SSN College of Engineering
Department of CSE
Management and Ethical Practices

Vishakan Subramanian
CSE - C
18 5001 196

CASE STUDY ON
CYBER SECURITY ETHICS

Case Study:

1. Consider the well-known data scandal incident that shook the world in 2018 - Cambridge Analytica. According to news reports, personal data of millions of Facebook users were collected without consent by the British consulting firm Cambridge Analytica, which was then supposedly used to influence the 2016 US Elections by means of targeted political advertising.
2. In 2018, upto 50 million Facebook accounts were exposed due to a security breach through a new feature that Facebook had rolled out.
3. In 2021, Facebook & subsidiary apps faced an outage for about 7 hours.

We'll explore these three incidents with respect to some of the concepts highlighted below and analyze what Facebook could have done better to avoid the above issues.

Concepts Covered:

- Controlling Access Flow
- Protecting Privacy
- Dealing with Intrusion
- Managing Distributed Resources
- Encouraging Exploration
- Fostering Responsibilities
- Asserting Ownership and Ethical Framework.

Controlling Access Flow:

According to news reports, millions of users' data were collected by means of a third-party app called "This is Your Digital Life" which had a series of questions to build psychological profiles on users and collected the data of the user's Facebook friends with the OpenGraph API platform provided by Facebook.

Generally, when users authorize an app to use their Facebook account for login purposes, Facebook prompts the user with the details of what user information would be shared to the application. Most users absent-mindedly click OK without even reading through these warnings.

Nevertheless, we cannot claim that it wasn't Facebook's fault that users got misled and manipulated. Facebook should implement more stricter control in providing access to user information and not reveal details that are not pertinent to the application's needs. For instance, here, the digital life application had no reasonable intent to collect data of the user's Facebook friends - it was collected only to target these circles with further ads.

Access control is thus very essential to prevent unethical use of personal information.

Protecting Privacy:

Facebook's founder & CEO Mark Zuckerberg called the situation with Cambridge Analytica as a "mistake" and a "breach of trust". Cambridge Analytica's work was found to have violated several UK privacy laws.

What we can learn from this incident is that, in the modern age, data is a commodity, and needs to be treated with respect and care. Users' privacy needs to be protected. Cambridge Analytica grossly violated users' privacy by collecting their personal Facebook information and their friend circles - and using it to promote targeted ads for a specific political campaign, which in turn might have unduly influenced a whole country's presidential elections.

Facebook, and all other tech giants in general need to protect the privacy of its users by implementing safeguards and allowing only minimalistic permissions & accesses to third-party applications.

Dealing With Intrusion:

In the 2nd incident, upto 50 million Facebook accounts were left exposed due to a new feature that Facebook rolled out to its users. Attackers were able to exploit vulnerabilities to gain control through obtaining the accounts' private access tokens. Mark Zuckerberg's own account was also affected.

While Facebook should've thoroughly checked their feature for weaknesses and vulnerabilities themselves, it's hard to be 100% sure that there won't be any issue at any given time.

Facebook here correctly implemented measures to log out all the affected users off their accounts immediately, thus triggering an expiration of the affected private access tokens.

Time is of the essence in dealing with intrusion - actions need to be taken immediately, otherwise, private data will be lost. Facebook acted with some sense of urgency and were able to fend off any major intrusions to their user base, but from a public standpoint, we do not know the amount of damage done.

Facebook should thus be very careful while rolling out new features - especially ones that can leave a user vulnerable. They need to implement various encryption & digital verification measures to ensure user authenticity and build failsafe mechanisms in case of an intrusion.

Managing Distributed Resources:

Facebook, like most software giants, do not keep all their data in one place - the resources are distributed throughout the world. It is important to keep the data secure while stored in data centers spread across continents and also to keep it secure while in transit.

In the 3rd incident, i.e. the recent Facebook outage, the issue was caused by a bug in an audit tool that Facebook used, resulting in a disconnection between Facebook data centers and the Internet, following which the BGP protocol withdrew Facebook's IP addresses, thus resulting in DNS queries to be responded with a SERVFAIL.

From this incident, we can clearly understand the need for proper system administration apart from security features like authentication & encryption to provide data privacy. The outage was not of malicious nature - it was caused by Facebook's own team. Thus, data centers and CDNs must be well-engineered and properly managed. Even if one data center fails, the others must still be resilient and provide network access to an increased community of people. It must be able to handle varying loads and sudden spikes in consumer usage.

Prior planning is absolutely necessary to manage distributed resources on a global level.

Encouraging Exploration:

Facebook should be encouraged and motivated to perform better with regards to maintaining user privacy. Governments should regulate big tech to control the amount of data that can be collected on its users. The EU has taken a step in the right direction by doubling down on Facebook in relation to anti-trust and privacy violations. Currently, the EU has proposed drafts for the Digital Services Act (DSA) and the Digital Markets Act (DMA) which will regulate big tech, make companies like Facebook to be more transparent, guarantee user safety and hold them accountable for misuse of data. It also fosters competition by making it easier for new platforms to enter the market.

Private services only get better if there is something at stake - Facebook has enjoyed a long period of almost no competition since it has bought out rival companies like WhatsApp, Instagram etc. Their focus has shifted towards profits more than user safety, and thus should be nudged back to the right path.

Government policies, rules and sanctions are one way to ensure that technology evolves in the right direction and to ensure that exploration never stops in using technology to make human lives better.

Fostering Responsibilities:

Facebook needs to be held accountable for mishaps and data breaches that happen on its platform to ensure that they do a good job of protecting users online. They must also be held accountable for the data that they collect from its users, and regulations must be passed to limit the amount of data that can be collected in the name of targeted ad profiling.

Strict standards and guidelines should be laid down such that an agreeable bare minimum is being done by companies like Facebook with regards to collecting data, maintaining transparency and protecting user privacy.

Heavy fines must be imposed in case of misconduct so that these companies stay vigilant and responsible.

Wider awareness amongst the general public is also necessary apart from governmental regulations to push for further change in these online platforms. Most people aren’t even aware of the extent to which they are being profiled by social media for targeted ads.

Asserting Ownership and Ethical Framework:

Utilitarian principles that greenlight decisions if done for “the greater good” must not be practiced in the cyber world, as it might negatively affect even the smallest of communities. With hate speeches, racial comments and heated political battles becoming commonplace in platforms like Facebook and Twitter, they must stop discussions from escalating sourly. While it is necessary to provide the right to Freedom of Speech in these platforms, people must not abuse this right. Social media platforms must impose restrictions on sensitive topics, as they are hotspots for conflict.

Fundamental rights should be written down in the online world - for example, a right to privacy. It should be a duty ethic to always abide by such fundamental rights and should be followed despite the outcome being right or wrong.

Illegal & questionable content must not be allowed on the platform no matter what costs - this also means that users should be held accountable for the content they post online. Social media platforms must take down such content immediately and take legal action.

Despite the fact that they are not the origin source of such content, platforms like Facebook and Twitter must be held responsible for them because their platform is what allowed such content to flow publicly without oversight - which might be the fundamental reason for further conflict.

Their ownership towards the data and users in their platforms must be asserted and reminded from time to time so that they keep updating their algorithms and guidelines to disallow the spread of misinformation, especially with regards to sensitive topics. It is also necessary that free speech is always promoted, and their actions should be kept in check so that they do not externally influence the narrative or flow of information for their own personal gain.