**Eastern Visayas State University**

Tacloban City

**GRADUATE SCHOOL DEPARTMENT**

**Master of Science in Information Technology**

GSMMSIT208 - Security Procedure and Policies

ACTIVITY NO. 1

**Case Study 1: The Yahoo Data Breach (2013–2014)**

*Answers*:

1. Yahoo was affected by the extensive 2013-2014 data breach, as a result of its lack of incident response capabilities, existing security posture, and the total absence of any investment in cybersecurity. The Yahoo security team was reportedly constrained to being defensive because of a lack of executive support, human capital, and financial resources, therefore it was stuck defending against increasingly sophisticated threats. By not recognizing its vulnerabilities, state-sponsored hackers were able to exploit them in order to obtain access to Yahoo's system and remained in and unseen for a number of years. Presumably, hackers were able to utilize user credentials, account recovery information, and internal tools to move laterally throughout the systems. Yahoo's failure to be aware of the ongoing breach for years signifies the absence of effective monitoring detection and response capabilities that are critical to modern-day cybersecurity.
2. The fact that MD5 was used for hashing did amplify the problem because MD5 is a cryptographic algorithm that has been insecure for years and is known to be susceptible to collision attacks and brute-force decryption. Any hacker that got the hashed passwords could easily manipulate the hashes using freely available tools. However, weak passwords would have been especially easy to manipulate since there are many resources where hackers can find those passwords. A much stronger and modern security approach would've been the use of bcrypt, scrypt, or Argon2 for hashing passwords which are password hashing algorithms that also include salting, and computing difficulty, for a greater computational effort outside of just brute force. So if Yahoo used MD5, they made it easy for attackers who bought hacked and stolen hashes to turn those hashes into login credentials, which developed the extent of the breach.
3. The decision to delay for such a long period of time had serious ethical and legal ramifications. From an ethical perspective, Yahoo failed users by not communicating to them in a timely manner, thereby not allowing them the opportunity to take preventative steps (e.g., change passwords or stop using other accounts). From this delay, Yahoo exposed millions of consumers to the risk of identity theft and fraud. Legally, it is highly likely that under current laws, such as GDPR in Europe, or the various states' data breach notice laws in the U.S., it would be a violation to be delayed for that long. For example, GDPR mandates a communication of a breach within 72 hours of when a breach has been discovered. The delay by Yahoo, not only cost it significant reputational harm but also brought regulatory scrutiny, lawsuits, and monetary penalties. It showcased the consequences of failing to comply with changing data protection laws.
4. Upon discovering the breach, Yahoo should have initiated a full incident response plan as soon as possible. This should include isolating affected systems, conducting an incident analysis that includes a forensic investigation and gaining as much information as possible on the breach, and engaging law enforcement and other cyber security professionals. Yahoo should have also immediately contacted affected users to let them know and offer solutions for addressing the breach including recommending users reset their passwords and adopting multi-factor authentications. Had information about what happened been communicated to users in a comprehensible format, it could have built a level of trust, and allowed users to address potential actions that could harm them personally. Yahoo should have also evaluated their security infrastructure, and taken immediate steps to enhance their security posture to prevent subsequent breaches, this included upgrading to better encryption methods and increasing network monitoring activities.
5. A modern Zero Trust Architecture would have significantly reduced the likelihood or impact of the Yahoo breach incident. Zero Trust was premised on the idea that no Users or systems (inside the network or outside the network) gets trusted by default. All users and systems would have gone through strict identity checks and monitoring, and access would have been granted in accordance to the principle of least privilege. Yahoo would have benefited from Zero Trust Architecture, to the effect that if an attacker breached the perimeter, they would have had a much more difficult time moving laterally. Also available tools that provide micro-segmentation, behavioral detections and real-time anomaly detection would have raised alerts early on. Lastly, access to the sensitive user data would have been used and monitored much more closely and would have reduced the ability for large volume attacks to the back-end databases.

**Case Study 2: Facebook–Cambridge Analytica Scandal (2018)**

*Answers*:

1. The Cambridge Analytica scandal was allowed to happen because of Facebook’s poor data-access policies and weak oversight of third-party applications and data-handling practices. Prior to the scandal, Facebook broadly allowed app developers to not only leverage data from friends of users who had authorized the app, but also obtain that information without the friends' knowledge and consent. It was a researcher’s personality-quiz app that did just that. By the app collecting data from about 270,000 users, Cambridge was able to leverage data from the other 87 million users’ profiles. Facebook's policies did not require proper consent or allow for the limitation of information gathering or use of the data collected to legitimate purposes. As well, there were no provisions for auditing or enforcement of policies, which enabled Cambridge Analytica to misuse the data collected as part of political profiling and manipulative action.
2. There is a basic level of ethical obligation for social networking sites to safeguard user privacy, ensure informed consent prior to collecting any personal data, and protect against the abuse/misuse of the "personal" information of users. To comply with ethical responsibility, they cannot place vague disclaimers and expect users to read and agree to how they will use their personal information. Placing the "onus" on users to decide what data to share with companies is not adequate. Protecting users from unauthorized access to their accounts, or the exploitation of their personal information, is also an ethical responsibility of the company. From an ethical standpoint, companies should not treat user data as commodity to be sold for corporate profit, it should be treated as a trust that users have placed in the companies. Social networking sites should be principled and be actively engaged in discovering and prohibiting harmful uses of their sites in cases of user experience involving psychological manipulation, misinformation, or unjust political interference. Furthermore, social media companies have an ethical commitment to disclose their data-sharing collaborations with their partners. They should also be liable for their partners' compliance with the same ethical principles.
3. Facebook’s convoluted data-sharing policies produced a climate in which users were generally uninformed of the ways in which their personal data could be obtained or be accessed. Many users likely did not even perceive that through a friend simply interacting with a third-party app, they could unwittingly disclose their own data and privacy. Facebook provided no sufficiently clear warning of the risk entailed to their data or users’ permission access mechanisms. Further, Facebook’s failure to promptly or transparently disclose the breach worsened the situation, and destroyed public trust by signifying a clear priority for data monetization over user rights and safety.
4. If the General Data Protection Regulation (GDPR) had been in effect at the time of the data breach of Cambridge Analytica, it is likely that Facebook would have faced some serious legal outcomes. GDPR generally mandates explicit and informed consent by users when they collect and share data. It also states that a data controller is held responsible for misuse of that data by a third party. In the case of Cambridge Analytica, Facebook had not adequately gotten proper consent and they failed to make the appropriate measures to protect users data and or notify the authorities within the time period. If Facebook had been covered by GDPR at the time, they would faced staggering amounts of fines given that they violated some serious provisions. GDPR law states fines can be up to 4% of a companies worldwide annual revenue. In Facebook's case, they would have been in the billions during their 2019 revenue from the breach as a potential fine. Further, even at the time, GDPR provided users with a higher level of rights to data access, correction, and erasure then was available at the time.
5. In order to deter similar events from taking place, Facebook and other social media sites should implement a mix of technical measures and policies. Technically, they could limit third-party apps' access to only the data they need for their functionality. They could implement stronger permission models and allow users more granular control on what data they share with app developers. If platforms elected to have regular audits of the APIs to catch misuse early, it would be beneficial. Doing more restriction, vetting, and monitoring of developers accessing their APIs should also help to mitigate abuse. Platforms can create and enforce better data encryption operations and anonymize data obtained from API access, which might reduce the risks during privacy breach if user data is not linked back to individuals. On the policy side, platforms should provide clarity on data-sharing practices, defined flows of user consent, and have a publicly accountable mechanism to verify compliance with data partners. Lastly, platforms should require ongoing privacy impact assessments and verify compliance against international regulations such as GDPR. This aspect of organization should be put at the forefront of the platform's governance structure.

**Case Study 3: Equifax Data Breach (2017)**

*Answers*:

1. Equifax’s biggest blunder in security was failing to address a known vulnerability in Apache Struts (CVE-2017-5638) in a timely manner. While Equifax was aware of the Apache Struts vulnerability due to previous advisories and notifications, Equifax did not identify and remediate the known vulnerability in a timely manner. Thus, the attackers capitalized on the vulnerability to steal personal identification data of more than 147 million individuals. With a good patch management process, the breach may not have happened. A good patch management process includes identifying vulnerabilities in a timely manner, assessing and prioritizing the vulnerabilities, and remediating the high-risk vulnerabilities in a timely manner. Lastly, Equifax did not have good internal communication or accountability with its IT teams, which compounded the problem. Regular vulnerability scanning, good change management, and regular audits go a long way to reduce the risk of exposure.
2. Patch management is important in cybersecurity because unpatched systems are likely to be one of the biggest avenues for cyberattack success. When software vendors release patches for security flaws, they are essentially showing the entry for the attackers. Organizations recognize that they need to patch vulnerabilities but for some reason delay the patching process. If an organization does not apply their patches, they keep the door open for an attacker to access their system. Organizations dealing with vulnerability patching should have an established patch management program that includes automated vulnerability scanning, risk assessment, patch testing, and rapid deployment. Organizations should have policies outlining the expectations for timely patching, in particular for critical patches and the expectations for how quickly they apply patches (usually days or hours of the patch discovery date). The organizations policies will also include working time frames for patches to be applied. Your organization should have a cross-functional team of experts that includes IT, security, and operations to avoid the logs being the end of communication.
3. The Equifax breach quickly became a blend of financial and reputational disaster. Immediately thereafter, Equifax was subject to multiple lawsuits, regulatory investigations, and up to $700 million settlement with the Federal Trade Commission (FTC), Consumer Financial Protection Bureau (CFPB), and states. The breach had financial ramifications. Despite Equifax's allegations against the FTC regarding the impact of its credit monitoring responsibility, there were a range of costs involved, including providing credit monitoring for affected individuals and spending on security improvements. From a reputation perspective, the breach destroyed consumer trust—people could not believe that a company that was entrusted to protect their most sensitive financial information could fail so badly. The breach also ushered a slew of scrutiny from lawmakers and regulators and led to new discussions about the need for better data protection laws in the U.S, and became a moment that could define the conversations about accountability in cybersecurity as well as corporate conduct.
4. Organizations can save time and money in the long run - and ultimately achieve better cybersecurity awareness - if they invest in continuous role-based security training. All levels of staff must understand the basics of practicing proper cybersecurity hygiene, which includes recognizing phishing attempts whether in an email or imbedded in a link, safe browsing and safe downloading, along with the importance of maintaining and updating their systems in a timely manner after any new software updates or bugs are released. Regular drills, workshops, and simulated attacks can conduct in the workplace help make these training exercises stick. Additionally, organizations must foster a culture of security that would allow for mistakes or damages to be reported without any fear of punishment. Leadership must communicate tirelessly not just why security matters but also integrate it into everyday business processes so that awareness and diligence does not become an employee burden but instead becomes part of a pervasive corporate environmental expectation.
5. Had the Equifax hack happened today, given the new regulatory environment with GDPR in place, it could have resulted in catastrophic fines, including a penalty of up to €20 million or 4% of its global annual revenue (whichever is greater) for inadequate security of personal data and not providing timely notification and reporting of the breach. The GDPR requires data breaches to be reported to the appropriate regulators and damaged individuals within. Some of the largest potential penalties would be in cases where a company knowingly failed to protect data, initiating CCPA or other applicable laws. The nature of the breach would have likely resulted in class-action lawsuits and other regulatory actions from both the state and federal level, leading to financial, reputational, or economic damage more severe than its current harm.

**Case Study 4: Uber Data Breach and Cover-Up (2016)**

*Answers*:

1. Uber's breach occurred primarily as a result of inadequate security practices around its cloud infrastructure and associated access control. The hackers were able to access Uber's private GitHub repository and discover credentials for Uber's Amazon Web Services (AWS) account. Armed with those credentials, they accessed substantial amounts of personal data about riders and drivers. Specifically, the breaches in security were lack of access token protection, OCI failings on implementing strong authentication controls including multi-factor authentication (MFA), and failure to have proper scans and monitoring if they have potentially exposed sensitive credentials in their repositories. These flaws represented a fundamental failure of basic cyber hygiene across several domains like credential management, and the principle of least privilege.
2. Uber's unethical business conduct is evident when they decided to pay the hackers $100,000 to remain quiet and delete the data. Uber did not prioritize user and driver safety, but rather their public reputation to buy time in the best interest of the company. Uber has not only encouraged future illegal activity; by engaging with cybercriminals, it is also forfeiting the trust of its stakeholders. Uber should have chosen the ethical option and reported the breach to the appropriate authorities, notified the people affected, and initiated an investigation openly and transparently. Instead, by concealing the breach, Uber forfeited responsibility and failed to be accountable to those who it has a responsibility to; i.e., its users and its employees.
3. Bug bounty programs and responsible disclosure policies are a structured, ethical way for security researchers to report vulnerabilities. These programs will prompt external experts to find and divulge issues before malicious actors apply them. Companies will provide benefits for legitimate vulnerability reporting. By providing these benefits (rewards), companies can leverage white-hat hackers' goodwill to improve their security. In addition, responsible disclosure policies provide clear rules of engagement for the company and the researcher, facilitating a cooperative process to resolve their issues quickly. If Uber had been more proactive about external vulnerability reporting and regularly scanning their repositories for exposed secrets, they may have been able to prevent this breach.
4. Uber faced major legal liability for its cover-up including a $148 million settlement with U.S. states and inquiries from the Federal Trade Commission (FTC). The executives involved in the company’s cover-up faced scrutiny for their personal involvement in concealing the breach. Uber also violated several state data breach notification laws by not disclosing the breach in a timely manner. Organizations should implement breach response processes, maintain ongoing legal advice, and have processes in place that allow for timely discovery and reporting of a breach. Compliance should never be an afterthought, but a core part of organizational risk management and governance.
5. If I was Uber's CISO, and I had just discovered the breach, my first concern would have been to contain the incident as quickly as possible, and to preserve evidence for forensic analysis. I would have notified executive management, legal counsel and, if warranted, appropriate regulatory agencies. I would have soon notified riders and drivers, as applicable, along with overall public disclosures. I would have started an internal review about how we store credentials, our access controls, and third parties. I would have worked on strengthening Uber's security culture by instituting better controls around code repositories, automate secret scanning, and create a bug bounty program. Ultimately, my focus would have been on accountability, transparency and user trust.

Submitted by:

***Joshua P. Casas***

MSIT-Student

Prepared by:

***Sarah Jane L. Cabral, DIT-CAR***

Faculty