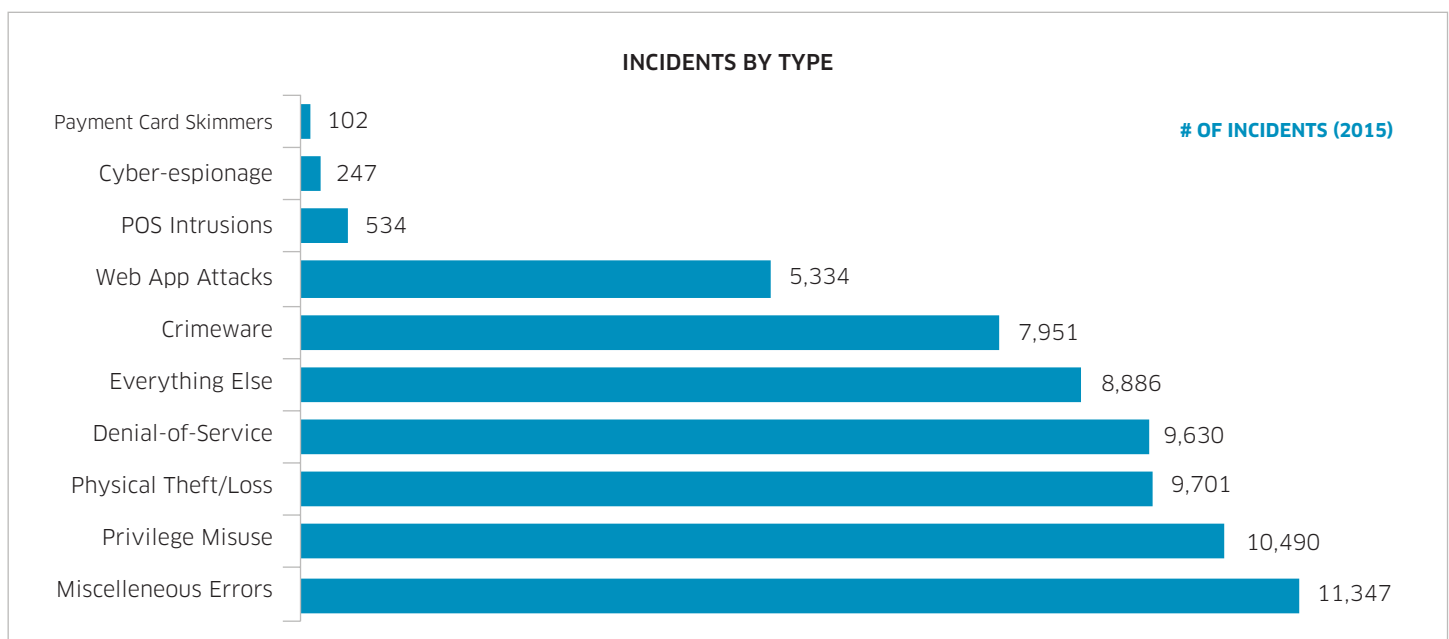Nasdaq

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, then it will discuss the most recent Equifax cyberattack, and then it will talk about 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

 # OF INCIDENTS (2015)

Type	# of Incidents
Payment Card Skimmers	102
Cyber-espionage	247
POS Intrusions	534
Web App Attacks	5,334
Crimeware	7,951
Everything Else	8,886
Denial-of-Service	9,630
Physical Theft/Loss	9,701
Privilege Misuse	10,490
Miscelleneous Errors	11,347

http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf
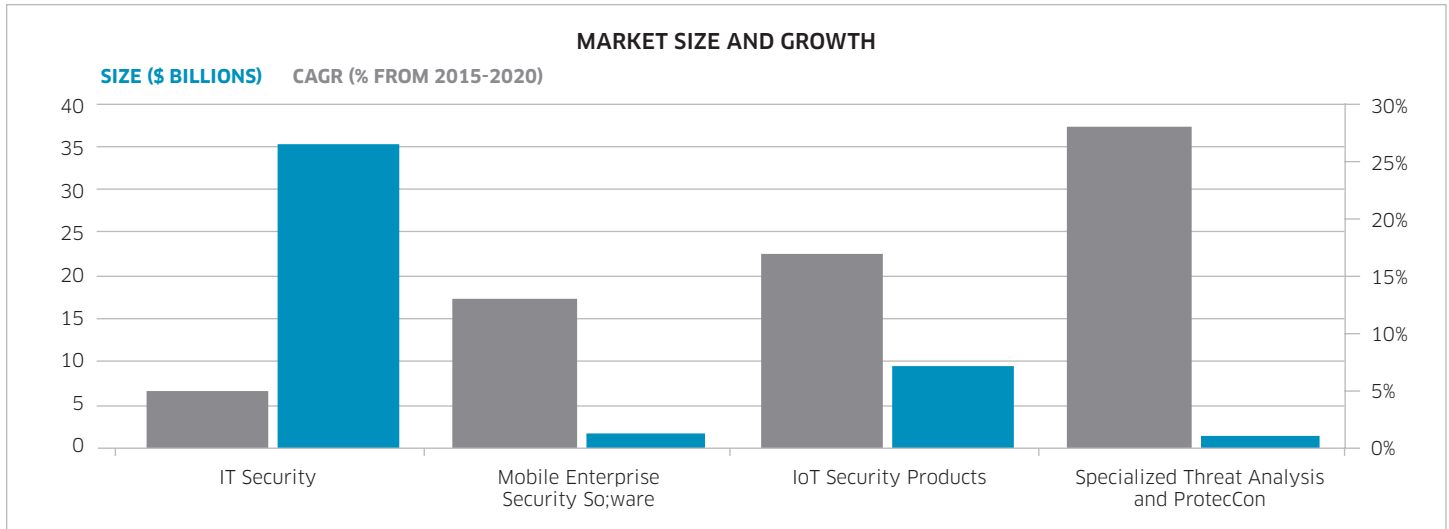
A description of each of the above incidents and which industries are most affected by them is given below:

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
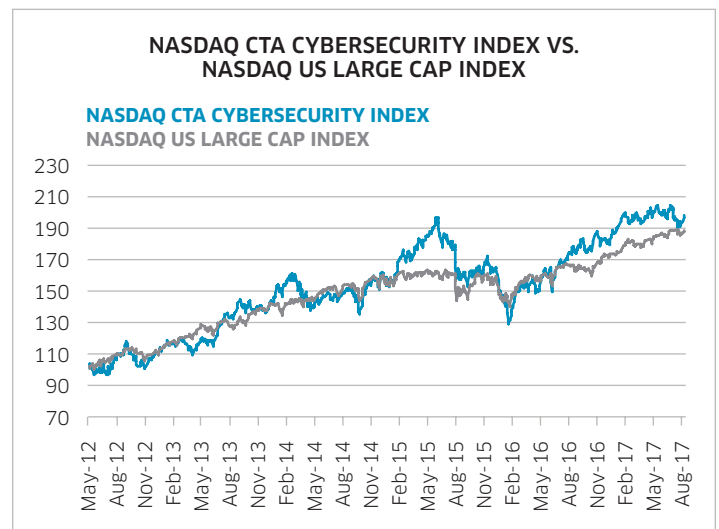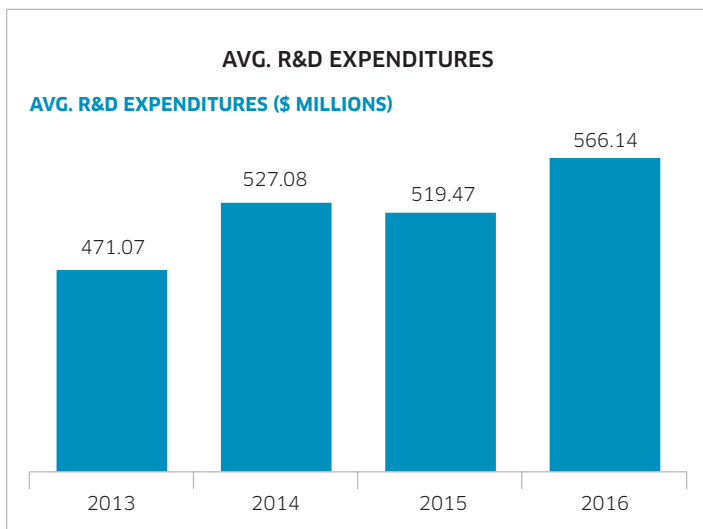
Almost all cybercrimes can be classified into one of the above categories. Most recently, many people in the United States were affected by the Equifax cyberattack. Equifax, a credit reporting agency, announced that their systems were struck by the cyberattack that may have affected about 143 million U.S. customers[2]. This incident is unique when compared to other cyberattacks that have happened in the past because, as one Business Insider analyst called it, the type of data that has been breached as well as the breadth of it is of "perpetual value"[3]. In other words, people's social security numbers, names, addresses, and credit card numbers were hacked and there were a lot of people, 143 million, which were affected, showing the massive breadth of this attack. This type of data is very valuable to hackers, as this data does not change over time. People do not change their names or social security numbers, so it is very easy for criminals to steal someone's identity and then misuse it in any way. Although Equifax has taken some steps to respond to this incident by allowing affected consumers to sign up for their TrustedID Premier service, the vast amount of reputational damage that cyberattacks such as this one can cause to a company, are very difficult to reverse[2].

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

SIZE ($ BILLIONS)   CAGR (% FROM 2015-2020)

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

A large number of companies in the Nasdaq CTA Cybersecurity Index (NQCYBR), 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 NQCYBR 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.

AVG. R&D EXPENDITURES

AVG. R&D EXPENDITURES ($ MILLIONS)

NASDAQ CTA CYBERSECURITY INDEX VS. NASDAQ US LARGE CAP INDEX

NASDAQ CTA CYBERSECURITY INDEX
NASDAQ US LARGE CAP INDEX

From 5/18/2012 – 8/31/2017

The chart above shows the performance of the Nasdaq CTA Cybersecurity Index against the Nasdaq US Large Cap Index. As the chart, illustrates, the Nasdaq CTA Cybersecurity 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 Equifax cyberattack affected many people in the United States, in which private identity information was compromised. 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 Nasdaq CTA Cybersecurity 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 products tied to the Nasdaq CTA Cybersecurity Index, such as the First Trust Nasdaq Cybersecurity ETF (CIBR) or the Betashares Global Cybersecurity ETF (HACK).

More Information

For more information on the Nasdaq CTA Cybersecurity Index (NQCYBR), please visit business.nasdaq.com/indexes.

Footnotes

1. http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf
2. https://www.bloomberg.com/news/articles/2017-09-08/consumers-struggle-to-get-answers-from-equifax-after-massive-hack
3. http://www.businessinsider.com/equifax-breach-hack-exposed-most-valuable-information-2017-9
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