THE CASE STUDY OF WALGREENS BREACH INCIDENT



ASSIGNMENT - 4

NAME: NEMA AENUGU.

STUDENT ID: 11611974.

**INFORMATION SECURITY MANAGEMENT- IMPORTANCE AND IMPLEMENTATION.**

In the past decade, Walgreens encountered severe security breaches, the breaches that broke out in the year 2017 and 2020 will be the incidents to be remembered because of the potential loss that left behind after its outbreak. It has to be noted that the security breaches in Walgreens is observed year after year since 2015 which calls for implementing more intense, challenging and resilient security processes, procedures and protocols to bring down the possible consequences like the Illegal access to the computer systems, financial losses, loss of trust and Loyalty, legal liabilities, regulatory fines and penalties, loss of the confidential data , Malicious Software attacks, data breaches etc. These ramifications must be addressed with the potential strategies to shut them off and avert the greater risks.

Following are the four important potential consequences and the actions that must be taken against them.

**1.Loss of Confidential Data:** When the sensitive or the private information goes public, stolen or otherwise made accessible to unauthorized individuals or entities, then it is referred as a loss of the confidential data. This includes customer records, bank records, trade secrets etc. The theft of the confidential data can have the devastating effects on an organisation ranging from monetary damages to brand assault. As a result, policies, procedures, and strategies must be in place to ensure that the data kept safe such that any illegal access will be reported appropriately and remedied.

**Potential Action Plan includes:**

**a)** Generate an elaborate information safety and security policy that details out who has access to private information, where and how it should be stored, and the repercussions for policy violations.

**b)** Monitor and verify the user to access the private information on regular basis to verify that only those with the authorization have permissions to access the data.

**c)** Use robust safety precautions, such as data encryption, biometric information, and two-factor authentication, to prevent unwanted access to confidential data.

**d)** Educate staff about the necessity of sensitive data protection and the detrimental effects of violating it.

**2. Illegal access to the computer systems:** Illegal access to the computer systems is an alarming issue that has surged in prominence in the digital era. This sort of act which is also known as hacking, and it marks its roots when someone gains unauthorised access to a computer system containing the data assets. In many countries, acts like these, are illegal and they end up in serious punishments such as fines and the imprisonment, if caught. Immaterial what might the reason could be for the outbreak of it, the people associated with the incident be it the organisation and the customers in conjunction with, find themselves spending the enormous amounts of money and time to remediate the damage. There are several tactics that ought to be implemented to forbid the unauthorised intrusion into the computer system.

**Potential Action Plan includes:**

**a)** Using robust authentication techniques like the two-factor authentication for guaranteeing that only those with the proper authorisation will have access to the computer system.

**b)** Firewalls, intrusion detecting systems, antivirus software will all help in securing the computer systems from being accessed illegally as these will monitor the network interactions against the unusual patterns and activities, will notify administrators of the upcoming dangers and threats.

**c)** Using the screened subnet firewall architecture (with DMZ) will regulate the network traffic and can prevent malicious traffic from traversing the system.

**d)** Encrypting the confidential data so that only an authorised person holding the decryption key can decode it.

**3. Malicious Software attacks:** This is commonly referred to as malware. This involves use of illicit code or the software to disrupt the computer system. This malware can be propagated by emails, portable devices, portals, web pages, peer-to-peer network which mainly disrupts the flow of the operations and steals the confidential information and jeopardize system. Malware may additionally be employed to deploy distributed denial of service (DDoS) assaults, which can overload and damage the system.

**Potential Action Plan includes:**

**a)** Ensure that all network applications and software are kept latest with the most contemporary security patches and upgrades. This will assist in hindering malicious malware from violating any software vulnerabilities.

**b)** Monitoring network traffic on regular intervals can aid in the detection of any suspicious or malicious activities. Any inappropriate activities can then be thoroughly investigated, and necessary actions can be taken against.

**c)** A VPN (Virtual Private Network) is an encrypted means to connect to networks. It can be utilized to safeguard data communicated over the internet by encrypting it and limiting access to authorized users.

**d)** Firewalls are critical for guarding against malicious software attacks. They can be used to manage the flow of traffic in and out as well as to prevent dangerous malware from accessing the network.

**e)** Antivirus software should be installed on all computers and devices linked to the network. It should be maintained on a regular basis for defence against the most prevalent dangerous software threats.

To effectively avoid harmful software attacks, it is critical that all employees are informed of the potential risks connected with surfing the web as well as the sorts of dangerous software that may be endured. This can be accomplished by holding frequent training sessions and giving personnel with current expertise on the most recent dangers and strategies.

**4. Data Breaches:** Data breaches are becoming more widespread in the modern era. With the advancing state of technology, knowledge is more readily available than ever before. Tragically, this also means that a likelihood of data breaches is ever-present, with devastating repercussions for individuals, corporations. This occurs when a person or organisation publishes sensitive information without authorisation, either intentionally or unintentionally. Sometimes data breach can be the result of hostile actors, such as intruders, hackers, or can be the result of an incident, in a way as a breach of information is triggered by an external service provider. As an instance, an organisation may be unaware that an employee is storing client data on an external service, so this service may end up exposing the customer data.

**Potential Action Plan includes:**

**a)** Notify customers as soon as feasible after reporting the breach to the appropriate authorities.

**b)** Establish a team to respond with experts from IT, the legal profession, and public relations including the implementation of the effective incident response plan outlining the potential incident strategies to manage any data breaches.

**c)** An organisation can be shielded from the expenses of data breaches by purchasing cyber insurance. Costs involving attorney's fees, forensic analysis, and consumer notifications may be covered with the aid of cyber insurance.

**d)** A reliable backup system should be in place so you can restore any lost data if it transpires.

**e)** Creating a secure network will assist in lowering the possibility of data breaches. Firewalls, lists of access controls, and intrusion detection systems are all capable of execution.

Despite of all the precautionary measures in action and the security protocol being in place, if a breach outbreak occurs in an organisation, it must be addressed carefully and effectively. This can be done through the contingency planning which enables any organisation to be prepared for any possible potential risks and disruptions that might occur in the future and counterattack them. This typically involves first assessing the circumstance thoroughly, taking into consideration all pertinent variables and finding any feasible remedies or risk-mitigation measures making sure of the steps, taken promptly, immediately and efficiently. This contingency planning enables the organisation to carry out frequent evaluations and changes to make sure the plan continues to be applicable, practical, and productive. Because the contingency planning is the hands-on document that allows the organisation to start the action plan soon after the outbreak of the breach. Following are the steps that are involved in the contingency planning.

**A. Identifying the possible threats:** The initial step in the process of contingency planning is to recognize possible risks that might have an impact on organisation’s operations. Pandemics, recessions, catastrophic events, and cyberattacks are a few examples of risks.

**B. Assess Risks:** Following the identification of potential threats, you must evaluate the risks connected to each one. This involves determining the threat's propensity to materialize as well as any possible effects it might have on your company.

**C. Draft a Plan:** The third stage is to create a plan to deal with each identified risk and evaluated. Both risk-mitigation measures and steps should be included in this strategy.

**D. Implement the Plan:** After the Plan is completely developed, it must be put into action and tested. This include educating personnel including not just the supervisors and employees but also the customers and vendors about the plan, setting up procedures and protocols, and making sure the required tools are available to address the threat.

**E. Monitor and Evaluate:** Monitoring and assessing the plan is the last phase in the contingency planning process. This involves assessing the strategy frequently and making the required modifications. To make sure the plan is effective, data collection and regular testing are also required.

Having such firm contingency plan in place, will allow effective execution of the action plan in response to the outbreak of the breach. Realistic and viable goals are essential for a reliable action plan. It should be precise and thorough enough to serve as direction while remaining adaptable enough to sink in unanticipated scenarios. The plan should have checkpoints and success criteria that allow you to gauge your progress.

**1. Assemble the Evidence:** The initial step is putting in together all the relevant data in conjunction to the breach. The nature of an incident, the date and time of the occurrence, the systems that were impacted, and the likely origins and effects of the breach are all included in this. In the case of the Walgreens as the breach is occurred due to the force intrusion of the individual groups into multiple Walgreens stores, the entries and the exits to the stores should also be examined carefully.

**2. Examine the Effects:** After the preliminary information is acquired, the impact of the incident is evaluated. This entails figuring out the extent of the incident, the severity of its impact, and any anticipated expenditures in connection to the breach. In connection to the Walgreens breach incident as it hampered the looting of the confidential data stored in the hard discs, it is quite essential to outline the cons associated with it. This is crucial because after the breach the damage is so severe that the decisions must be taken on closing a few stores completely to undertake the repairing and fixing of not just the physical stores but also shutting down the operations of the entire organisation.

**3. Determine the Source:** The subsequent step is to determine the cause of the breach after evaluating the incident's impact. Examining the affected systems, logs, and network activity can assist to accomplish this. Doing so will allow Walgreens determining itself on underlaying reasons.

**4. Evaluate the Vulnerabilities:** Next to the identification of the incident's origin, is the following step is to examine the flaws, imperfections, limitations that led to the breach. This outlines, examining the configurations of the impacted systems to find any flaws or errors that might have been potentially attacked. Throwing light on the cause of the outbreak of the incident it is observed that the moto is different than that of the usual, it is not intervening with the confidential data. The breach incident happened in response to following the Minneapolis police shooting death of George Floyd, unarmed black man. This serves an emphasis to Walgreens that security considerations like the entries and exits to the stores, CC cameras, alarming systems, security guards, must be given equal attention unlike the software systems.

**5. Execute the Remedial Action:** The final phase is to fix the problem after studying the flaws in the system. This involves:

**a. Notifying the victims of the breach.**

**b. Alert the Regulatory authorities.**

**c. Update the security measures and procedures.**

**d. Monitor the incident continuously.**

**e. Address legal potential consequences.**

This line of action resonated to me because it is precise, practical, and proactive. It enables a detailed examination of the problem and the creation of a strategy that is customized to the unique set of circumstances guaranteeing that the breach is promptly controlled, investigated, and remedied. This course of action also validates that Walgreens is taking necessary precautions to secure the data which is confined to the organisation and the sensitive private data of the customers associated with the Walgreens. Additionally, it guarantees that all parties are informed of the strategy and that any unexpected events can be immediately dealt with.

**WHAT HAVE I LEARNED?**

As I am an Undergraduate Architecture student, I’ve always enjoyed studying about science behind the planning, designing, and developing the structures. Late in time, during the final semesters of my graduation I’ve additionally nurtured a growing curiosity in the field of Technology. Then with lot of research and in depth understanding of the coursework, I considered to switch to the Information Systems and Technology as it would be advantageous to my career. I enrolled myself into various courses laid down in the framework and Information Security Management was part of my second semester of master’s in information systems and technology.

My experience in this course has been quite instructive. I see myself having thorough understanding on the importance of safeguarding data and information from the outside threats and dangers, learning about the various security approaches, practices, and measures that must be considered to prevent the unauthorised individuals from accessing the confidential information and the data. I now have the better grasp of many security policies that can be followed to guarantee the protection of the data assets, by recognising the potential risks and how to react to them timely and appropriately.

I recognise myself to learn developing and implementing security strategies which is ought to be a crucial skill of any organisation. I gained the fundamental knowledge of the cryptography which is a vital part of information security management and the understanding of the many authentication systems that can be employed and that must be in place to ensure the security of the private data. When my professor shared her professional work life experiences, I also understood how essential and crucial the personal security is, when working with the data. This was helpful in making me more conscious of the possible potential risks associated when using the data and working on it.

This course enabled me to have better understanding and awareness of how critical it is to accept the accountability for the choices that I make and the results of it in response to the choices, making me more cognizant of the significance of incorporating the precautionary steps to safeguard the data and the information. Furthermore, I now gave a greater overview of various rules, regulations and laws that must put in place to safeguard the data and ensure that it is employed appropriately and am acutely mindful of how vital it is to abide by these rules, laws and regulations and how doing so could have dire repercussions.

As a part of the course, I’ve learnt the numerous hazards, attacks, threats that exist and the ways to identify and react to them. This allowed me to understand the need of the effective incident response plan in place that details what should be entitled in case of an assault or the breach. This made me realise the importance of how crucial it is to keep up with the sophisticated security trends and technologies to tackle the risks. I’ve begun to comprehend the need of testing and auditing systems to make sure that they are reliable and secure. Additionally, I gained insight into the value of having a workforce that is educated, well trained, and skilled in guarding, defending the information and data of an organisation.

The assignments created by the professor were very practical as we got the opportunity to pick our own organisation to work on the assignments that are related to the information security management. The organisation I chose was Walgreens. This was the valuable opportunity for me to learn closely about the significance of the information security, effects of the data breach and how to avoid similar occurrences in the future. The framework of assignments is so in a way that, if I am exposed to the real time situations in the coming days of my career, I can be more acquainted with the measures required to protect the sensitive data by analysing the incident, as the assignments included the step wise process of addressing the security breach. I’ve had the exposure on the lawsuits which are the formal legal procedures in which a person or the organisation calls on other party which could be a government or the business agency to provide the financial or any other remedy for the losses, damage incurred because of their carelessness or illicit behaviour. I also presumed the significant role it plays in directing the focus on the information security incidents like the one encountered by Walgreens.

As the part of this course, I now have a better understanding of key concepts like the Risk assessment, Risk Management, Business Continuity plan. The risk assessment and the risk management are quiet useful lessons for me as a learner because it aids me in identifying, managing, and evaluating the potential risks connecting specific activities, circumstances. It necessitates considering the sort of danger, its extent, magnitude, and the likelihood that it will materialise. This taught me that to deal with the risk that has been recognised, a plan must be established, considering decisions on risk reduction, risk management and risk monitoring, all being the part of the process. In conjunction to this another firm concept in conjunction to any organisation is the Business Continuity Planning. I’ve the better understanding on how the organisation can resume its operations and functions after being hit by the security breaches. The concept of business continuity planning helped me to do so. From my learning experience I understood how crucial it is to create a thorough disaster recovery plan and the execution of the steps necessary to put into action. This Business Continuity plan will also outline how the organisation should communicate the plan with clients, employees, stakeholders to guard its facilities, systems and the data that must be backed up to recover from the disaster. This enabled me to realise that risk assessment, risk management and the business continuity planning will give the organisations a thorough understanding of how to better foresee and handle threats. I grasped the knowledge on how to recognise, evaluate and create plans to lessen, eliminate the risks and operate the systems swiftly in the event of an emergency through this process.

In conjunction to the above concepts another powerful concept is the security auditing. This allows me to fetch skills to find the potential security risks and vulnerabilities in the operation of the systems. This entails evaluating a security posture and locating any potential vulnerabilities that might be used by the hackers. This allows the organisation to confirm that an organisation’s security procedures, protocols are sufficient to conflict with the risks, and it points out perspective areas that needs to be improved to boost the overall security of the organisation. This also signified me to become familiar with different rules and regulations that govern the security of the information and data as well as the consequences of violating them, ensuring the organisation to guarantee that this is being managed appropriately by learning about these standards. All these concepts strengthened my ability to ace my skills and created a sense of the responsibility of being cautious about the data I give or take.

**WHAT HAVE I LEARNED ABOUT WALGREENS?**

The case study on Walgreens breach incident is an excellent illustration of the significance of information security management in the modern world. As we all know that Walgreens, one of the biggest pharmaceutical chains spread across the states of the United States, was stood to be prey for hackers starting from 2018-2021 as it was hampered with the data and the security breaches with multiple factors and reasons. This demonstrates how simple it is for the hackers to obtain the private, sensitive and the confidential information and how essential information security is. This occurrence of the breaches reminds us how vulnerable the data is and how greater safety protocols need to be implemented, highlighting the consequences if the requisite defences aren’t in place. This severs as warning to be watchful when it comes to the security implied not just to the software and the operating systems but also to the physical infrastructure of the organisation.

In conjunction the breaches the Walgreens was exposed to, hackers got access to the business networks, online website of Walgreens, physically looted multiple Walgreen stores, and did steal the sensitive client data including the medical records, financial records. To recoup the losses and demand compensations from the individuals who robbed off the stores, Walgreens filed many lawsuits and to stop future thefts, the Walgreens Organisation also requested a restraining order. This incident in 2020 had its weight raised because it suffered a severe data breach in the year 2019, where the online application of Walgreens was exposed to the data breach compromising the personal data of more than 80K individuals including the names, addresses and date of births. In conjunction to this incident, by the announcement made by the Federal State Commission, Walgreens reportedly broke the Gramm-Leach-Bliley Act (GLBA) and FTC Act. In compliance with the settlement terms, Walgreens was forced to pay $700,000 civil penalty and started employing sophisticated and robust information security programs and protocols to secure and safeguard the sensitive customer information and data it gathers. This incident is meant to serve as a strong remainder on how readily and rapidly a breach can outbreak as well as how terrible the effects can be. This event stays as a classic example of the need of being aware of the risks posed by the cyber-attacks, physical attacks, and the necessity of employing powerful security measures in place to guard against them. This demonstrates how imperative it is to have a thorough incident response strategy as a firm base to lessen the effects of such breaches with a clear and detailed communication plan to ensure that the clients and other stakeholders are notified in the case of the breach.

This case study stands as the prime example in demonstrating how even the most advanced and sophisticated security systems can be attacked. Walgreens implemented multiple security measures and multiple layers of security like the data encryption after the outbreak of the 2018 massive security breach. Yet, it was prone to such attacks in the later consecutive years serves to be an alert that security practices are not the finite solutions that are documented at once and put into action force but it is a process which must be sculpted as the organisations expands it horizons and the business grows in terms of the number of the numbers, the amount of revenue it generates. The alterations and the modifications must be considered coping with the potential risks of the modern world.

The case study taught me how scalable the security system which is flexible enough to grow with the organisation. This throws light on the fact that security protocol should be able to expand and alter to accommodate the developments, growth, and changes in conjunction with the organisation. This is vital to support new users, emerging technologies, software, hardware, networks, and data types while also integrating with the current systems or procedures that the organisation may be employing. In addition to this the security strategies must recognise malicious behaviour and react decisively and efficiently if a breach occurs, entailing the capacity of the security system to promptly patch any vulnerabilities and implementing defensive measures in place to ward off further intrusions. I had also the understanding that it should be simple and smooth for the organisation to integrate with any third-party services or applications that are used by the organisation. After the detail study of 2020 breach incident of Walgreens, it emphasises the importance of the security of the physical infrastructure. This physical infrastructure security refers to the safety protocols that are put in place to safeguard an organisation’s physical assets and the facilities like the lock systems, access control systems, video surveillance, security guards, Security technologies including the motion sensors, facial recognition systems, infrared cameras, physical barriers like fences, walls, gates together help protecting people and property from unlawful entry, theft, and physical harm. This will limit access to certain locations within the organisation.

I understood how three parties of interest in connection to the Walgreens should behave and react after the outbreak of the breach. Talking about the Walgreens who holds the direct responsibility of safeguarding the customers private and sensitive information failed to secure their systems from external threats. The customers on the other hand have right to question about their personal data being compromised and have equal right to be provided with compensation and assistance from Walgreens to help them in securing their lost data. Stakeholders should urge to reassess its security measures and procedures to avert such occurrences from transpiring.

I also learned how to contain a security breach by having an in-depth case study on Walgreens by keenly examining the reactions of the security professionals and the criminal justice system, soon after the outbreak of the breach. They not just employed the appropriate security measures like giving alerts, warnings to the individuals with the suspicious behaviour and procedures are set up for handling any possible stolen property, strengthening the security, but they also collaborated with the law enforcement and outside partners to effectively contain the breach and apprehend those who were responsible. Additionally, they also gave customers information and guidance on how to safeguard their data without being exposed to the fraudulent activities. These overall responses of the security professionals made me realise their determination to ensure safety and security of retail establishments and their patrons. I also had a fair understanding that such large-scale breaches turn out to be a trend if not addressed quickly and appropriately.

**WHAT I LEARNED ABOUT INFORMATION SECURITY?**

The operation that governs the security of an organisation’s computer systems and infrastructure containing the confidential data and information is called as the Information Security Management (ISM). This functions with the goal to avoid, spot, respond and react to the security threats and risks, averting the unauthorised access ensuring the CIA traits which are Confidentiality, Integrity and Availability of the data and information. It also focuses on the necessity to formulate the plans, policies, strategies, and procedures. As the part of this course, I have had the opportunity to be acquainted with various concepts. The following are the few concepts I would be enthusiastic to use in the real time professional career.

**1. Fire Walls and Network Security:** The fundamental and key components to secure a network are the firewalls and Network Security. These are essential because they track down and regulates the network traffic that enters and leaves the network in compliance with a set of approved security rules and standards. It is framed to guard the private network against unwanted access and the malicious actors to stop the illicit communications and intrusions from entering and exiting the operating systems.

Talking about my real time application of the firewalls, I can use **Packet Filtering Firewall** to filter incoming and outgoing network considering the parameters like IP addresses of the source, destination, port number and configure it in a way to accept and reject certain sorts of the transmissions. Talking about using this for an organisation will allow the only specific type of the network connections prohibiting the malicious access to the current systems. There are certain categories of the Packet Filtering Firewalls like the **Static Filtering** which is the most efficient and easy way to give the network certain level of security, can be commonly applied to the household personal networks to guard from the harmful network transmissions. The next type is the **Dynamic Filtering** which is more robust compared to the Static Filtering. Even if the malicious traffic presents itself as the regular traffic, it can still identify and can stop the intrusion. The other category is the **Stateful Packet Inspection** which is like the dynamic filtering but also it can maintain the records of the URL’s status. I can use each of these techniques in different places be it my workplace or residence to guard my networks.

**2. Cryptography:** A specialised field of mathematics is called as Cryptography, concerned with developing safe transmission techniques. It serves as the shield against unauthorised access, modification, and disclosure of the data. As we all know that the data security is a daily concern and cryptography assists effectively with that. I personally log into various websites for studying, online shopping and many of these websites encrypt the data I fed in before sending it over internet using the encryption making sure that no one can access and intercept my data. The application of this concept is very beneficial and practical to me right now and as well as in the future. This enables me to guard my private data like the financial transactions, e-mails etc. This allows me to confirm the legitimacy of a text message, file, or a paper, ensuring that it was sent from the intended source.

The two concepts that caught my attention are the Substitution cipher and the Transposition cipher. **Substitution cipher** is a type of cryptography that substitutes different symbols or letters to every word in the data or the text. This sought to be the earliest form of the encryption techniques. I can use this more often when sending confidential messages, emails, data to the intended recipient such that only he/she houses the decryption keys to decode them. This highlights that the recipient must hold the appropriate code to decode the message sent by guarding with the substitution cipher. The next concept is the **Transposition Cipher,** which is a sort of encryption where the characters, letters in the data, message, text are shuffled to produce a unique text. The location of the letters is adjusted rather than changing their original order. This transposition cipher can also be amalgamated with the substitution cipher, to make it more dynamic. As an example, I can also use this transposition cipher to encrypt the data exchanged between me and the web server so that only the intended audience can view it. The recipient of the message encrypted with the transposition cipher need to be aware of the sequence key in which the characters or the letters were switched around and this key or the original sequence can be referred as the code that helps to decode the message.

**3. Disaster Recovery Planning:** Planning for the disaster recovery is crucial aspect of anyone’s life, any organisation or business. This entails the development of strategies and plans to recover from the diverse potential threats hampering personal level and the organisational level. This plan will allow and will serve as pathway to resume the operations swiftly after being hit by the disaster. This concept inculcated a sense of being proactive in being prepared for the disasters that I might face in the upcoming days of future in connection to the data. For example, if someone steals my personal laptop which contain the sensitive and confidential data. I can effortlessly get remedied if I have a disaster recovery plan in place. This includes setting up more storage options, establishing backups for the confidential data. This planning should be in such a way that regular testing must be conducted to make sure it is robust and functional. The use of cloud base serves to back up the data and the programs would assist me with this because the applications, data and information economically secured and reliably backed up using the cloud computing ensuring that the data is accessible and can be efficiently retrieved in the event of any disaster.

**4. Security awareness and Training:** A key component of protecting the personal and professional data is the security awareness which can be attained through the security training, and you can acquire this through variety of ways. The knowledge and the practice are the two important aspects of this concept. Comprehending the fundamental, recognising the threats and spotting them down are the goals of the **Knowledge**. Employing the optimal and efficient security protocols, strategies including usage of the strong passwords, two factor authentication, refusing the clicking of dubious links are all the part of **Practice** aspect of the Security awareness and training. This course gave me awareness about the potential threats like the phishing attacks, social engineering, malware, using public Wi-Fi etc. which assist to me to be cautious and be prepared for the disaster that might happen in the future. This will also allow me to guard the data more safely, securely, and effectively by understanding the significance of doing so. I learnt the importance of being in line with the robust security trends because as all we know as the technology emerges and progresses so do the threat. As the part of the security awareness and training I grasped the knowledge of securing the sensitive data including the passwords, financial transactions, and the personal details. This hampered me with fundamental knowledge to be prepared to start of my professional career, to be alert and updated with the time by recognising the signs of the malicious and the fraudulent activities such as interruptions in the performance of the systems, unauthorised access, and odd emails.

**WHAT TOPICS THAT RESONATED WITH ME?**

For variety of reasons the concepts like the access controls, firewalls, and the VPN’s reverberated with me. Since all the three concepts are vital and crucial components of the security system of any organisation. I felt these are very intriguing topics to study and explore them more in detail because these elements ensure that the data is saved securely and can be accessed only by the authorised, desired users. The following descriptions gives an overview of the topics and why they are incredibly relevant to the modern world.

**1. Access controls:** The access controls regulate the access to the resources, and they stand as the crucial security mechanism. These can also to be used to govern the access to part of the system, part of the resource or the data system and serves as the guide to whom the access must be given and to what extent the activities must be performed. This idea gave me a broader understanding of how to deal with the sensitive data from being prone to the breaches. The two important controls that drew my attention are discretionary and non-discretionary access controls. **Discretionary access controls** solely operated by the user permissions by checking the authentication of the users like the username, password, bio metric identifications etc. and the access to the systems and the activities that the user can perform will be granted after the authentication check. **Non-discretionary access controls** are the controls that are not concerned with the user permissions, but these controls depend on the pre set rules and guidelines which specifies which resources to be given access and to what extent the certain user can perform the activities with the resource given.

**2. Firewalls:** Network security tools like the firewalls are deployed to secure the network against the hostile activities. Firewalls software and hardware components function together to monitor, regulate, and filter the communications entering and exiting the network. Apart from the firewalls processing modes like the Packet filtering, MAC layer firewalls by MAC address and the Hybrid walls there are various network connection architectures that firewall devices can be aimed for. The configuration to the networks is determined by the three important factors like the network’s goals and objectives, company’s ability to design and deploy architecture, funds available for the activity, function, and the program. Single Bastion Hosts, Screened hosts, Screened subnet (with Demilitarized Zone -DMZ), Multi Bastion Hosts are the four most prevalent architectural configurations of the firewalls.

**Single Bastion Hosts:** Providing a solitary and safe means of entry from an open or untrusted network to a private or trusted network is the primary goal of a bastion firewall. It often sits between the private network and the Internet in a demilitarized zone (DMZ). This Bastion firewall serves as an entry point, and it is set up to permit access to only the certain services. Additionally, it can also be programmed to restrict the access to confined IP addresses and people. This firewall is quite essential because it constantly serves as the sole access point between the two networks.

**Screened Hosts:** A host that is safeguarded and secured by a screening router is known as the screened hosts. The hosts can be a server, computer, or any other network device. Typically, this kind of security mechanism is put in place to stop malicious traffic from accessing the private network to guarantee that only those with the permissions can access the network. The potentially hazardous actions can be blocked by using the screened hosts which can be installed in the corporate business networks. These can also restrict and limit access to certain applications, programs, services of the network.

**Screened subnet (with Demilitarized Zone-DMZ):** This is a network security tool that isolates certain portions and parts of an internal network from rest of the internal network which typically houses the sensitive services. By placing the external filtering routers are used to re direct the connections from the open and unauthorized networks. By allowing the connections enter and exit the external filtering routers by guaranteeing the isolation of the DMZ segment. The connections are then permitted to the trusted network through the DMZ or the DMZ bastion host servers. This ensures that only the approved traffic to enter the trusted network.

**Multi Bastion Hosts:** A security architecture called the Multi Bastion Hosts is used as shield to an organisation’s information systems from potential threats, this is accomplished by dividing the network into several secure zones. Intrusion Detection Systems, firewalls, and various security protocols, procedures collectively constitute a multi bastion host system. Implementing these layers of security at key locations inside the network must be done by every organisation to stop the malicious activities, threats, and dangers.

**REFERENCES:**

<https://scsonline.georgetown.edu/programs/masters-technology-management/resources/top-threats-to-information-technology>

<https://cybersecuritycareer.org/cybersecurity-risks/>

<https://www.rapid7.com/fundamentals/information-security-risk-management/>

<https://netshopexpert.com/Cybersecurity%20Solutions?og1=fa6763c4-b034-4383-948d-2037697e4919&acid=cid54291&gclid=&msclkid=739928340a5e1d20c6ab4c72cb8c515d&avid=4784&asrc=bing>

<https://www.comptia.org/content/research/trends-in-information-security-study>

<https://blog.bit.ai/information-security-plan/>

<https://www.techtarget.com/searchsecurity/feature/10-types-of-security-incidents-and-how-to-handle-them>

<https://unt.instructure.com/courses/83326/pages/wk12-materials-2?module_item_id=5003585>

<https://unt.instructure.com/courses/83326/pages/wk13-materials?module_item_id=4957753>

<https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2018/application-security-a-three-phase-action-plan>

<https://www.cio.com/article/222076/how-to-implement-a-successful-security-plan.html>

<https://www.mtu.edu/it/security/policies-procedures-guidelines/information-security-plan.pdf>

<https://www.resolver.com/blog/enterprise-security-plan/>