AENUGU NEMA

INFORMATION SECURITY MANAGEMENT

THE CASESTUDY OF WALGREENS BREACH INCIDENT

![A picture containing text, outdoor, sign

Description automatically generated]()**WALGREENS** is the second largest American unified Healthcare Pharmacy and Retail Leader serving the millions of Patients and Customers on daily basis was founded in the year 1901 by Charles Rudolph Walgreen who rooted the first store in Chicago under his own name. Later, on December 31, 2014, Walgreens and Switzerland-based Alliance Boots merged to form a new holding company called **WALGREENS BOOTS ALLIANCE,** with total employees more than 325,000 peoplewith the headquarters being in Deerfield, Illinois, United States.

WALGREENS faced a severe data breach in the year 2020 due to which approximately 72000 people got effected according to the Office of Civil Rights (OCR) breach Portal during the tenure of then **CEO, Stefano Pessina.**

According to the notification from OCR and the spokesperson of Walgreens, **Jim Cohn,** during the protests between May 26th and June 5TH , various groups of individuals made a forced entry into multiple Walgreen stores in multiple locations and robbed many items which also included health related information like prescriptions as the number of hard drives that were connected to the cash registers, an automated machine used for printing the prescription labels were also part of the robbery. It was noted that 180 selected locations out of the total locations were looted. Although Walgreens has promised its customers that personal information about the social security numbers and credit/debit card transactions are authenticated, other personal information like Patient Name, Contact Details, Addresses, Prescription Numbers, Insurance plan, Balance Rewards Number etc. are compromised. The loss that Walgreens faced due to this breach was approximately $3.7 billion as it said that this damage was 40% - 50% greater than it was before 2020.

After this incident broke out, Walgreens has taken the steps to prevent such data breaches, like closing out and re-entering the impacted prescriptions and reversing the insurance claims for filled prescriptions and they also claimed to set up the incremental security in the first quarter of the stores.

It is a well-known fact that the data breach is a cybercriminal activity. This includes extracting valuable and sensitive information from the saved data, which will be a great boon to the hackers and the other cyber criminals to make money by replicating the credit/debit cards. Moreover, using the individual’s personal information for framing fraudulent activities like black mailing and apart from all this, as we all know that the information is the new age wealth, this information is sold in large amounts in dark web marketplaces. This will affect the organisation because the victims have all the opportunity to exercise their right to take legal actions against the firm and the lawsuits which are filed on the organisation might lead to the loss of the firm in terms of penalty. The main reason behind such data breaches is not securing the saved data especially by the large retail chains, be it any industry like the Manufacturing industry, Banking Industry, Educational Institutions, Government/Military and Pharmaceutical Industry.

Data breaching from the renewed organisations can be due to various reasons, the primary reason being authentication of the passwords, weak passwords and accidentally sharing of the passwords, will make it easy for the hackers to access the data that is stored. Poorly designed applications are very vulnerable as the flaws in the designed system will give a direct access to the hackers if the application or the software is not updated or maintained on regular basis. Online data and cloud systems which are not configured properly are unsafe and hackers can easily access it. Too many permissions during the software and application installations will also lead to accessing the data in the system. The data breach is also possible due to the loss of the hardware devices which will be counted as human error.

Data Breach won’t just affect the victim-organisation but also the customers associated with it. This will turn out to give rise to conflicts between the employees in the organisation because the person in charge will be accountable and will be answerable to the incident and this will also ultimately affect the revenue because it breaks the trust between the organisation and the customers. The lost data will be handful to the hackers to mint money through various ways. The personal information will lead for the unauthorised purchases and also the customers may become victims of fraudulent invoices. The victims of the data breach in the organisation will have consequences if the breach is not identified at the earliest. As we all know today's world runs mostly on the online data and incidents like the data breach will have an adverse impact on the people associated with it and data breach in connection with the largest retail chain like Walgreens with millions of customers will turn out be a serious issue because the personal data is compromised, and this will lead to fraudulent activities.