|  |
| --- |
| Logo  Description automatically generated |
| WALGREENS BREACH INCIDENT  ASSIGNMENT 3 |
| |  |  |  | | --- | --- | --- | | NEMA AENUGU |  | 11611974 | |

The data breach that happened in Walgreens in the year 2020 will remain as a serious caution to many reputed organisations and will be a potential reminder of the importance of Information Security. The organisations considering the information security as a part of their organisation will have set Information Security Characteristics like Confidentiality, Integrity, Availability, Authentication, Non-Repudiation, Authorisation, Accountability, Anonymity, Privacy, Access Controls, Encryption etc. Security breaches and unwanted incidents in the organisation or in conjunction to the organisation will affect these properties of the information security.

After the outbreak of the breach incident in the year 2020, in a widely spread organisation like the Walgreens, the aspects in connection to the information security have been affected. **The traits of the information security that were affected after the data breach are:**

1. **Confidentiality:** The outbreak of the breach resulted in compromising of the private customer information which includes names, addresses, birthdates, and the social security numbers in return putting the victims at danger of the identity theft and other criminal/malicious activities associated with it.
2. **System Integrity:** Due to the unauthorized access to the client data, the data's quality and completeness was jeopardized, which could lead to false customer records.
3. **Availability:** As a result of this unwanted intrusion, the services offered by the Walgreens were significantly disrupted, which led to unhappy customers, potentially costing the company’s sales.
4. **Authentication:** Because of the unauthorised access to the client data was hampered because of the data breach, it allowed the malicious actors to impersonate the real customers.
5. **Non-Repudiation:** Since the customer data was accessed without the proper authentication and the authorisation as the result of the breach, it was difficult to demonstrate the legitimacy of the customer transactions.
6. **Access Controls:** Due to the inappropriate and inadequate measures undertaken by the Walgreens organisation, the sensitive and the private information of the customers was exposed to the unauthorized users.
7. **Encryption:** As the Walgreens failed to encrypt the data it saved, it was open to intrusion.

The components that include the information security is a three-tier comprising **Computer Security, Data Security and the Network Security** popularly known as the C.I.A triad which means the Confidentiality, Integrity and Availability of the data and the services. There are various measures like Access Controls, Control/Safeguard/Counter Measure, Data Encryptions, Employee Education, training and Awareness, Network Segmentation etc. that can be opted to avoid the data/security breaches which has to be implemented and practiced within the organisations. The impact on the Walgreens Organisation after the breach was not only in monetary aspects but also in terms of the trust between the organisation and the customers. Walgreens must have taken the preventive measures to avoid the breach and the potential loss hampered with it. Following are the few Information Security Measures that Walgreens could have implemented to prevent the breach.

1. **Physical Security:** The physical security measures include the protection of the physical assets of the data. The physical security measures including:

* **Installation of the security cameras** in all possible entries and exits in the stores.
* **Installation of the alarm systems** with the sensors and the motion detectors which sends alerts to the officials if any suspicious activity takes place.
* **Hire security Guards:** Hiring the number of security guards to regularly patrol the stores which will assist dissuading thieves from trying to break in.

1. **Multi-Factor Authentication:** This makes sure that only the authorised users have access to the data which prevents the malicious actors to access the data and put their hands on the sensitive and private information of the customers. This cannot be achieved only using strong passwords, there must be other practices like the biometric information, voice recognition etc. in addition to the passwords.
2. **Network Segmentation:** This mechanism will assist in segregating the important network components and monitoring the resource access which ultimately helps in minimizing the effects of the breach and reduce the exposure of data leading it to the fraudulent activities.
3. **Firewall:** Installing a firewall can assist in guarding the network of the company against any such data breaches from outsiders.
4. **Consistent security audits:** This practice will allow the organisation to find and fix the vulnerabilities that could be exploited.
5. **Employee education, training, and awareness:** This focuses on the standards, policies and guidelines of the respective organisation that are related to the security of the sensitive information of the organisation and the customers associated with it. This involves the training the employees to identify the potential threats like the viruses, malware etc and guarding their systems against such attacks.

In any organisation, all the parties of interest i.e., **the Management, the Customers, the Stakeholders** are in charge for extending their resources, assistance, and support to help the organisation accomplish its goals and objectives. Each of the three parties will have their roles and responsibilities that must be discharged efficiently for the future of the organisation.

**The objectives and roles of three parties of interest in association with any organisation**

|  |  |  |
| --- | --- | --- |
| **Management** | **Customers** | **Stakeholders** |
| Creating Vision and Mission | Provide Feedbacks | Profit Maximization |
| Establishing Goals | Provide Insights | Help in improving Customer satisfaction. |
| Planning | Establish Loyalty | Enhancing brand image |
| Organising | Promote the Brand | Adopting innovative technologies |
| Communication | Value for Money | Increase Efficiency |
| Risk Management | Trust and Transparency | Increase Market Share |

Talking about the breach that happened in Walgreens, the three parties of interest share equal responsibility for the breach to take place by not paying attention on the importance of the information security and consequences associated without it, if not addressed properly. Let’s discuss how the individual parties failed to function.

1. **Management:** Walgreens faced the security breach in the year 2020 where the individual groups of people broke out into multiple Walgreen stores spread across the United States which resulting in compromising the private and the sensitive information of approximately 72K individuals. In connection with the incident, it’s important to understand that it’s not just the practices and procedures we follow in securing the data technically meaning the software or the internal systems, it’s also the physical and the external factors or elements of the organisation like the entries and exits to the stores, security guards, security systems and the alert systems that detect the suspicious activities within the stores that has to be hampered, that would have avoided the occurrence of the breach. In addition to this, employees failed to adhere to the security practices and the protocols which can be counted as the fundamental duty on their part to safeguard and secure the data in connection to the organisation and the customers which contains the confidential and sensitive information. Some of the security measures that have to be quoted includes, using firewalls, changing of the passwords on regular basis, following multiple-factor authentication, failure in the encryption of the data etc.
2. **Customers:** In relation to the breach that broke out in Walgreens, the customers didn’t contribute directly to the breach. They did share their personal information with the organisation as the part of the protocol within the organisation, it’s the organisation who must follow the appropriate security protocols to safeguard the customers private and sensitive information. But talking about the breach that occurred couple of months prior to May 2020 where the Walgreens online application suffered the massive breach compromising the number of customers personal data. In connection to this the customers didn’t follow or adhere to the efficient security practices like using the two-factor authentication, strong passwords and they weren’t cautious of the phishing attacks, fraudulent links that might divulge the personal information if the data is not secured properly.
3. **Stakeholders:** The absence of the efficient communication between the organisation and its stakeholders is also one of the factors that may be the reason of the breach to occur because lack of proper communication results in the lack of awareness of the risks and potential damage that might happen if the security measures are not followed properly when such massive data breaches breaks out. Throwing light on the consecutive breaches in Walgreens one being the cloud attack on the Walgreens application and second being the attack on the Walgreen stores spread across the United States, states that the first stakeholder that contributed to the breach is Walgreens itself as a whole, because it failed by not securing the software systems but also the physical elements in connection to the stores.

This gives us the clear understanding that the three parties of interest should have the proper co-operation and communication and should discharge their individual roles and responsibilities efficiently for the future of any organisation.

For any organisation, the business and the security requirements must be harmonised to achieve the goals and maximize the revenue. The commercial or the business requirements should be put forth and they have to be guarded by the security strategies and protocols. One has to keep in mind that the security of data or the systems is not the final end result but it is the process and it has to be evolved as the business flourishes. It has be examined regularly and modified accordingly keeping in mind the business demands and requirements. The organisation’s ability to discharge its duties and offer services should not be hindered with the security practices of the respective organisation but it must be done hand in hand in effective and the cost-efficient way.

As Walgreens is a biggest pharmaceutical chain spread across the different locations in the United States, there were many times where the business and the security needs / requirements collided. As Walgreens is a significant company interacting with millions of customers on daily basis through both offline and online medium, and operating highly competitive retail chain often handles the private, confidential, sensitive information of the customers and the organisation and it is also subjected to various policies and regulations conjunction to the health, safety and security. It is indeed necessary to follow the security protocols to safeguard the large data and information while keeping in mind and attempting to meet the increasing customer expectations. So, it is very important on Walgreens part to strike the balance between the Business and the Security needs. But keeping in mind about the complexity of the retail chain business of such huge organisations like Walgreens it is not unusual for a conflict to arise between the business and the security needs and requirements keeping in mind the efficient and convenient manner of allowing the customers to make purchases and access the services.

In my opinion, Walgreens would want to invest more on the security measures after the back to back security breaches in the consecutive years 2019 and 2020, to safeguard the data and the information but if it focuses on the security protocols, it might restrict itself and limit its capacity in delivering the innovative services as on the basis of the security grounds. Instead, it should focus more on investing on the secure technologies that would help the organisation’s bottom line which can put the security concerns at odds with the business needs and requirements.

The other possible factor that may lead to area of friction between the business and the security needs is the decision Walgreens has to take in choosing the amount of the confidential and the sensitive customer and the organisational data that it has to store and for how long it has to store. Because keeping the business in mind and the decisions that has to be made for the future of the Organisation, Walgreens might want to keep the track on the historical data. But this is contrary to the security grounds, adhering to the data privacy policy. Hence this would give rise to the potential conflict between the business and the security requirements.

There are many policies laid in connection to the security and specific to the organisation like the Access Control Policy, Data Protection Policy, Issue Specific Security Policy, Enterprise Information Security Policy, Systems Specific Security Policy, Physical Security Policy etc.. These policies will allow the organisation to prevent the security breaches to occur. Let’s see how few of these policies would have prevented the occurrence of the Walgreens security breaches.

**Issue Specific Security Policy:** Issue Specific Security Policy is a document with specific instructions and the guidelines, designed to safeguard the organisation’s data and systems from the unauthorised access and malicious use. The following are the ways describing how the Issue Specific Security Policy could prevent the breach.

1. **Limiting access to the Confidential data:** The access to Sensitive and the Private data should be limited only to the employees confined to the specific job role by making sure that only authorised users can access the data and login to the system having in place the authorisation, authentication to the system.
2. **Updating the software and hardware:** Making sure that the most sophisticated security systems are in place and the updates must be done regularly.
3. **Systems and Network Security:** Encryption of systems and network must be done to make sure that both of them are safe and secure following the security tests and monitoring.
4. **Employee Education:** Walgreens must have focused more on the Employee Education, Training and Awareness regarding the need of Information Security and would have conducted the regular audits to find out the potential weakness.

**Enterprise Information Security Policy:** It is a set of rules and regulations, that aid in avoiding the illegal and unauthorised access to use, dispose, modify the organisation’s digital assets like the data and the systems. It specifies the authorised use of the networks, software, E-mails guaranteeing the CIA triad. In addition to this it also specifies the roles, duties, and the methods, addressing the system vulnerabilities.

As the Enterprise Information Security Policy is a comprehensive framework for the Organisation’s Security Architecture, the breach would have not been occurred if the security policy was in place. It would have included the incident response plan and the strong encryptions etc. In addition to these, instructions on how to identify the potential dangers to the organisation, methods to be followed if the incident occurred ,methods to safeguard the customers sensitive data, steps to ensure that the network and the IT systems used by the Walgreens were continually updated and monitored should also made part of the policy in order to stop the breach that broke out in the year 2020.

**Systems Specific Security Policy:** Systems specific security policy includes rules, instructions that are created to safeguard the Confidentiality, Integrity and Availability of the organisation’s system. It describes the precautions that have to be taken by the person in charge of maintaining the security of the systems to protect the data and safeguard the systems when the breach occurs. This policy includes guidelines for the user account management, patch management, malware protection and will also outline the obligations of users, system administrators, and the IT department with regard to upholding system security.

The breach that broke out in Walgreens would have prevented if the policy was implemented effectively, ensuring that the compromised data was encrypted properly and stored in the secure system. The upgradation of the policy should have been made mandatory, creating the multiple layers of the security for the customer data. This check and upgradation, if was in place, would have identified the potential vulnerabilities to the data and the system where the data is being stored and could lay the guidelines to be followed in order to avoid the attack. The policy would have compelled to implement the Incident Response Plan thoroughly, implementing the regular patching, giving the business the ability to respond to the breach promptly and effectively if it occurred to minimize the harm bought on by the attack.

In spite of having in place, all the security strategies, if the breach occurs then the breach have to be addressed effectively following the appropriate incident responses. Following are the few incident responses have to put in plan of action soon after the breach occurred.

1. **Notify the Appropriate Authorities:** Informing the proper authorities is the first step of response to the breach. This involves the state regulators, local law enforcement, federal law enforcement and few other external entities depending upon the nature and scope of the breach.
2. **Establish the Security Incident Response Strategy:** Walgreens must have the incident response plan in place to respond to the breach swiftly and effectively. The active, practical procedures and practices has to be followed to stop the breach and it’s occurrence in the future, including strategies , roles and responsibilities of the key stakeholders.
3. **Investigate the breach:** After notifying the proper authorities, Walgreens should launch an internal investigation, to determine the causes of the breach and the impact of it. All the security systems, policies and the practices should be thoroughly examined to find out the flaws that might contributed to the breach incident.
4. **Isolate the Affected Systems:** To stop the further damage, all the affected systems should be cut off from the networks. This entails turning off or disconnecting any wireless networks, such as Wi-Fi, as well as turning off PCs or servers.
5. **Change the access codes and the passwords:** Update the passwords and the authentication credentials including the employee accounts, customer user accounts and the databases on which attackers may keep their hands on.
6. **Adapt the Data Loss Prevention measures:** To stop the further breaches, Walgreens must launch the data loss prevention measures and the practices. This incorporates safe-guards like the data encryption, two-factor authentication and tracking all the suspicious activities.
7. **Notifying the affected customers:** It’s important on the organisation’s part to inform the victims of the breach. This can be done through E-mails, text messages etc. and the organisation should also guide them to take the necessary steps to protect their data from being used for the fraudulent activities by giving them the information about the customer service and the privacy teams.

If I was asked to design the security framework for the largest pharmaceutical chain like the Walgreens, I would create an information security strategy using the NIST Cybersecurity framework (CSF). The NIST CSF is a thorough framework offering the firm pointers explaining how to secure the computer systems and the data against the cyber-attacks and the online dangers.

This framework offers the methodical and the standard procedure for organising and establishing the security policies in action that the organisation can use recognise, evaluate, and govern their cyber threats. The five focal points or the core objectives of this framework includes:

1. **Identify:** Identify and document confidential data, develop the rules, strategies, and procedures to make sure of their privacy and security.
2. **Detect:** Maintain surveillance on the systems to track down the suspicious activities.
3. **Protect:** Prevent the unwanted access to the systems allowing the modifications in the data by using secure data storage and other security measures.
4. **Respond:** Act promptly in the event of the security breach, investigate and fix the issues.
5. **Recover:** Creating a plan for the swift recovery from the from the security breach incidents including the data and the system restoration.

It also offers advice to the organisation on how the business should create a risk-based environment in the organisation to control their cyber security posture in addition to the tools and resources they require to successfully monitor and respond to the cyber-attacks. This is an ideal approach to the organisation to rely on because it offers a thorough risk-based approach to the cyber security that can be tailored, customised and modified in accordance to the needs of the organisation.

To protect and support the organisation in implementing and maintaining the framework, NIST CSF also additionally provides variety of resources like the implementation manuals, case studies, best practices, training, and certification programs that are intended to assist organisations in strengthening their security grounds. Throwing light on these aspects I feel that the NIST Cyber Security framework is a firm base for any organisation, and I will design the framework based on this as it is efficient and thorough structured and is widely used across sectors and offers the required direction to support Walgreens in safeguarding their information assets.

**REFERENCES**

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

<https://www.securitymagazine.com/articles/98325-the-impact-of-a-data-breach>

<https://www.citizensjournal.us/walgreens-security-breach-leaked-millions-of-patients-covid-test-data-to-hackers-including-your-birthday-and-home-address/>

<https://cyberthreatportal.com/types-of-data-security-measures/>

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

<https://unt.instructure.com/courses/83326/pages/week-5-materials?module_item_id=4957738>

<https://unt.instructure.com/courses/83326/pages/week6-materials?module_item_id=5003423>

<https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework>

<https://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide>

<https://www.csoonline.com/article/3513899/what-is-information-security-definition-principles-and-jobs.html>

<https://dotsecurity.com/insights/blog-what-are-the-components-information-security>

<https://chat-gpt.org/>