INFORMATION SECURITY MANAGEMENT

NEMA AENUGU.

ID: 11611974.

CASE STUDY OF WALGREENS BREACH INCIDENT

A picture containing text, sky, outdoor, road

Description automatically generated

WALGREENS, the widely spread retail pharmaceutical chain in various locations across the United States, has experienced a data breach in the year 2020 compromising the personal data of over 72000 individuals. This incident will be a caution to all of us that when social disruption like this takes place, our data can be compromised not just through cloud but there is an equal chance of break out of our personal data through the documents we leave behind. This incident was worse because there was a data leak a year prior to this i.e. in 2019 which happened through the Walgreens mobile app which lead access to third parties to access the personal information of the users like first name, last name, contact details, addresses etc. Walgreens didn’t inform the customers till about a month but later it aided this through a technical correction to the app and conducted testing to make sure that no such breach can happen in the future after the upgradation in the application or the software. Incidents like this will have tremendous impact on the victims because the medical data is on the higher demand in the dark web black market which sells out for millions of dollars depending upon the wholeness in the data information. The highly possible reflection after such medical data breach is the “INFORMATION EXTORTION**”** where hackers play around with the victims, whose data got exposed out. This is a serious theft because not just the information regarding the bank transactions but also the health records will lead to the fraudulent activities on which hackers are going to roll their dice with the victims on a compensation for the return of the records. The consequences that might one go through after their information got compromised varies from the unusual banking activities like unknown transactions, accessing the credits and debits, securing the loans etc. and using health data would be more threatening because the information is so sensitive when it comes to fact with the dreadful and dangerous health conditions which is handful for the hackers to play their game upon the affected.

This security breach happened one after the other in Walgreens is purely because of the weak servers that are not encrypted properly and the data leaks happened in consecutive years in Walgreens prove that the privacy of the data can be compromised not just through the cloud server attacks but it can also be due to the improper security measures to guard the physical records or the hard disks that are available within the stores. Failure in following the proper strategy of focusing on the potential threats that might occur taking the present and future into concern. In addition to this the constant security alerts given by the multiple security tools in the inbuilt system are often misunderstood by the system maintenance team and the security professionals due to the scale of the data sets and the other vulnerabilities they must deal because of listing out, prioritising, addressing the wrong concerns which will allow the hackers pave their way to access the system. Though the data leak that happened in 2019 was of a limited data of a week span yet the customers suffered viewing of their private information by the other individuals, but the suffered parties had to go through long procedures and monitor their profiles to make sure that their data is not used for the fraudulent activities. This could possibly happen because of the improper security measure, technical software failures and errors to the code provided while developing the application. As we all learnt that the software development and the security management should go hand in hand if not the flaws in the designed systems would lead to such incidents. In organisation like Walgreens which have an approximate count of 4-5 million customers on site and 1.5-2 million customers online everyday using the Walgreen application, shouldn’t fail in having an appropriate security encrypted code while designing and should have an appropriate technical infrastructure in place keeping in mind the size and scale of the organisation.

As we all know that the data breach can happen not just with the cloud servers but also though robbery, the incident happened in 2020 adds weight to this. Theft which led to the robbery is completely because of the improper security practices in the stores due to which the looters were able to access the hard disks and the physical hard copies of records of the patients and the customers with their personal and sensitive health information. Talking about the breach that happened in later months, opting out the theft is a very dangerous move by the hackers because this will not only include accessing the systems during the time of robbery but also, they can put their hands on the valuable and confidential patient information like the historical data stored in the hard disks as well as the printed records. Marilyn Jerominski, a long-time pharmacist technician employed at Walgreens stated in an interview that the employee to the customers/patients ratio, walking into the stores everyday across the United States is very low which puts the safety and security of the patients at risk. This clearly proves that not just the technicality of the servers matters but also the employees to hamper such data breaches will lead to the human errors may or may not be intentional. This proves that employees can highly likely be the reason for the security breaches.

When the incident broke out in 2020 the current mitigation process for the damage happened was executed in accordance with policies laid down by the board of the Walgreens Boot Alliance. Walgreens was collaborated with the Alliance Boots which is a company formed in 2006 by the British based largest pharmaceutical group Boots group and Pan European retail pharmaceutical chain Alliance UniChem. Walgreens was with 55% stake in the Alliance Boot and formed Walgreens Boot Alliance on 31st December 2014 with various committees with guidelines, roles, and responsibilities, having the headquarters grounded on the lands of Deerfield, Illinois. The oversight of the board is being responsible for the policies, procedures, and processes in relation to the risk management and also to ensure the sustainable growth of the business focusing on the resources and the opportunities potentially available by overseeing the risks that might hamper later in the future and ways to mitigate them. In co-ordination to this and to effectively manage the functioning of the system seamlessly they called for an Enterprise Risk Management Program “ERM” led by the Company’s Chief Global Compliance and Ethics officer. The assessment and the management of the risk was taken care by the Audit Committee. There are other committees like The Compensation and Leadership Performance Committee, The Nominating and Governance Committee taking care of the risks and their management by having set policies that must be implemented when needed. Later in the year 2019 Walgreens Boot Alliance and Microsoft Corporation shook hands to offer innovated delivery models in health care, technology, and retail fields. This collaboration solely had its vision in upgrading the existing systems and to upbring the new ideas for the future of the Walgreens. Since they signed an agreement, the Microsoft became the cloud server provider for Walgreens which gave rise to the innovative grounds in not only pharmacy but also to the retail and business services which improves productivity, analytics, and the advanced security systems. Despite all these measures there was yet a space for the security breaches to take place, for which the Walgreens is taking its steps and measures to tighten the security of not just cloud data but also the hard coded records.

Events like security breaches will have strong impacts on the organisations ranging from loss of the sensitive data, facing the legal law suits , financial loss, loss of reputation, downfall in the revenue, decrease in stock value and count, disturbance in the operations, trust break between the customers and the organisation. There are many ways the cyber hackers opt to steal the valuable data and the most common we see is the “RANSOMWARE” and the hardest truth is that organisations under the attack of the ransomware will be paying the ransom to get their data back which in turn is a drawback to the financial statistics of the organisation. This unintended incident will also be an obstacle to the seamless flow of the operations in connection to the organisation because there must be a technical check to see what all systems the hackers accessed for which the operations have to shut for a while. The penalties the organisation must bear will also hamper the huge numbers and they have to proceed legally and pay the regulatory fines imposed in connection to the scale of the damage happened following the set regulations laid under the Data Protection.

In connection to this Walgreens suffered a huge penalty for the breach in 2019 on compromising the patient’s health data including names, contact details, addresses etc. for which legal measures were taken. A lawsuit was filed against Walgreens for not keeping up the word of safeguarding patients’ information and it was charged up to $180,000 because the victims also had to go pay huge amounts to protect their information in short period of time to avoid the fraudulent activities that might happen. This breach also had the break of trust between the active patients and the organisation. The increase in revenue was also in single digits, keeping the revenue graph unchanged. For 2 consecutive years from 2019-2022 the loss rate due to the thefts and data breaches is about to 3.25% which was about to 2% prior. Throwing light on the historical data on annual stocks, there is noticeable differences in the stock prices considering the last 5 years, ranging from 51 dollars in 2019 to 36 dollars in 2021.

There are severe consequences that organisations had to face post security breaches like this, because it creates a hurdle to not just the organisation but also to the customers/patients associated with it. Because as we notice it is not just the organisation who has to bear the loss it is also the victims associated with the incident. The victim parties has to spend huge amounts of money to take control of their information as soon as possible to make sure that their personal information is not subjected to any of the fraudulent and criminal activities possible. Security breaches will turn out to be a headache to the victims because they must keep changing the passwords, monitor their accounts every time. The common yet dangerous fraud we notice after the occurrence of such incidents is the false transactions associated with the individual credit and debit details, which hackers can tap on even from the distinct locations. We can see the hike in the credit bills which keep increasing over the time, if we don’t keep an eye of the transactions happening after the incidents like this and fixing the issue as earliest as possible. The one thing we must be cautious about is opening or responding the messages or mails from unauthorised accounts. This is not just one instance but there are other impacts of the breach on victims including the psychological trauma, hopelessness, helplessness etc.

I opted for the articles available online to study about the breach incidents, cybercrime and the in class PowerPoint presentations to understand the flaws in the organisation which led to the incidents like this. Am attaching the references here below:

REFERENCES:

<https://www.bitdefender.com/blog/hotforsecurity/walgreens-discloses-data-breach-impacting-personal-health-information-of-more-than-72000-customers/>

<https://www.classaction.org/news/class-action-claims-walgreens-data-breach-placed-customers-private-health-info-in-the-hands-of-thieves>

<https://www.bitdefender.com/blog/hotforsecurity/walgreens-discloses-data-breach-impacting-personal-health-information-of-more-than-72000-customers/>

<https://www.securityweek.com/walgreens-discloses-data-breach-related-mobile-app/>

<https://unt.instructure.com/courses/83326/pages/week-4-materials?module_item_id=5003309>

<https://s1.q4cdn.com/343380161/files/doc_downloads/governance_guidelines/Board-Report-on-Oversight-of-Risk-Related-to-Opioids-June-2019-rev.-August-2019.pdf>

<https://news.walgreens.com/press-center/news/walgreens-boots-alliance-and-microsoft-establish-strategic-partnership-to-transform-health-care-delivery.htm>

<https://www.businessinsider.com/walgreens-shrink-rate-50-higher-retail-theft-2022-1>

<https://www.macrotrends.net/stocks/charts/WBA/walgreens/stock-price-history>

<https://paintedbrain.org/blog/the-psychological-impact-on-the-lives-of-cyber-attack-victims>

<https://kybersecure.com/what-are-the-consequences-of-a-data-security-breach/>