# A STUDY OF CYBER ATTACKS AND IT’S AFFECTS ON EQUITY MARKETS AND STOCKS

KUNJ DESAI, FELIX ANDERSEN, DHRUV PATEL

Keywords: cyber security, cyber-crime, stock performance, cloud computing, equity markets.

## 1. INTRODUCTION

It is clear that over the last few years the world has seen an increased need for cybersecurity. While cyber-attacks are not new, it has become more prevalent in the last two decades as a result of the exponential growth in the incorporation of technology into daily business activity – data storage, CRM systems, IT infrastructure, and the like. Cyber-attacks cost companies significant damage, both in a fiscal and reputational sense. Security breaches cost companies billions of dollars annually in stolen assets, lost business and damaged reputation. The knock-on effect results in loss of goodwill and customer turnover, which ultimately results in loss of revenue and a contraction in profits. Cybersecurity Ventures estimates that cybercrime damage will cost the world $6 trillion annually by 2021. It comes as no surprise then that companies pour money continuously to upgrade digital defences in an effort to curb attacks. According to Gartner, as of December 31, 2019, average spending on cybersecurity now stands between 5 and 8 percent of firms’ overall technology budget across industries. For instance, in 2018, J.P. Morgan disclosed spending on cyber-security stands at roughly $600 million per year. Microsoft invests over $1 billion each year on cybersecurity; they have stated the budget will continue for the foreseeable future. Bank of America, on the other hand, stated they have an unlimited budget for cybersecurity, the only department with no constraint on spending. The ability for companies to defend against cyber-attacks is a key top of mind issue. As such, it is reasonable and clear that cyber-attacks have an adverse impact on financial markets. As such, the main topic this paper will cover will be relationship between cyber-attacks and equity markets.

## 2. BRIEF OVERVIEW OF CYBERATTACKS AND INCREASE IN SPENDING

In an article released by CNBC in mid-December of 2019, they showed that hackers had accessed nearly 8 billion consumer records for the year 2019. The Identify Theft Resource Center ranked the largest data breaches in 2019, based on the number of accounts compromised. Additionally, within the report, companies such as WhatsApp and Fortnite reported security flaws that potentially exposed customer data for millions of users. In looking at the five largest hacks of 2019, it becomes apparent that nefarious actors target a range of industries – healthcare, financial institutions and mobile gaming. It is not surprising since hackers seek rich consumer data, which can be found in a wide range of industries.

The fifth largest attack hit the billings and collections vendor of Quest Diagnostics, American Medical Collection Agency (AMCA), with roughly 12 million records stolen over a period of eight months. The records included medical, financial and personal information of 11.9 million customers. Credit card numbers, bank account information, medical information and Social Security numbers were all compromised. The AMCA hack also hit

LabCorp, a competitor of Quest, exposing the personal and financial data on around 7.7 million customers.

Experian published a report in 2017 detailing how much information can be sold for on the Dark Web. Social security numbers sell for a single dollar. Credit, or debit, cards go for between 5 and 110 dollars depending on the accompanying information, such as if bank information is included. On the other hand, medical records can sell for between 1 and 1000 dollars. It's therefore quite possible the hack on Quest Diagnostics could have profited the hackers well into the millions. The result was catastrophic for AMCA. AMCA's largest clients, including Quest and LabCorp, dropped the company after learning of the breach. Weeks after revealing the breaches, AMCA's parent company was forced to file for bankruptcy citing the enormous expenses related to notifying customers and being dropped by its largest customers. The case of AMCA depicts that kind of reputational damage a cyber-attack can have on a company, and the level of damage that can be inflicted. In an article released by CNBC in 2019, they cited a report by insurance carrier Hiscox, which states that 60 percent of small businesses go out-of-business within 6 months of being the victim of a cyber-attack. The issue of data security has become top of mind for many business leaders now.

Around fifteen years ago, the cybersecurity market worldwide was worth $3.5 billion dollars. In the next thirteen years, the market grew around 35 times. Largely driven by spending, the market will continue to growth further into the future and spending largely acts as a function of an increase in cybercrime activity. For comparison, spending in other tech sectors is driven by reducing inefficiencies and driving productivity.

Already mentioned in the introduction, several big companies – Bank of America, JP Morgan and Microsoft – have dedicated a significant portion of company budgets to building strong, cybersecurity infrastructure. On a more macro level, Cybersecurity Ventures predicts that global spending on cybersecurity products and services will exceed $1 trillion cumulatively between 2017 and 2021. On an annual basis, predictions are for global spending on information security to be $170 billion in 2022.

It's interesting how spending varies between industries. Energy companies, for instance, invests less than 0.2 percent of their revenue into cybersecurity. This is in despite of energy networks being vulnerable to cyber-attacks. This vastly differs from financial institutions and technology companies that believe cybersecurity is a must. Hackers can cause power outages, placing national defence infrastructure at risk and putting many citizens at risk. In 2020, it is projected that half of all organizations in healthcare, technology, retail, manufacturing and business services to increase overall information technology spending. In a survey on business leaders, 36 percent noted that spending is largely driven by a need to improve security infrastructure and cyber risk management. On an overall basis, 62 percent of organizations are increasing cybersecurity spending for full year 2020. While cybercrime will find ways of affecting businesses despite measures taken, companies will continue to divert resources to building out infrastructure that can make their data and systems more secure. In this paper, we will discuss three companies – Equifax, Marriott and Capital One – who have experienced significant cyber damage and discuss the impact it had.

## 3. CASE STUDY ON CYBER-ATTACK AT EQUIFAX

### 3.1 About Equifax

Equifax is one of the three major credit reporting agencies (CRAs) – also known as credit bureaus – in the U.S. It creates credit report on any individual giving a detailed picture of a person’s credit history along with the loan and credit card payments. They get this information through the businesses i.e. the credit card companies, bank, employers, and others. So, how does this credit card systems work?

When an individual applies for a credit card, the lender will pull out his/her information from one of the CRAs to check the history of repaying their debts. Based on the reports, an individual gets his/her credit card with the limit to spend and repay them. Credit report can have a major impact on people’s lives.

### 3.2 About the attack

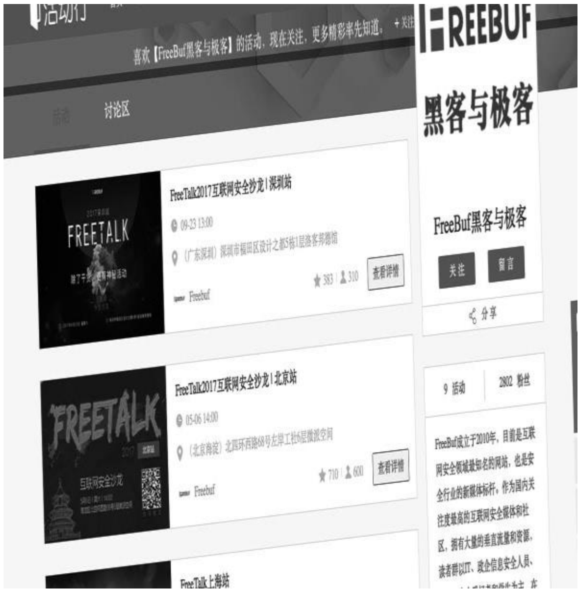
On September 7, 2017, Equifax announced that it had breached the data of almost 143 million U.S consumers. It was not limited to U.S as some consumer from UK and Canadian were also affected but were not given specific numbers. The company claimed stated that it happened from mid-May through July 2017. Furthermore, they also said that the data was not breached from the Equifax’s core consumer database but from the U.S online dispute web portal.
The data included:

1. Names
2. Social Security Numbers
3. Birth dates
4. Address
5. Driving License Number

The vulnerability stemmed from a custom-built tech system that dated back to the 1970s and had not received an important software patch, according to the 96-page report by the House Committee on Oversight and Government Reform. The US Department of Homeland Security had alerted Equifax to the software risk and the company’s teams had even discussed the necessary patch, yet it was not fully implemented. The following day, the Department of Homeland Security contacted Equifax, Experian, and TransUnion to notify them of the vulnerability.

Nike Zheng, a Chinese cybersecurity researcher from a bustling industrial center near Shanghai, probably knew little about Equifax or the value of the data pulsing through its servers when he exposed a flaw in popular backend software for web applications called Apache Struts. Information he provided to Apache, which published it along with a fix on March 6, showed how the flaw could be used to steal data from any company using the software.

Even though the Americans had no reason to investigate it. But the global hacking community noticed. Within 24 hours, this information was posted to FreeBuf.com, a Chinese security website, and showed up the same day in Metasploit, a popular free hacking tool.



喜欢【FreeBuf黑客与极客】的活动，现在关注，更多精彩率先知道。 + 关注

FreeTalk2017互联网安全沙龙 | 深圳站
09-23 13:00
（广东深圳）深圳市福田区设计之都5栋1层洛客邦體館
383 | 310
Freebuf

FreeTalk2017互联网安全沙龙 | 北京站
05-06 14:00
（北京海淀）北四环西路68号左岸工社6层微派空间
710 | 600
Freebuf

FreeTalk上海站

FreeBuf黑客与极客

9 活动 | 2802 粉丝

FreeBuf成立于2010年，目前是互联网安全领域最知名的网站，也是安全行业的新媒体标杆，作为国内关注度最高的互联网安全媒体和社区，拥有大量的垂直流量和资源，读者群以IT、政企信息安全人员、

On March 9, 2017, an internal email notification was sent to Equifax administrators directing them to apply the Apache patch. Equifax's information security department ran scans on March 15, 2017 that were meant to identify systems that were vulnerable to the Apache Struts issue, but the scans did not identify the vulnerability. But between March 9, 2017 and March 15, 2017, i.e. on March 10, 2017 hackers started scanning the internet for computer systems that may be vulnerable to the attack and that time Equifax got hit, according to the investigation.

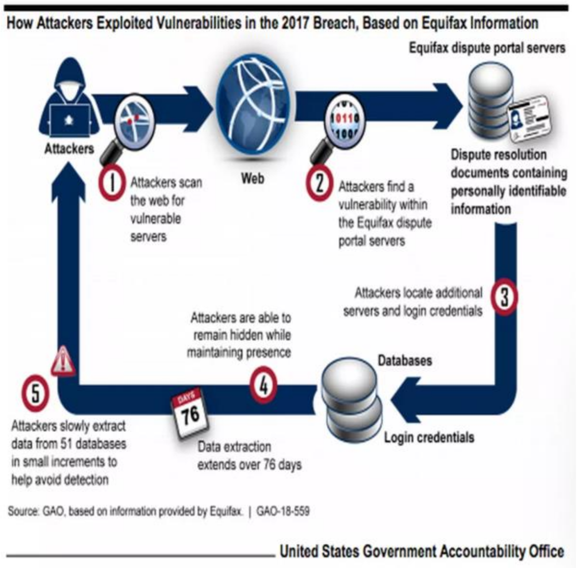
This vulnerability was left unpatched until July 29, 2017 when the company’s information security department discovered ‘suspicious network traffic’ associated with its online dispute web portal and applied for Apache patch. Later, they again observed a similar network traffic after which they immediately took the system offline. After careful investigation it was revealed that an additional 2.5 million U.S consumers were affected by the breach adding up to 145.5 million. This time Equifax announced that around 8000 Canadian and 693,665 UK consumers were affected. However, the web portal was offline for 11 days while the security team found out and closed the backdoor the intruders had set up.

## 3.3 Technical aspects of the attack

As the details about this vulnerability was available on the Chinese website, intruders simply installed a backdoor know as web shell. Although it did not matter whether Equifax had fixed the vulnerability after that. The hackers had an invisible door into the company’s network.

The Moloch data suggests the initial group of hackers struggled to jump through internal roadblocks like firewalls and security policies, but that changed once the advanced team took over. Those intruders used special tunneling tools to slide around firewalls, analyzing and cracking one database after the next-while stockpiling data on the company's own storage systems.

Besides amassing data on nearly every American adult, the hackers also sought information on specific people. It was not clear why, but experts suggest two possibilities: They were looking for high-net-worth individuals to defraud, or they wanted the financial details of people with potential intelligence value. So, here is an overview of how Equifax data breach happened –


How Attackers Exploited Vulnerabilities in the 2017 Breach, Based on Equifax Information

Equifax dispute portal servers
Attackers
1 Attackers scan the web for vulnerable servers
Web
10110
100
2 Attackers find a vulnerability within the Equifax dispute portal servers
Dispute resolution documents containing personally identifiable information
3 Attackers locate additional servers and login credentials
Databases
Login credentials
4 Attackers are able to remain hidden while maintaining presence
DAYS
76
Data extraction extends over 76 days
5 Attackers slowly extract data from 51 databases in small increments to help avoid detection

Source: GAO, based on information provided by Equifax. | GAO-18-559

United States Government Accountability Office

## 3.4 After the attack

One person briefed on the probe being conducted by the Federal Bureau of Investigation and U.S. intelligence agencies said that there is evidence that a nation-state may have played a role, but that it does not point to China. The person declined to name the country involved because the details are classified. The security consulting firm hired by Equifax reports that they did not have enough data to identify either the attackers or their country of origin.

According to an internal analysis of the attack, the hackers had time to customize their tools to more efficiently exploit Equifax's software, and to query and analyse dozens of databases to decide which held the most valuable data. One U.S government official said leads being pursued by investigators include the possibility that the hackers had help from someone inside the company.

Future steps taken:

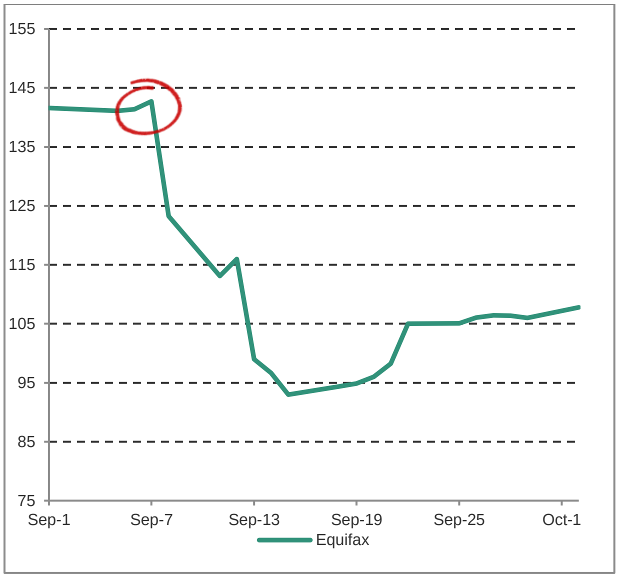
1. Work to help consumers (you can offer credit monitoring or other services).
2. Increase your cybersecurity measures to prevent future attacks.
3. Show your customers how you are improving security through open communication and a commitment to transparency.

### 3.5 Impacts on business and equity prices

The breach made national and international headlines and caused its shares to drop 13 percent in the immediate aftermath. Lawsuits regarding the incident are still ongoing. Most people surveyed were aware of the Equifax hack. A year after the incident, 72.9 percent of survey respondents knew about the breach, compared to 84.2 percent who knew immediately after the breach occurred.

Below figure shows of the change in equity price:

*Changed day returns since it's a very new cyber attack



| | |
|---|---|
| 1 - day return | -13.66% |
| 5 - day return | -32.27% |
| 15 - day return | -25.74% |

How did Equifax improve its company image?

After the data breach, the company took two steps intended to remedy the issue: free credit monitoring for one year and a waiver of the requirement that all disputes be settled through arbitration. These offers were meant to both protect consumers from the impact of the hacking and soften the public relations blow on Equifax.

The LendEDU survey found that consumers were of two minds about Equifax's attempts to remedy the problem. Almost one-third (30.6 percent) said these steps had helped to change their minds about Equifax for the better, but nearly as many (28.4 percent) had not yet forgiven the company (20.3 percent did not have an opinion).

Although after-the-fact remedies can appease some consumers, they may not be enough to prevent hackers from utilizing stolen data. Such actions also might not satisfy other customers, who may be angry that their data was not secure in the first place.

### 3.6 Possible preventions

1. Demanding more from data brokers
2. Boosting breach notification
3. More protection for Social Security numbers
4. More consumer protections—for free

## 4. CASE STUDY ON CYBER-ATTACK AT CAPITAL ONE

### 4.1 About Capital One

Capital One Financial Corporation is an American financial institution holding organization specializing in credit cards, auto loans, banking, and financial savings accounts. It is ranked 11h on the list of largest banks in United States by assets. With a market share of 5%, it is the second largest auto finance company in United states. Capital One follows mainly three divisions – credit cards, customer banking and commercial banking. The overall revenue of Capital One in the fourth quarter of 2019 was. 5.61B and net income was 1.18B.

### 4.2 About the attack

Capital One operates a Responsible Disclosure Program where security researchers can report security vulnerabilities identifies in any product, system, or asset belonging to Capital One potential via email. This breach started between the 22nd -23rd March and was discovered almost four months later. On July 17th, 2019 the company received an email where the sender attached a GitHub link of Paige A. Thompson’s account on which the sender claimed there was the leaked s3 data of the company. Later on, FBI and Capital One disclosed that the data breach contained 106 million credit card applications that compromised information like names, addresses, phone numbers, and dates of birth, along with 140,000 Social Security numbers, 80,000 bank account numbers, and some credit scores and transaction data and the posted data on GitHub contained a file directory related to the stolen information, but not the data itself. The breach also affected 6 million Canadians, including one million Canadian Social Insurance numbers, in addition to the more than 100 million US consumers impacted.

The details set it apart from breaches of companies such as Equifax and Marriott, which were attacked from the outside by criminals with a nation-state connection. It’s also different from the spate of ransomware attacks against major U.S. cities, which were likely committed by groups of individuals outside the U.S.

Paige A. Thompson’s, 33-year-old, formerly worked as a system engineer from 2015 to 2016 for Amazon Web Services(AWS) simply took advantage of a misconfiguration in the Amazon Web Services (AWS) and web application firewall (WAF). Thompson went by the hacker name "erratic" in many online accounts and forums, but she did not use any alias while uploading the data on GitHub. Moreover, Thompson also made statements on social media for evidencing the fact that she has information of Capital One, and that she recognizes that she has acted illegally. She was also listed as the organizer of a group on Meetup, a social network, called Seattle Warez Kiddies, described as a gathering for “anybody with an appreciation for distributed systems, programming, hacking, cracking.” Once alerted to the breach, the authorities found what they said were Ms. Thompson’s online boasts that she wanted to “distribute” the materials.

One screenshot of a Slack conversation from the criminal complaint shows an unnamed individual saying, "sketchy shit, don't go to jail plz," after Thompson allegedly posted a link to information about the stolen data. Another screenshot shows some of Thompson's alleged messages sent over Twitter direct messages. "Ive basically strapped myself with a bomb vest, fucking dropping capitol ones dox and admitting it. I wanna distribute those buckets i think first. There ssns…with full name and dob."

After the tipster alerted Capital One about the breach, Capital One quickly alerted law enforcement to the data theft allowing the FBI to trace the intrusion. The FBI connected the incident to Thompson quickly because it was easy to link the GitHub page which included Thompson’s full name and resume. The FBI also noticed Thompson’s activity on Meetup and used it to trace her other online activities, eventually linking her to posts describing the data theft on Twitter and the Slack messaging service. They verified her identity after she posted a photograph of an invoice, she had received from a veterinarian caring for one of her pets. Thompson had her full name and resume on the GitHub account where she posted the data. They also found devices in her possession that reference Capital One and Amazon as well as other entities that may have been targets of attempted or actual breaches.

### 4.3 Technical aspects of the attack

The type of cyberattack Thompson did is known as a Server-Side Request Forgery (SSRF), which makes a server execute unauthorized commands on behalf of a remote user. This trick enables the attacker to treat the server as a proxy for requests and gaining access to private endpoints. Thompson attempted to Capital One’s data around March 12, 2019 from a TOR endpoint using the VPN company IPredator and the credentials for a WAF-Role (WAF protects web applications such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others). Nearly two weeks later on March 22nd, the WAF-Role listed all of Capital One’s buckets and downloaded the credit card application data from one of them. According to Capital One, this role does not usually invoke the List Buckets action, and this was the only time it accessed these files.

### 4.4 After the attack

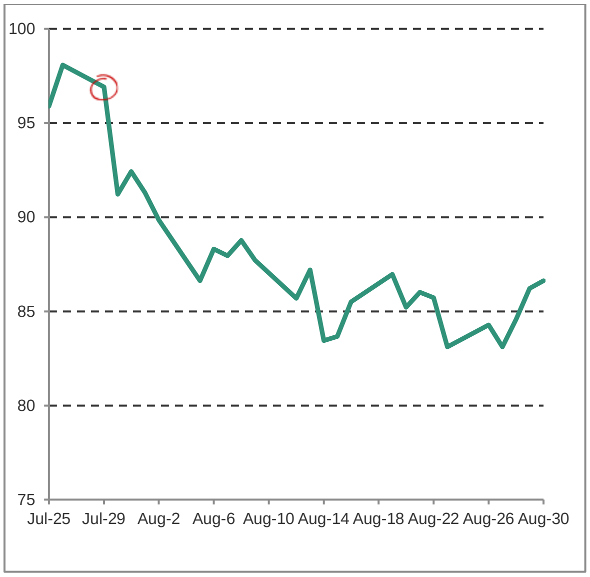
Amazon made a statement saying that AWS was not compromised in any way and functioned as designed and also briefed about the reason for breach stating that it was a misconfiguration of firewall settings on a web application that was managed on the cloud server by Capital one and not a vulnerability in the cloud server itself.

Capital One said that they immediately fixed the exploit and started working with the federal law enforcement on the breach. They also stated that the attacker who stole the data was captured by the FBI. Capital One will reach out to customers who were part of the hack and will offer free credit monitoring and identity protection to those customers affected by the breach. The company also ensured to have heavy investment in cybersecurity and will continue to do so. The government stated that they believe the data has been recovered and that there is no evidence the data was used for fraud or shared by this individual.

### 4.5 Impacts on business and equity prices

The breach affected approximately 100 million individuals in the United States and costed around $100 million to $150 million. The shares of Capital One skipped by 5.89% on July 29th, 2019 and shares of Amazon skipped by 0.5% even though Amazon was not compromised by the breach. Capital One was majorly affected by this attack and the stock has fallen from around the $100 mark before the breach to roughly around $85. The breach has also exposed the bank to several class-action lawsuits and regulatory fines. Moreover, customer confidence is likely to remain low over subsequent quarters which can impact Capital One's revenues by 3% between 2019 – 2021.

The figure below shows the graph for equity prices drop from July 29th, 2019.



The table below shows price drops in stocks on the basis of days after the breach.

| | |
|---|---|
| 1 - day return | -5.89% |
| 5 - day return | -10.63% |
| 15 - day return | -10.27% |

While Capital One has a cyber-security insurance policy in place but this policy will not yield any payments for Capital One over the next three years which will cost the company higher total expense and thereby reducing the EBT figure over these three years. This would have an adverse effect on EPS figure, which is expected to reduce by roughly 15% for each year. In the third quarter of the year 2019 right after the breach, net income dropped by 11.25%, revenue dropped by 2.07%, EPS dropped by 10.03% ,and net profit margin by 9.36% which by the end of the fourth quarter came down to 10.61% reducing the net change in cash by $3.79B which is 303.55%.

4.6 Possible preventions

Capital One's WAF-Role had permissions to access credit card application data which should have been avoided. The WAF-Role may require access to the list of the names of all Capital One's buckets, but the web application firewall should have avoided to download a bucket containing private customer information and the resources should have been restricted over the roles with appropriate permissions and access. Capital One should have avoided to hold both WAF and private customer information in the same bucket and also should not have WAF and credit card web applications run from the same server with both justifying its role to own permissions for that bucket.

Capital One is one of the largest users of AWS and developed Cloud Custodian (a rules engine for managing public cloud accounts and resources). This product should have been used to alert authorities at Capital One to the suspicious activity made by WAF-Role. WAF-Role accessed files which it should not have from an external IP and not one inside Amazon. Amazon offers a WAF solution which integrates with CloudFront and blocks suspicious requests before they reach your servers. In Capital One's data breach, the attacker had the public IP address of a server and thus, the attacker did not pass through CloudFront at all. Using the CloudFront service would have stopped the attacker from gaining the public address of the server and may have blocked the requests. To avoid such attacks, the identity permissions and access must be well defined and carefully verified.

## 5. CASE STUDY ON CYBER-ATTACK AT MARRIOTT

### 5.1 About Marriott

Marriott International, Inc. is an American multinational diversified hospitality company that manages and franchises a broad portfolio of hotels and related lodging facilities. It has 30 brands with 7,003 properties in 131 countries and territories around the world, over 1,332,826 rooms (as of March 31, 2019), including 2,035 that are managed with 559,569 rooms, 4,905 that are franchised or licensed with 756,156 rooms, and 63 that are owned or leased with 17,101 rooms, plus an additional 475,000 rooms in the development pipeline and an additional 25,000 rooms approved for development but not yet under signed contracts.

### 5.2 About the attack

On November 30, 2018, Marriott disclosed that its Starwood Hotel brand had been subject to a security breach. After the disclosure, New York Attorney General Barbara Underwood announced an investigation into the data breach. This was the greatest ever data breach suffered by the Hotel group Marriott affecting over 500 million customers. The firm revealed its Starwood division's guest reservation database had been compromised by an unauthorised party.

The Information accessed included:

1. Payment information.
2. Names
3. Mailing addresses
4. Phone numbers
5. Email addresses
6. Passport numbers.

This is a major incident affecting a huge number of customer details. Even Facebook's hack affecting 50 million is dwarfed by this latest breach of up to 500 million. Even, if as Marriott says, the number of customers that suffered a breach of personal information is anywhere near 327 million, the implications are massive.

But the actual dates bring us back to September 8, 2018. On this day, an internal security tool flagged as suspicious an attempt to access the internal guest reservation database for Marriott's Starwood brands, which include the Westin, Sheraton, St. Regis, and W hotels. But the attackers were already inside the systems of Starwood Guest Reservation Database since 2014. Marriott recently discovered that an unauthorized party had copied and encrypted information and took steps towards removing it. The Guardium alert was triggered by a query from an administrator's account to return the count of rows from a table in the database, according to Sorenson. This query stood out because it indicated a human operator was interfering with the database.

### 5.3 Technical aspects of the attack

On September 10, Marriott called on third-party investigators to investigate whether it had been breached. Soon afterwards, malware on the Starwood IT systems was found: A Remote Access Trojan (RAT), which allows hackers to covertly access, survey, and gain control over a computer. At this point, the customers were not informed about their data being compromised. This investigation continued through October 2018 and they discovered a penetrating tool called Mimikatz (a tool for discovering usernames and passwords in computer systems' memory). This raised suspicions because the tool is also used by hackers to search a device memory for usernames and passwords and could have been used by attackers to move from Starwood to other parts of the network.

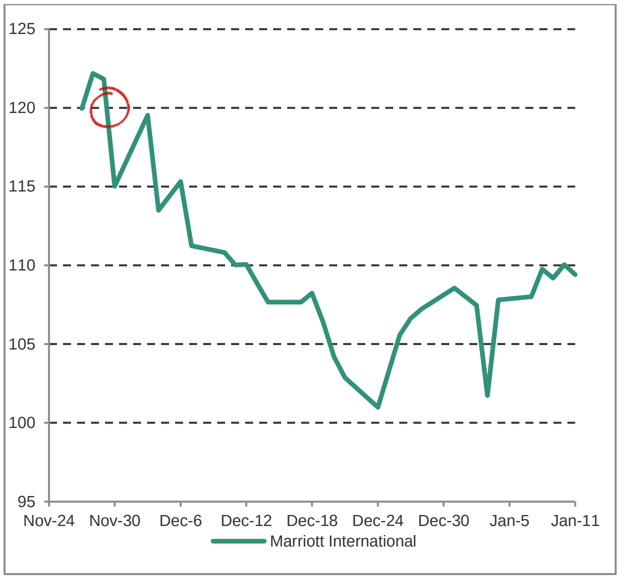
It was in November that Marriott realized hackers had been in the system since July 2014. And later that month, the firm found that customer data had indeed been breached. Sorenson descried how, on November 13, investigators discovered evidence that two compressed, encrypted files had been deleted from a device. On November 19, 2018, Marriott was able to decrypt the information and determined that the contents were from the Starwood guest reservation database.

### 5.4 Impact on business and Equity Price

After GDRP's new regulation proposed in May 2018, Companies will be fined up to 4% of global revenue for a violation of European privacy and protection laws. Rettas compared the Marriott breach to the one Equifax suffered in 2017, and how, in the aftermath, shares of Equifax fell more than 35% after the company disclosed it. While noting that he's not a financial analyst and doesn't give financial advice, Rettas said he believes “The company's not in big trouble, especially if we look at how these types of incidents have affected the finances of other companies who have experienced similar incidents in the past.”

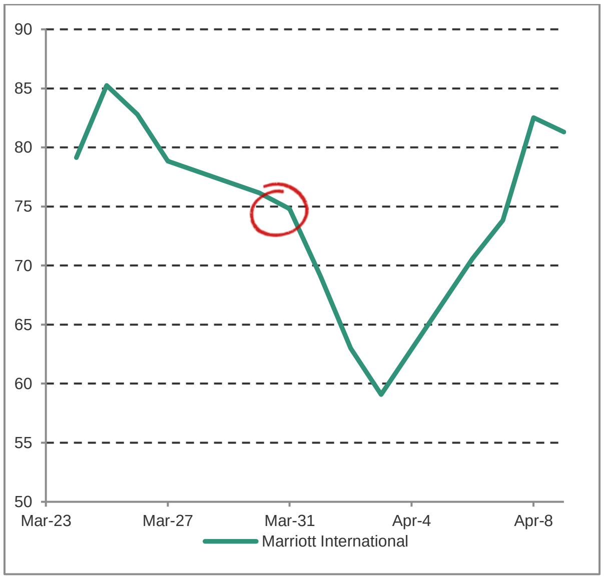
**Note**: Day returns are from when the cyber-attack was disclosed

Marriott Nov. 30/2018



| 1 - day return | -5.59% |
|---|---|
| 5 - day return | -8.69% |
| 15 - day return | -15.56% |

Marriott Mar. 31/2020



| | |
|---|---|
| 1 - day return | -7.57% |
| 3 - day return | -21.03% |
| 5 - day return | -1.32% |

5.5 Possible Prevention

1. Differential Privacy
2. Pseudonymization
3. Risk Based anonymization
4. Tokenization
5. Data Masking

## 6. CONCLUSION

Cyber-attacks can cause major damages to any business. Severe breaches can affect the business standing as well as customers' trust. Impacts of a security breach for any company can be financial, reputational, or legal. Cybercrime is estimated to cost over $400 billion dollars annually to the global economy. Studies have also shown that stock market reacts strongly to the events of cyber-attacks. Also, the excess returns drop the day after the breach announcement and continues to up to 35 days in average case. In this paper, an attempt has been made to explore and explain the cyber-attacks on some of the largest financial firms and the effects on stock market due to these data breaches. Although our results are obtained studying merely three case studies, our work can be deepened to understand the source of the attack, the motivation of cyber-criminals, preventions for these breaches, and global affect of these attacks on equity markets. Figure 6.1, shows data breaches occurred since 2005 and the economic loss of each organisation in millions.

## 7. REFERENCES

1. https://www.cnbc.com/2019/12/17/the-5-biggest-data-hacks-of-2019.html
2. https://www.cnbc.com/2019/07/30/capital-one-breach-customer-records-social-security-numbers.html
3. https://www.csoonline.com/article/3520988/cybersecurity-spending-trends-2020.html
4. https://cybersecurityventures.com/cybersecurity-market-report/
5. https://www.wsj.com/articles/tech-chiefs-plan-to-boost-cybersecurity-spending-11577701802
6. https://www.forbes.com/sites/kateoflahertyuk/2018/11/30/marriott-breach-what-happened-how-serious-is-it-and-who-is-impacted/#7fc1dfc7d25a
7. https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html
8. https://www.forbes.com/sites/kateoflahertyuk/2019/03/11/marriott-ceo-reveals-new-details-about-mega-breach/#21074d1f155c
9. https://www.cshub.com/attacks/news/the-aftermath-of-the-massive-marriott-data-breach

10. https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros
11. https://epic.org/privacy/data-breach/equifax/
12. https://www.cnet.com/news/equifaxs-hack-one-year-later-a-look-back-at-how-it-happened-and-whats-changed/
13. https://tdwi.org/articles/2018/10/29/biz-all-impact-of-equifax-data-breach.aspx

14. https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html
15. https://dashboards.trefis.com/no-login-required/6wWMG2mo/Capital-One-Earnings-Performance-and-2019-Forecast
16. http://www.documentcloud.org/documents/6224691-Paige-Thompson-DOJ-complaint.html
17. https://www.wired.com/story/capital-one-hack-credit-card-application-data/
18. https://www.capitalone.com/facts2019/2/
19. https://www.usatoday.com/

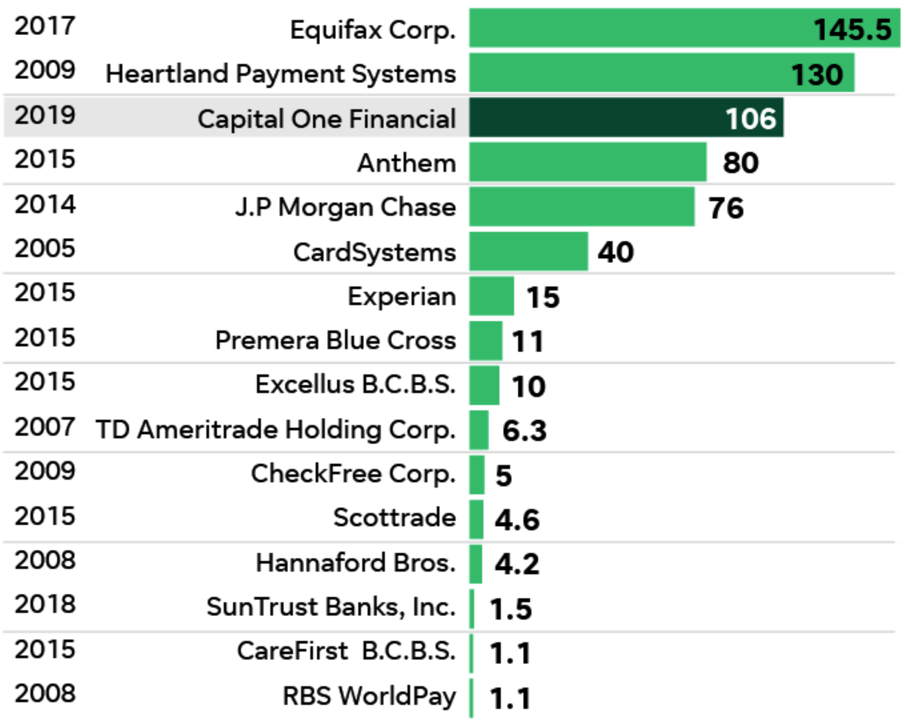


Figure 6.1 Records breached in millions