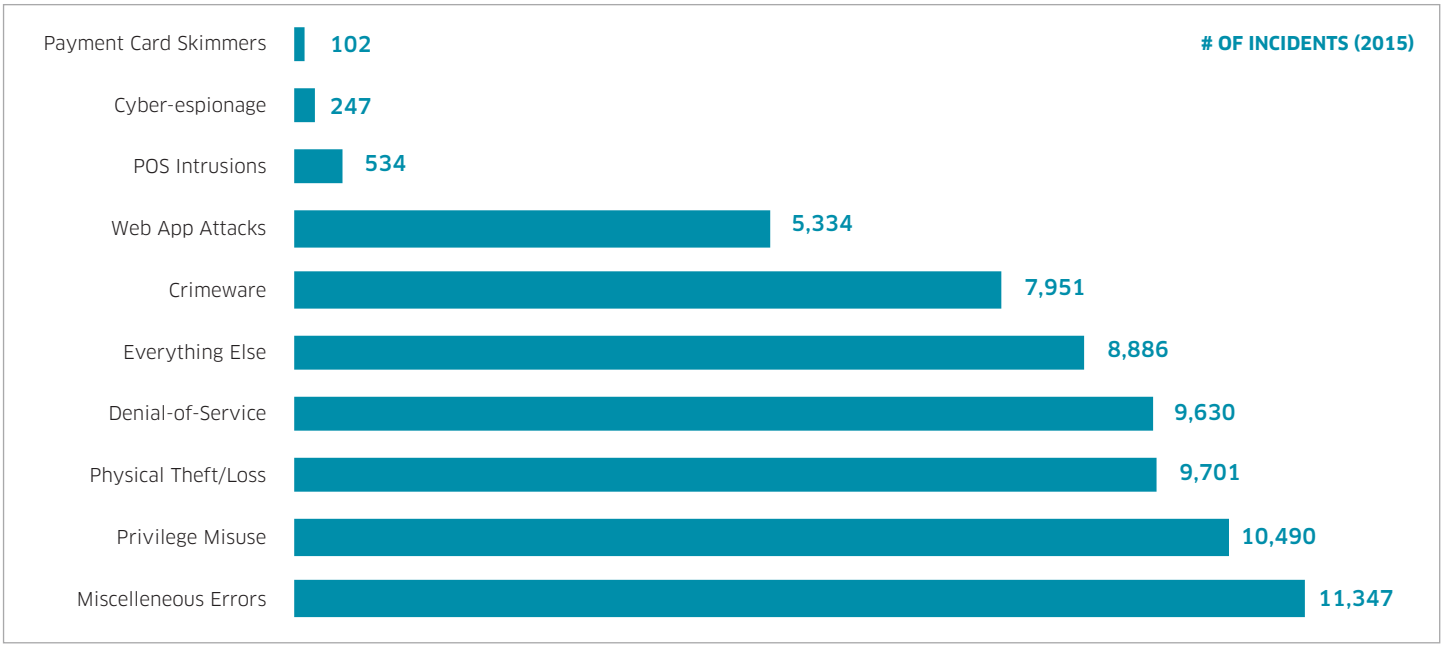
Cybersecurity

Proliferation of Cybercrimes & Reaction by Governments/Corporations

Cybersecurity focuses on protecting computers, networks, programs, and data from unauthorized and/or unintended access. Cybersecurity has become increasingly important recently as governments, corporations, and people collect, process, and store vast amounts of confidential information and transmit that data across networks. Data breaches have become almost commonplace in the last few years. The following will explain the different types of cybercrimes and discuss the most recent "WannaCry" ransomware attack, effects of social media on cybercrimes, and then it will discuss the ways in which corporations and governments are reacting to the threat of cyberattacks.

There are many different types of cyberattacks and the number of incidents varies. The chart below from the 2016 Verizon Data Breach Investigations Report shows the frequency of certain types of incidents in 2015[1]. Although the frequency might change year over year, this chart highlights the prominent threats that people and organizations face when dealing with cybersecurity attacks.

Incidents by Type



http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

A description of each of the above incidents and which industries are most affected by them is given below:

INCIDENT TYPE	DESCRIPTION	INDUSTRIES AFFECTED
Web App Attacks	Any incident in which a web application was the source of attack. This includes exploits of code-level vulnerabilities in the application as well as thwarting authentication mechanisms	Finance, Information, Retail
Point-of-Sale (POS) Intrusions	Remote attacks against the environments where card-present retail transactions are conducted	Accommodation and Food Services, Retail
Privilege Misuse	All incidents tagged with misuse - any unapproved or malicious use of organizational resources - fall within this pattern (mainly insider misuse)	Public, Healthcare, Finance
Miscellaneous Errors	Incidents where unintentional actions directly compromised a security attribute of an information asset	Public, Information, Healthcare
Physical Theft and Loss	An incident where an information asset when missing, whether through misplacement or malice	Public, Healthcare
Crimeware	Any incident involving malware that did not fit into a more specific pattern. Majority of incidents that comprise this pattern are opportunistic in nature and have financial motivation behind them	Public, Information, Finance
Payment Card Skimmers	All incidents in which a skimming device was physically implanted on an asset that reads magnetic stripe data from a payment card	Finance, Retail
Cyber-espionage	Incidents include unauthorized network or system access linked to espionage motive	Public, Information, Manufacturing
Denial-of-Service Attacks	Any attack intended to compromise the availability of networks and systems. Includes both network and application attacks designed to overwhelm systems, resulting in performance degradation or interruption of service	Gaming, Information Technology & IT Services, Finance
Everything Else	Any incident that did not classify in one of the patterns above	Public, Finance, Professional Services, Healthcare

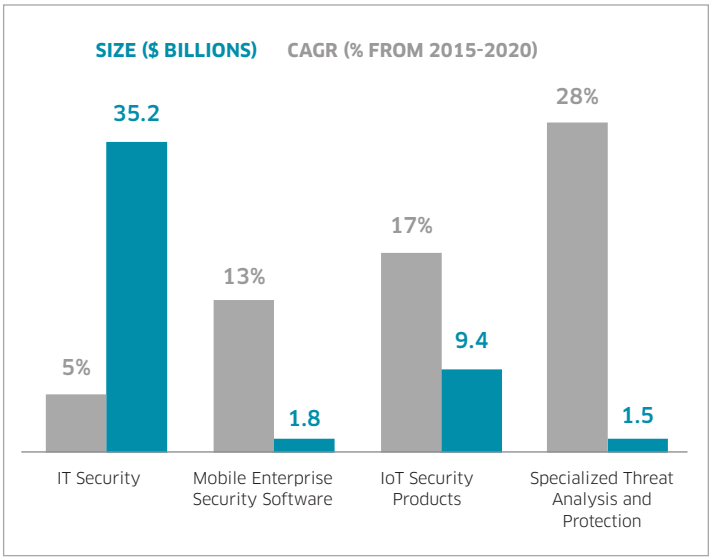
http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

Almost all cybercrimes can be classified into one of the above categories. Most recently, many people were affected by the "WannaCry" ransomware attack. Ransomware is a type of Crimeware (described in the table above) which targets computers, first encrypting the data and then demanding ransom payments in exchange for return of service. Specifically, the "WannaCry" attack targeted computers running the Microsoft Windows operating system and demanded payments in bitcoins. According to numerous reports, the countries affected the most included Russia, Ukraine, Taiwan, and India and roughly $70,000 in bitcoin have been collected by the hackers to date as ransom[2]. Although the attack was briefly thwarted, it has continued to spread through standard file sharing technology used by PCs. An incident such as this one highlights the devastating ramifications that cybercrime can have on people, governments, and organizations.

One of the ways in which cybercrimes have proliferated over the last few years is the growing use of social media on mobile devices. In a research report from Cisco, Facebook scams, which include fake offers and media content along with survey scams, ranked 3rd on the list of most commonly observed malware behind potentially unwanted applications (PUAs) and Trojan droppers[3]. Due to the plethora of people that are on social media, this is a logical territory for cybercriminals to dupe users, which affects not only end-users but also organizations that use social media on corporate networks.

In order to combat cybercrimes, governments around the world have been increasing their cybersecurity spending. The White House states that the U.S. Government will invest over $19 billion for cybersecurity as part of the 2017 budget, a 21% increase from the prior year budget[4]. Cybersecurity Ventures' Q1 2017 Market Report predicts that global cybersecurity spending will exceed $1 trillion over the next five years from 2017-2021. To put it in perspective, in 2004, the cybersecurity market was $3.5 billion, and in 2017, it is expected to be worth more than $120 billion; an approximately 33-34x increase in 13 years[4]. In addition, many companies offer cybercrime prevention services. For example, a lot of the cybersecurity companies offer services along the lines of threat intelligence and prevention. As the chart below illustrates, there has been increasing demand for services that use data analytics to detect insider threats and external attacks, as the Specialized Threat Analysis and Protection segment is projected to have the highest compound annual growth rate even though it is the smallest segment currently[5].

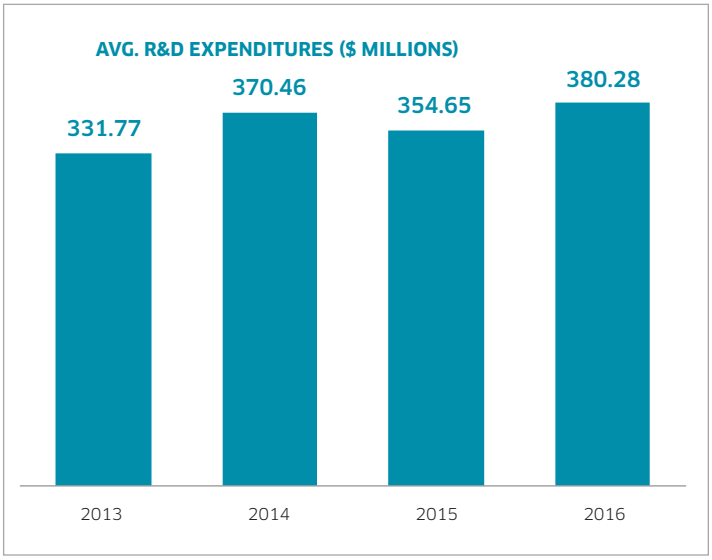
Market Size and Growth



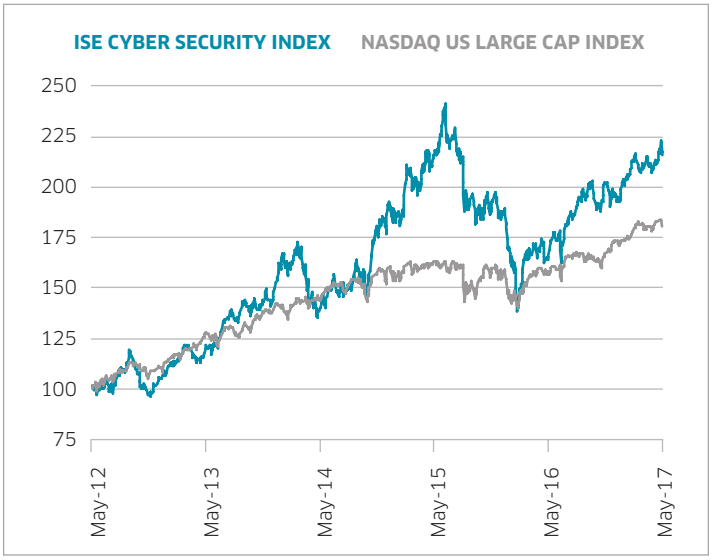
Bloomberg Intelligence (Anurag Rana – Senior Industry Analyst), Sept. 22nd, 2016 and IDC

A large number of companies in the ISE Cyber Security Index (HXR), such as Splunk, FireEye, Palo Alto Networks, amongst many others, offer these types of services to protect consumers, organizations, and governments from cybercrimes. As the chart below shows, average R&D expenditures of companies in HXR have been increasing steadily over the last 3-4 years, which shows that the companies in this index are constantly responding to new threats. This clearly shows that these companies are investing more and more in products and services that prevent cybercrimes, which in turn will help protect their customers: governments and organizations around the world.

R&D Expenditures



ISE Cyber Security Index vs. Nasdaq US Large Cap Index



From 5/18/2012 – 5/18/2017

The chart above shows the performance of the ISE Cyber Security Index against the Nasdaq US Large Cap Index. As the chart, illustrates, the ISE Cyber Security Index has outperformed the benchmark over the last 5 years, which affirms the fact that there is strong demand for companies in the market that provide cybersecurity related services.

In conclusion, the above analysis reveals that there are numerous types of cybercrime incidents that affect people, organizations, and governments. Most recently, the "WannaCry" ransomware attack affected many countries around the world and the attack is continuing to spread. One of the ways in which cybercrimes has augmented over the years has been through the rapid rise of social media. Governments and corporations, however, have been increasing their spending rapidly on cybersecurity measures, specifically on specialized threat analysis and protection measures. This can be seen in the increase in the average R&D expenditures of companies in the ISE Cyber Security Index. As a result, this reveals that companies in this index are continuing to offer products and services that will help mitigate future cybercrimes. Investors looking to invest in companies that provide cybersecurity measures can invest in the product tied to the ISE Cyber Security Index, the PureFunds ISE Cyber Security ETF (HACK). Investors looking for a leveraged product tied to this index can invest in the Direxion Daily Cyber Security & IT Bull 2X Shares (HAKK).

FOOTNOTES:

1. http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf
2. https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/
3. http://www.cisco.com/c/dam/m/digital/1198689/Cisco_2017_ACR_PDF.pdf
4. http://cybersecurityventures.com/cybersecurity-market-report/
5. Bloomberg Intelligence (Anurag Rana – Senior Industry Analyst), Sept. 22nd, 2016 and IDC
6. Data mentioned in the piece is from Nasdaq Index Research, Bloomberg, and/or FactSet, unless otherwise stated

BY GAURAV PENDSE, SENIOR PRODUCT DEVELOPMENT ANALYST, NASDAQ GLOBAL INFORMATION SERVICES