Facebook Data Breach Case Study

There are multiple cyberlaw principles that a company must follow to protect their assets as well as the information of their users. It is also important that a company follow laws put in place to protect consumers both online and offline following best practice standard throughout the industry. I have chosen to base my case study on the recent Facebook Data breach which is known to have occurred in September 2018. This attack on Facebook is now considered the largest in the Company’s 14-year history, one where personal information of nearly 50 million users were exposed (Isaac, 2018).

One principle of cyberlaw is to conduct risk assessments, this is meant as a way to design a comprehensive program or strategy to identify assets, vulnerabilities, and predicting attack vectors. This could have been useful in the case of Facebook because there were potentially three software flaws which allowed hackers to break into user’s accounts. If they had done proper assessments, they may have been able to spot or identify the flaws before it led to an attack by implementing an information security program to help with mitigating risks found. It is another principle to involve the board of directors in cyber security management. This could have helped with the hacks by holding the company accountable for their security division, making sure that the company was following strict policies to protect its users and keeping problems away.

There must be a designated individual in Charge of cybersecurity usually a Chief Information Security Officer (CISO), which overlooks security protocol to ensure it is up to standard as well as be held accountable if any incidents take place. The company actually lost their Chief security officer in August to a teaching position at Stanford University, which lead to a reshuffling of their security staff right before the incident (Isaac, 2018). By not quickly appointing a new CISO they may have led to a lack of leadership and accountability to the security division which may have led to an unsecure environment allowing the breach. It is important to maintain an Incident Response Program in the case of an attack which should be tested against at least annually to be sure they have experience with handling any situation that arises without having to improvise. Facebook has now been hacked multiple times in different ways; each have been handled poorly and reported slowly due to lack of preparation and ability to spot breaches. Another principle is to manage cyber security of third party vendors. The breach which took place on Facebook led to the potential of the hackers gaining access to users 3rd party connected apps such as Spotify, Instagram, and more. Because of the ease of transition and login between apps, having Facebook as an acceptable login leaves the user with even more risk if Facebook is hacked because they will then have to worry about their accounts being target on any connected app. The last few principles which should be practiced are conducting routine security training and regularly updating policies, software and hardware. It was noted that the first flaw came from an update in 2017 which had allowed Facebook to easily update videos to people’s accounts. This shows that there was a lack of training and updates in the program as it was over a year since this update took placs and there were no attempts to update the issue which led to a vulnerability in people’s accounts. I think that with the proper training and updating they could have not only removed the flaw tied to tool uploading the birthday video but also stop the bug which allowed attackers to steal access tokens, which are digital keys to gain account access.

Facebook is a massive company and the largest of social media platforms, due to this it is important to note the severity of the attacks that have occurred as well as the lack of disclosure to the public immediately after an attack has occurred. It is an ongoing issue that is being settled to this day with more information coming out all the time. Facebook is such a large company that they should be held to the highest standards in protecting its users.

Facebook has been facing a ton of scrutiny due to many questions about the company’s ethical integrity. One of these issues is related to Facebook’s privacy policies which are intentionally misguiding and confusing, allowing them to gain insight into their users lives. Many of these privacy policies which are accepted and legally binding just by adding and launching a new app and under very extensive terms and conditions that people do not read.

In Facebook’s auto privacy setting it sets all apps, sites, and private information to be shared with your Facebook friends, which you must manually go and turn off. Allowing friends to have access to information may not seem like a problem, but it allows for access by more than just friends without even realizing it. Due to friends’ abilities to gather your information they can share your information to different apps or games they use without first gaining your permission (Lam, 2018). This was one of the main problems which led to the Cambridge Analytica data breach earlier in 2018. The policy had come under scrutiny previously leading to Facebook has stating they told the company to cease gathering information but did not take steps to ensure the company ended information gathering. The next hack which happened later in the year could have been caused due to the loss of security engineers who felt they could no longer morally work for the company and asked for assignments to knew divisions of Facebook such as WhatsApp and Instagram. I believe this helped lead to the hack because they were without a chief security officer during the time and possibly more security engineers which led to the software not being fully protected.

Based on the agreement users are required to accept when using the site, you are giving Facebook free reign to information. This gives Facebook almost no legal obligation for what they gather or share. The company was facing questioning from the courts over the possible interference from Russia to help with swaying the outcome of the presidential election in 2016. The main questions about the interference was aimed at the company’s privacy and ethical guidelines, and whether Facebook should have more restrictions put in place by the government. They are still currently being investigated to whether or not they have broken any customer protection laws.

The impact of this data is said to allow sites, researchers, and Facebook to potentially know more about you than even your friends and family do. It can figure out more information about your habits, interests, thoughts, and ideas purely based on gathering likes and tracking all your activity in Facebook. This is not limited to adults only, there is data being gathered on youth which can lead to improved ads targeting children. The impact of that is that companies are gathering information on children which should be considered ethically wrong. Some of the types of information being gathered by Facebook and its connected apps are: Name, email, gender, birthdate, city, pictures, status and profile updates. All of these can be used to predict things about you including religion, sexual preference, interests, and politics. As you can see the issue with this is that it can specifically be used to help sway events through things like fake news, or propaganda which you may easily persuaded by, potentially changing the outcome of an election (Winston et. Al, 2018). Another issue is the ethics based on what age is it appropriate to begin gathering data on a person, or if it is ethical to gather data at all.

Because of the shared information between apps and using login tokens to verify, the data hack which happened later in the year went almost un-noticed. After the hack happened Facebook was silent, hiding in the background of other political issues going on in the media. They finally revealed that they were hacked again during the Brett Kavanaugh trial, without much attention from the public. The company has since changed some of their policies, making it slightly easier to understand the terms and conditions. Along with this change Facebook has limited the amount of data 3rd party apps can gather on their users to try to reduce the risk of more data breaches. Facebook has stated that they still do not know who was behind the second very large attack which occurred in September 2018, although the FBI and their security team are investigating the attack.

Since the attack which happened in September was based on vulnerabilities that were introduced through a video uploader from July 2017, there is a question of if the IT department was searching out vulnerabilities and fixing them to protect user information. Since the hack Facebook has fixed the potential bug causing the initial vulnerabilities, and reset the access tokens which should help people protect their account. Along with the hack Facebook is unsure of whether the hacker gained access to any linked accounts which have shared logins (dating apps, games, streaming services, etc.).

At this time Facebook is under investigation to decide if they breached European data protection rules, which if found guilty could hit them with fines up to 4% of the company’s global revenue (Whittaker, 2018).

I believe that the company allowing a vulnerability to go unfixed for over a year shows that the company was not following common security best practices to protect customer data. The claim was that they recently lost their Chief Security Officer, along with changes to their security team which they said could have led to the breach being un-noticed. It should be a standard that a company test for vulnerabilities and fix any they find immediately, reducing the risk of any data breaches.

Culturally these breaches Facebook has faced over the last year have led to an increased unsureness about private information security on social networks. It will be hard for a lot of people to trust a company as big as Facebook, who in the last year has given up information of almost 100 million users through multiple breaches. This may lead to people reducing their use of activity online, reducing uploading of information onto the site, and even use different logins for multiple sites and apps.

Overall Facebook could be in a lot of trouble if they are found to have broken the protection laws, but the trust they lost with many of their users could hurt them in other ways as well. This could be the needed push for Facebook to finally get serious about protecting user data and fixing many of the ethical problems that are facing the company.

Facebook has been under constant scrutiny for the multiple data breaches which have been occurring almost regularly over the last few years. The latest data breach has allowed information of over 50 million users to be stolen by an unknown source. The company recently had a hole to fill in their security team when the Chief Security Officer (CSO) left for a teaching job, although that is not an excuse to allow themselves to fall behind on upholding security practices which protect their customers. The first step the company should have done to prevent the hack would have been to hire or promote a new CSO, this would have given the security team a leader to help with holding the team accountable as well as implementation of new cybersecurity practices.

The biggest known issue which lead to the attack was a lingering bug which went un-noticed for almost a year and a half, which was uploading during a live update for video sharing. A bug that causes a huge vulnerability such as this should not have gone un-noticed for as long as it did. The company should begin doing probes immediately finding and fixing any vulnerabilities they find to ensure there are no easy ways to exploit the network. The company is currently sitting on a potential class action lawsuit for not practicing global best practices. This negligence allowed Facebook to be unable to spot the hack or the damages that occurred due to the hack. To fix this problem the company should set up a formal IS Governance which would have put a program in place which allowed Facebook to run risk-based investigation, detect incidents, and respond quickly (Donovan, 2017).

Facebook allows the data of all their members to be gathered, stored, and sold off to ad companies which allows for them to make money. Facebook also uses usage analytics to learn a person’s habits, likes, dislikes, tendencies, and anything else which could be considered useful in the long term. This effectively means that Facebook knows more about you than most of your friends and family. Facebook was in trouble for allowing a data privacy breach to Cambridge Analytica who accessed the data through a quiz app which gathered the data. This breach happened due to Facebook having multiple apps linked to your login including data sharing. Due to the large amount of data being gathered, stored and shared between apps through one login it creates an ethical dilemma of what data is ok to gather, store and share. Another issue that is in question is about the age of which a person should be old enough to have their data collected.

There is a new law recently put in place in 2018 called the General Data Protection Regulation (GDPR) which restricts data gathering and sharing for online companies (Palmer, 2018). This law helps to restrict companies from gathering data on people under the age of 16 years old, who were unprotected before (Onorato, 2018). This law requires that data is gathered legally and required to be protected from exploitation and misuse of anyone gathering it or they will face penalties. All data should be ethically protected no matter how small it is. There should be a better consent to data collection which tells exactly what is being gathered and where it is being used. This should have been added to Facebook earlier to ensure that people were aware of how their data was being collected and used.

One compliance standard that I already mentioned which was relevant was the GDRP. This compliance should have made Facebook change their data collection policy or get better prepared to protect from breaches. The company is now being sued and fined due to breaches the policy standards which were found to not be upheld. This should hurt Facebook’s money enough that they will take future steps to prevent noncompliance.

This incident impacted the global IT community by helping get companies to begin changing their privacy policies including making the consent collection easier to read. The Government stepped in to make Facebook become more accountable to the data they can give out without consent. This helped to get the GDRP into effect within the same year as the breach, making it easier to fine a company for not protecting data. Facebook was still only charged a max fine of $500,000 due to the original Data protection Act of 1998 being in place during the time of the event. This breach also leads to a lack of trust between consumers and large online companies. People tend to believe that their data is safe online because a company is taking precautions to secure it. These more observed and frequent breaches are giving online users more reason to distrust the data that they are allowing a company to collect, and some people are even leaving sites due to their lack of security.

The incident helped to lead to a change in privacy policy laws including the age which a user can have their data collected. Along with age minimum there is a larger restriction on what a company can do with the data they gather and how detailed the companies must be in their consent laws.

Although Facebook has recently been working on changing their data collection and privacy policies it has become public that companies were sharing more data than they had originally disclosed which is now being controlled as well.

Palmer, D. (2018). *What is GDPR? Everything you need to know about the new general data protection regulations | ZDNet*. [online] ZDNet. Available at: https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/ [Accessed 14 Feb. 2019].

Onorato, A. (2018). *GDPR and Children's Data: What Brands Need to Know*. [online] DMNews.com. Available at: https://www.dmnews.com/retail/article/13034540/gdpr-and-childrens-data-what-brands-need-to-know [Accessed 14 Feb. 2019].

Donovan, K. (2017). *10 Cybersecurity Best Practices for IT, IS, Network & Data Security | ObserveIT*. [online] ObserveIT. Available at: https://www.observeit.com/blog/10-best-practices-cyber-security-2017/ [Accessed 14 Feb. 2019].

Patterson, J. (2018). *Is Cybersecurity Dead? What Facebook's Biggest Security Breach Yet Teaches Us About Cybersecurity*. [online] transcosmos. Available at: http://transcosmos.co.uk/blog/is-cybersecurity-dead-facebook-data-breach/ [Accessed 14 Feb. 2019].

Perez, S., Whittaker, Z., Perez, S., & Whittaker, Z. (2018, September 28). Everything you need to know about Facebook's data breach affecting 50M users. Retrieved from https://techcrunch.com/2018/09/28/everything-you-need-to-know-about-facebooks-data-breach-affecting-50m-users/

Winston, J. (2018). *Opinion | Joel Winston: Yes, Facebook has your data. No, you can't sue to get it back*. [online] NBC News. Available at: https://www.nbcnews.com/think/opinion/facebook-data-breach-scandal-our-own-making-legally-there-s-ncna862211 [Accessed 22 Jan. 2019].

Leetaru, K. (2018). *The Problem Isn't Cambridge Analytica: It's Facebook*. [online] Forbes.com. Available at: https://www.forbes.com/sites/kalevleetaru/2018/03/19/the-problem-isnt-cambridge-analytica-its-facebook/#6a5d49dd58a5 [Accessed 22 Jan. 2019].

Feldman, B. (2018). *Hey, Just a Reminder That Facebook Revealed a Huge Data Breach Last Week*. [online] Intelligencer. Available at: http://nymag.com/intelligencer/2018/10/how-facebook-buried-the-biggest-data-breach-in-its-history.html [Accessed 23 Jan. 2019].

Isaac, Mike, and Sheera Frenkel. “Facebook Security Breach Exposes Accounts of 50 Million Users.” *The New York Times*, The New York Times, 28 Sept. 2018, www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html?register=facebook.

“The 8 Principles of Cyber Security Laws.” *LEO Cyber Security*, 25 Sept. 2018, leocybersecurity.com/the-8-principles-of-cyber-security-laws/.