The Cyber Defense Index: A Primer

Introduction

The world is more connected than ever before, with more than 3.5 billion internet users online as of 2017,[1] and another billion projected to join by 2021.[2] The range of activities we conduct online is also wider than ever before, and now encompasses banking, shopping, gaming, investing, and much more. In addition, the Internet of Things (IoT)—already making minor inroads with consumers via internet-connected devices including air conditioners, refrigerators, and home security systems—is expected to expand significantly in the coming years with the advent of 5G wireless technology.

There is a dark side to our growing interconnectedness, however: individuals and companies are now more vulnerable than ever to hacks, data breaches, and identity theft. Cybercrime is one of the fastest-growing threats to global security, costing as much as $3 trillion in 2015, and projected to grow to $6 trillion by 2021.[3] Cybersecurity is relevant to anyone who uses the Internet: it is estimated that two-thirds of internet users (more than two billion people) have had their information compromised or stolen.[4]

In the face of this looming threat from cybercrime, the cybersecurity industry has grown to occupy an increasingly critical role in the world economy. The Prime Cyber Defense Index allows investors to track the growing cybersecurity industry that has developed to safeguard governments, companies, and individuals from cyberattacks.

Cybercrime: A Growing Threat

Cybercrime has been a problem since the dawn of the Internet, but it has taken on frightening new proportions in the 21st century with record-breaking hacks and data breaches, vicious ransomware attacks, and the emergence of Cybercrime as a Service (CaaS), wherein cybercriminals sell access to hacking tools to non-experts, significantly broadening their reach and impact.[5] The pace of cyberattacks is only increasing: a recent study estimated anywhere from 300,000 to 1 million viruses and other malicious pieces of software are released every day.[6]

Hacks and Data Breaches

In recent years, the scale and impact of cyberattacks has continued to grow. In July of 2017, Equifax, a major U.S. credit bureau, announced that it had been the victim of a hack, potentially exposing the personal information of 143 million consumers (this has since been revised upward, to 147.9 million).[7] Personal data obtained in the breach included social security numbers, birth dates, addresses, and in some cases driver's license numbers and credit card information, leaving customers more vulnerable than ever to identity theft.

As damaging as the Equifax cyberattack was, in sheer numbers it pales in comparison to the 2013-2014 data breach that Yahoo revealed in September 2016, which impacted a staggering 3 billion user accounts, compromising real names, email addresses, dates of birth, and phone numbers.[8]

It appears no industry or computer system is out of reach to determined hackers; as a daring heist recently revealed, not even the banking sector is safe. In 2016, unknown hackers successfully penetrated the ultra-secure SWIFT messaging system, which banks use to communicate with one another to send international wire transfers. The cybercriminals penetrated the computer systems of the Central Bank of Bangladesh, compromised its dedicated SWIFT computer, and initiated a series of fraudulent money transfers on behalf of the Central Bank, making off with $81 million.[9]

Ransomware

The fastest-growing cybercrime, ransomware can prove uniquely damaging to individuals and organizations. Ransomware threatens to delete valuable user information on infected computers if a payment is not sent. In the first quarter of 2016, the FBI reported $209 million in ransom payments, a huge increase over 2015, when just $24 million in ransomware payments were reported through the entire year. This could just be the first salvo in an escalating onslaught of ransomware attacks, as the FBI sees ransomware ballooning into a billion dollar business in the coming years.[10]

Cybercrime as a Service (CaaS)

Perhaps most troubling of all, cybercrime is no longer the sole domain of sophisticated hackers and programmers thanks to Cybercrime as a Service (CaaS).[11] Facilitated by hard-to-trace cryptocurrency and the anonymous Tor network, CaaS enables criminally-inclined amateurs to purchase exploit kits, botnets, ransomware, computer viruses, DDoS attack programs, and much more on the dark web.[12] Some dark web markets offer services one might expect at an ordinary online store such as escrow payments, money-back guarantees, and seller support.

Growth of the Cybersecurity Industry

As cybercrimes have grown in scope, complexity, reach, and cost, the cybersecurity industry has quickly risen to confront the evolving security challenges of the 21st century. The industry has already experienced breathtaking growth: in 2004, global spending on cybersecurity totaled just $3.5 billion.[13] By 2015 the industry had grown to roughly $75 billion, and it is expected to reach $90 to 101 billion by the end of 2018.[14] As impressive as the growth has been, the cybersecurity industry may still be in its infancy. A recent report sees the cybersecurity market reaching $170 billion by 2020,[15] while some experts see the industry doubling in size within the next ten years.[16]

Ramped-Up Spending

Driven in part by headline-grabbing data breaches, as well as the need to protect their sensitive data stored in the cloud, companies worldwide are ramping up their cybersecurity spending. Companies in the financial services, consulting, healthcare, manufacturing, and transportation sectors have ample reason to increase cyber security spending, as these industries are most frequently targeted for cyberattacks.[17]

In a moment of candor, a Bank of America executive recently commented that their cybersecurity division is "the only place in the company that doesn't have a budget constraint." The bank is spending about $600 million on cybersecurity this year alone.[18]

After suffering a high-profile hack in 2017, Deloitte announced that it would be spending $580 million on cybersecurity in the next three years.[19] Previously, Deloitte had spent as little as $50 million per year.

Cost of Cybercrime by Region *Source: McAfee & CSIS, 2018*

Region	Region GDP (USD, trillions)	Cybercrime Cost (USD, billions)	Cybercrime Loss (% GDP)
North America	20.2	140 to 175	0.69 to 0.87%
Europe and Central Asia	20.3	160 to 180	0.79 to 0.89%
East Asia & the Pacific	22.5	120 to 200	0.53 to 0.89%
South Asia	2.9	7 to 15	0.24 to 0.52%
Latin America & the Caribbean	5.3	15 to 30	0.28 to 0.57%
Sub-Saharan Africa	1.5	1 to 3	0.07 to 0.20%
MENA	3.1	2 to 5	0.06 to 0.16%
World	***$75.8***	***$445 to $608***	***0.59 to 0.80%***

Cybersecurity in Our Daily Lives

In our increasingly digital daily lives, we rely on cybersecurity systems in myriad ways, many of which are invisible to us. We access our bank accounts through online systems that are safeguarded through constant investments and upgrades—by some estimates, banks spend three times as much on cybersecurity as non-financial companies.[20] We shop securely online thanks to advanced encryption techniques that ensures our credit card information is not intercepted during the transaction.[21] We safeguard our treasured documents and photographs stored in the cloud utilizing two-factor authentication—a noted cybersecurity innovation—to make sure that even if our password is cracked, a hacker still cannot gain access.[22] We rely on fraud detection services to flag suspicious transactions on our credit cards.[23] And we utilize antivirus software to prevent malicious software from compromising our devices.

Conclusion

Both in monetary terms and in terms of the number of people affected, the impact of cybercrimes has grown steadily worse in recent years—at least $445 billion was lost in 2017,[24] while at least two thirds of Americans have been the victim of a data breach.[25] Aided and abetted by Cybercrime as a Service (CaaS) and new anonymity tools, the threat from cybercriminals has never been greater, and shows no signs of slowing down. Thankfully, the cybersecurity industry is rising to the challenge, and has grown rapidly in recent years to the nearly $100 billion-per-year juggernaut it is today, with companies across the world expanding their cybersecurity budgets to address new challenges to their business models. The online world may never be perfectly safe, but with the cybersecurity industry ascendant, it stands a fighting chance of weathering cyberattacks in the future.

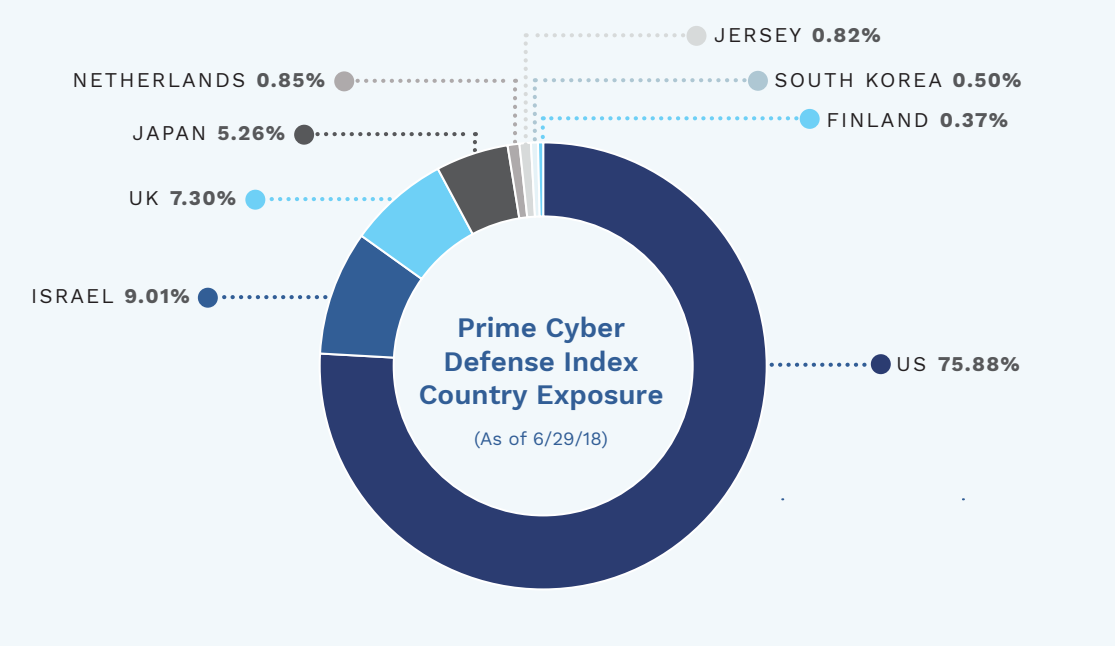
The Prime Cyber Defense Index

The Prime Cyber Defense Index was developed and is owned by Prime Indexes.The index is designed to measure the performance of companies engaged in the Cyber Defense industry that have satisfied specific eligibility requirements. To be considered as part of the Cyber Defense industry a company must either:

i. Engage in providing Cyber Defense applications or services as a vital component of its overall business, or

ii. Provide hardware or software for Cyber Defense activities as a vital component of its overall business.

Prime Indexes also uses additional eligibility and weighting distribution requirements as part of its methodology. Solactive AG calculates and distributes index data on behalf of Prime Indexes.



INDEX COMPOSITION (As of 6/29/18)

Component Name	Ticker	Weight
CISCO SYSTEMS INC	CSCO	4.59%
PALO ALTO NETWORKS INC	PANW	4.47%
SOPHOS GROUP PLC	SOPH	4.32%
QUALYS INC	QLYS	4.23%
FORTINET INC	FTNT	4.16%
JUNIPER NETWORKS INC	JNPR	4.14%
CHECK POINT SOFTWARE TECH	CHKP	4.13%
SYMANTEC CORP	SYMC	4.12%
CACI INTERNATIONAL INC -CL A	CACI	4.09%
TREND MICRO INC	4704	4.03%
IMPERVA INC	IMPV	4.00%
CYBERARK SOFTWARE	CYBR	3.99%
PROOFPOINT INC	PFPT	3.95%
AKAMAI TECHNOLOGIES INC	AKAM	3.93%
COMMVAULT SYSTEMS INC	CVLT	3.86%
SAIC INC	SAIC	3.76%
FIREEYE	FEYE	3.75%
CARBONITE INC	CARB	3.64%
SPLUNK INC	SPLK	3.63%
VERISIGN INC	VRSN	0.99%
F5 NETWORKS INC	FFIV	0.94%
NETSCOUT SYSTEMS INC	NTCT	0.94%
FORESCOUT TECHNOLOGIES INC	FSCT	0.94%
OKTA INC	OKTA	0.94%
BAE SYSTEMS PLC	BA	0.89%
RADWARE LTD	RDWR	0.89%
DIGITAL ARTS INC	2326 JT	0.88%
ULTRA ELECTRONICS HOLDINGS PLC	ULE	0.87%
LEIDOS HOLDINGS INC	LDOS	0.87%
CARBON BLACK INC	CBLK	0.86%
EVERBRIDGE INC	EVBG	0.86%
BOOZ ALLEN HAMILTON HOLDING CORP	BAH	0.86%
VERINT SYSTEMS INC	VRNT	0.86%
GEMALTO NV	GTO	0.85%
MANTECH INTERNATIONAL CORP-A	MANT	0.83%
VARONIS SYSTEMS INC	VRNS	0.82%
MIMECAST LTD	MIME	0.82%
QINETIQ GROUP PLC	QQ	0.82%
ZSCALER INC	ZS	0.79%
ONESPAN INC	OSPN	0.79%
RAPID7 INC	RPD	0.76%
SECUREWORKS CORP - A	SCWX	0.75%
AHNLAB INC	053800	0.50%
KEYW HOLDING CORP/THE	KEYW	0.50%
MOBILEIRON INC	MOBL	0.45%
ZIX CORP	ZIXI	0.43%
A10 NETWORKS INC	ATEN	0.42%
NCC GROUP PLC	NCC	0.40%
F-SECURE OYJ	FSC1V	0.37%
FFRI INC	3692	0.36%

[1] https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

[2] https://www.gigabitmagazine.com/telecoms/cisco-forecasts-over-46-billion-internet-users-2021

[3] https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

[4] http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/

[5] https://www.mcafee.com/us/resources/reports/restricted/economic-impact-cybercrime.pdf

[6] https://www.mcafee.com/us/resources/reports/restricted/economic-impact-cybercrime.pdf

[7] https://www.csoonline.com/article/3223229/security/equifax-says-website-vulnerability-exposed-143-million-us-consumers.html

[8] https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

[9] https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html

[10] https://www.scmagazineuk.com/fbi-says-ransomware-soon-becoming-a-billion-dollar-business/article/630615/

[11] https://www.mcafee.com/us/resources/reports/restricted/economic-impact-cybercrime.pdf

[12] Europol, “Internet Organised Crime Threat Assessment 2017,” 2017

[13] http://www.wired.co.uk/article/job-security-cybersecurity-alec-ross

[14] https://www.barrons.com/articles/cybersecurity-spending-to-hit-90-billion-in-2018-report-1519405299

[15] https://www.investors.com/news/technology/cisco-ibm-dell-ma-brawl-whacks-symantec-palo-alto-fortinet/

[16] http://www.wired.co.uk/article/job-security-cybersecurity-alec-ross

[17] http://www.blumshapiro.com/kbarticle/five-industries-with-growing-cybersecurity-needs

[18] https://www.nytimes.com/2018/05/20/business/banks-cyber-security-military.html

[19] https://www.ft.com/content/535cf6f8-4f8b-11e8-a7a9-37318e776bab

[20] https://www.mcafee.com/us/resources/reports/restricted/economic-impact-cybercrime.pdf

[21] http://scienceline.org/2008/02/ask-mahan-cryptography/

[22] https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/

[23] https://www.cnbc.com/id/46907307

[24] https://www.nytimes.com/2018/05/20/business/banks-cyber-security-military.html

[25] http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/