that a market will develop for such securities. Each investment also carries its own specific risks and you should complete your own independent due diligence regarding the investment, including obtaining additional information about the company, opinions, financial projections and legal or other investment advice.

Accordingly, investing in private company securities is appropriate only for those investors who can tolerate a high degree of risk and do not require a liquid investment.

Exhibit Sources by Number

[1] SharesPost Research

[2] SharesPost Research: Reconstructed from Palo Alto Networks' Analyst Day Investor Presentation (September 17th, 2017)

[3] SharesPost Research: SEC, Carbon Black S-1 IPO Registration Statement, May 2nd, 2018, [Accessed May 2nd, 2018]

[4] Reconstructed by SharesPost Research: Zscaler, "Securing Your IT Transformations to The Cloud, Corporate Presentation", June 2018, [Online]. Available: https://ir.zscaler.com/static-files/f2f4c074-8bce-4b71-b7a6-16d904c4d778 [Accessed, June 1st, 2018]

[5] SharesPost Research's analysis of various companies and product offerings. Note: company coverage is not intended to be comprehensive or include every major cybersecurity company.

[6] The Privacy Rights Clearing House, "Data Breaches" [Online]. Available: https://www.privacyrights.org/data-breaches?title [Accessed April 6th, 2018]

[7] SharesPost Research using data from The Privacy Rights Clearing House, "Data Breaches", [Online]. Available: https://www.privacyrights.org/data-breaches?title [Accessed April 6th, 2018]

[8] SharesPost Research

[9] SharesPost Research

[10] United States Congress, "Legislation", [Online]. Available: https://www.congress.gov [Accessed May 15th, 2018]

[11] Data Interpolation by SharesPost Research, data from: Lewis, James, "Economic Impact of CyberSecurity, No Slowing Down", Center For Strategic and International Studies, February 2018, [Online]. Available: https://www.csis.org/analysis/economic-impact-cybercrime [Accessed May 15th, 2018]. Note: Estimates for the global cost of cybercrime are based off of extrapolations from data for countries with reliable cybercrime reporting statistics in 2014 and 2018

[12] Chart created by SharesPost Research based on Gartner research. Source: Gartner, Inc., "Forecast: Information Security, Worldwide, 2015-2021, 3Q17 Update.", 2017, [Online]. [Accessed Jun., 2018].

Gartner (December 2017); All statements in this report attributable to Gartner represent SharesPost's interpretation of data, research opinion or viewpoints published as part of a syndicated subscription service by Gartner, Inc., and have not been reviewed by Gartner. Each Gartner publication speaks as of its original publication date (and not as of the date of this report. The opinions expressed in Gartner publications are not representations of fact, and are subject to change without notice.

[13] The White House, "CYBERSECURITY FUNDING", [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_21_cyber_security-fy2019.pdf [Accessed May 15th, 2018]