

**BCIS 5740**

I**nformation Security Management**

**Assignment 3**  
 **“The Case Study of**

**Microsoft Breach Incident”**  
**Submitted to: Prof. Obi Ogbanufe**  
  
**Submitted By:**  
Preeti Chaudhry-11559290

Microsoft is such a big organization, and its market is considered the topmost in the world. In this case study, I want to discuss all my take on security-related practices that should be put into practicality for better and secure networks and will discuss their counterparts. In short, I will add all the details of the case study.  
  
**Aspects of Cyber Security That Gets Affected**  
  
These are the aspects of cybersecurity that were affected by the breach incident in Microsoft in 2021.

- Ransomware: This type of attack allows hackers to encrypt the files on the victim’s system and get it locked until the purpose of the hacker gets solved.

- Third-Party Vulnerabilities: The third part acts as an important role in the breaching of data. They don’t have proper security measures so leave the organization on the verge of getting the data leaked.

- Undetected Security Gaps: A lack of endpoint security on mobile devices and laptops gives hackers a chance of having a ransomware attack.  
  
- Confidentiality: The confidentiality of the data got scattered, as this data gets accessed by hackers now. Millions of people's details are distributed and are now under the control of hackers. Confidentiality is the first and foremost factor that gets affected when any breach incident happens. This incident impacted on an overall 250 million customer confidential records.

- Availability: The availability of data is an important aspect of any organization. Within the organization also, we have some hierarchy like how the flow of information is affected. Some sensitive data and information are accessed by only a limited set of people. But the breach incident leads to the leakage of information so badly and it really impacts and is available to the hackers. This breach incident leads to the sharing of data, personal information, and passwords of the affected users by the hackers. They also get access to the administrative rights on that system as a result of the breach. Once one gets the admin privileges, a hacker can play in the way he/she wants. Simply copy the code of the server to any of the locations and it runs out perfectly because the hacker has admin rights. Hackers are used to installing the web shell in the system, once the web shell is installed, Backdoor entry is possible. Backdoor entry allows you to access the system all the time from any location if your web shell is active there. Once a web shell is installed, hackers can access anything in the system.

- Integrity: None of the data integrity is maintained. Simply hackers have all the data they need and can play with it the way they want. Now, these people start playing with their emotions by putting false actions and promises. Sending them unwanted emails with the promise of jobs, and just needing their money, that’s it. None of the objectives and promises are true.  
  
**Prevention measures for Information Security**  
  
There are some factors that can help the organization to save the data at some extent:  
   
1) Management Security as I read the full content of the Microsoft case study. I would like to say that there’s some carelessness that arises from the management side also.   
  
- On 5 Jan 2021, there’s a security testing company named DEVCORE has made the earliest announcement that there’s some vulnerability for Microsoft data which Microsoft itself confirms on 8 Jan 2021. Later Volexity, a cybersecurity company confirms that hackers are spying on two Microsoft users and alerted Microsoft of the same.

- On 2 March 2021, another cybersecurity company ESET announced that multiple hackers are trying to access the data. The analysts of the security team have made the confirmation that hackers are running the crypto mining software not the servers.   
  
Even after having this much information, Microsoft also accepted and confirmed. Where there all the management people are!  
It means they’re in their chill mode. They didn’t care much about the content's seriousness.  
2) Operational Security: This incident was first reported at the beginning of Jan 2022. There were some zero-day exploits discovered on the Microsoft campus. The operations team has such a big responsibility on their shoulders regarding the maintenance of the entire data flow and security. The Management to take some steps to prevent it from going out. They can instruct the whole team and make it a big concern at that time. If some patches were run in the systems at that time, there’re chances that we can save our data. And why are employees not meant to install all the updated features? These types of practices should be made compulsion within the organization. New functionalities of system run patches are properly installed. This will not allow the hackers to install a web shell. Once the web shell is installed, we can’t do anything. Hackers can access it now. These precautionary steps had to be taken earlier before this incident even knocked out.  
   
3) Physical Security Controls:

- Immediately physical installation of software patches in the systems

- Built a kind of policy where the hierarchy members should individually do a proper check-up on whether employees install certain security checks or not. There should be a penalty if someone did not install the security checks already.  
  
**Roles of various communities for data security**  
  
The three communities of interest play a very vital role in maintaining the environment within the organization. These three communities of interest are  
   
1) The Information Security Community (InfoSec)  
 2) The Information Technology Community (IT)  
 3) The General Business Community  
   
The Information Security Community (InfoSec) - This team is comprised of IT professionals and managers. This team’s main responsibility is to protect the organization's data whenever any security breach incident tried to play with sensitive organizational information.  
   
The Information Technology Community (IT) - This team comprises IT professionals who provide all the information technologies and other technical resources required by the organization. This team acts as a kind of bridge between the organizational available information and all business needs. It supports the organizational objectives by providing the required services and satisfies the business needs at the same time. The General Business Community - This team comprises all the non-IT professional and Managers. It identifies all the organizational objectives and business needs and helps them to accomplish goals on time. This also supports the other departments within the same organization.  
   
These are the three main rock pillars within the organization which makes the organization worth it for employees to work on further and grow. Since Microsoft is such a big organization. I can never say that all these 3 pillars don’t work in sync. If it were like that then the company for sure wouldn’t be the company, it is now. And, even after this major breach incident, the company made a strong comeback in the market in terms of stocks and revenues. This is sure proof that the internal teams used to work in a very sync and organized way. That’s how the yearly predictions show.   
  
- Revenue   
In the year 2020 - $143.015 billion

In the year 2021 - $168 billion   
  
- Stock  
In 2020 - 193.0261

In 2021 - 275.9408   
  
But also, I want to make a point that before this breach incident happens, we got various security warnings in terms of a security breach. Microsoft confirms those warning that was shared by the social Engineering teams. But here comes the point, even after knowing this much info, how these teams wouldn’t be able to protect Microsoft from this coming breach incident. It shows that there are some hindrances in functioning within the internal team. As I read the whole article, I didn’t find any single place where it shows that effort was thrown in by these teams.   
  
But after this incident happened, they started working better than earlier. These are some of the changes and practices introduced by the organizations -  
   
- On 12 March 2021, the Microsoft security intelligence team deployed a new family of ransomware called DearCry to all the affected servers. This will demand the payment to recover the earlier files. And there is no guarantee that after making the payment, you will have access to the content.

- On 2 March 2021, Microsoft releases a one-click power PowerShell tool, which installs the protection updates against a particular threat, runs out of malware to detect the installed web shells in the system. These are all some temporary mitigation measures introduced by the teams.  
  
**Collision of Organization Business and Security Needs**  
  
We have had various times when business and security needs collide. This will come into action, especially during work-from-home times. Previously, the security and password-related things were meant to be managed by the security teams, but now this is more shifted towards the employee. Now, employees are responsible for all the security and password-related compliance. They’re the owner of their systems and have the power to manage them accordingly. Now IT and all security teams have started shrinking with the aid of more experienced and talented people. They stopped working on the micro level, now these teams are used to working at macro level. Let the employees manage their little things separately, and these teams used to take care of the puzzles and make sure that everything is safe and secure from the external point of view. It accelerates a more collaborative approach and shrinking of the teams in size.

But if an employee faces some issues and is not able to solve them by himself/herself, must contact the security team then. Here, it creates a problem during work from home time. Since we are used to being in offices, we can approach, and things will get solved in minutes by the IT security team and don’t have any impact on the business needs as well. This will help in the smooth transitioning of the process. Working remotely creates a problem to access everything remotely like email, login issues, and all troubleshooting. This is a difficult task even for the most experienced IT professionals. This is my personal experience when I used to do work from home, it was problematic when someday VPN is down, and VPN password expires, and other login issues. In all these cases, I used to have a session with the security team and solve everything the way it comes. It’s difficult for security to figure out everything remotely and it takes 3, or 4 hours to solve the dispute. This in return affects the other Business tasks that are assigned for an individual and must backtrack and start from there. This will put more pressure on employees also.  
  
**Introduction Of Policies that can prevent Breach Incidents**  
  
- Issue-Specific Security Policy (ISSP)

- Enterprise Information Security Policy (EISP)

- Systems-specific security policy   
  
We have some policies that surely help in protecting the organization from various breach incidents.   
  
- Issue-Specific Security Policy (ISSP): This policy is made by keeping in mind that there should be governance of all the existing technologies. This policy is used to govern all the individual technologies that exist within an organization. If this was present earlier in the Microsoft breach incident, we expect to have all our systems updated with the latest versions and the installation of web shell wouldn’t be possible further.

- Enterprise Information Security Policy (EISP): This is used to deal with all the security traits that prevail within the organization. Deals with everything starting from the security that persists, and what all new security modes have too instilled. This is used to direct all the organization's goals united and direct them toward building a better secure network. If efforts were put in place early, we can save our data breach with the help of this policy. If an organization picks the first warning seriously, all efforts combined with the help of this policy create a better network with more secure transactions.   
  
Systems-specific security policy: This comprises written documents that are used to help in providing us with standard procedures that help in configuring and implementing standard information systems. It helps us in managing the timesheet and all expenses management within the organization. This includes the installation of a firewall and other security protectors within the system. This will surely help to protect the data from any kind of breach.  
  
**Usage Of Incident responses for preventing Breaches**  
  
We have some security incidents that could have been used for Incident Management Overview that contains the Breach Incident -  
   
- Microsoft defines security as an online medium that confirms the breach of security in the form of loss, unauthorized access, confidentiality, integrity, and security of data. All of these are called security breach incidents.   
- All employees should have been given timely training for protecting their security from these kinds of incidents. This training should be conducted annually. - We have another facility available in the form of DPA (Data Protection addendum). With the help of this facility, Microsoft notifies affected customers the72 hours after the event had outlined. As and when a declaration of the event occurs, the notification process gets started without any further delay.  
 - Microsoft’s services need to be properly regulated against any other external compliance and certifications.  
  
**Information security Framework with Mandate KeyPoint Intro**  
   
If you were to help design an information security plan for this organization, which information security framework would you use, and why?  
  
We as an IT world used to have various strategies that help in maintaining the security privacy and other policies within the organization. The IT security framework used to have a documented set of procedures and policies that used to follow in a way that helps to maintain the name of the organization and protects from any kind of breach attacks. would like to mention some of the frameworks which I want to use for the privacy of the Microsoft organization in terms of security-  
  
1) NIST Cybersecurity Framework: This framework is very broad and complex and comprises documents, procedures, and other steps comprised of a total of 41 pages. But the framework is quite easy to understand. This will basically work in 5 aspects. i.e., Identify, Protect, Detect, Respond and Recover. Let’s discuss each of its factors separately to get a clearer understanding.  
   
- Identify: This will focus on the future steps taken by the company in terms of cyber-security. This will consider factors like what current dangers exist in the system, and what dangers are likely to occur. After having an evaluation of these two factors and considering the company’s goals, further steps of cybersecurity will be taken.  
   
- Protect: This framework consists of a category called PR.DS stands for “Protect Data Security”. Furthermore, it has more than 7 categories and all are responsible for data protecting data. It has three parts (PR.DS-1) and (PR.DS-2). It has the protection of data at Rest and its protection in transit also, so on and so forth.   
  
- Detect: It includes the creation and implementation of necessary cyber security operations to detect the presence of any future cyber security incidents.  
  
- Respond: This step makes sure that the SDLC process filtration is done properly through the phases of planning, and analysis, and mitigation operations. It makes sure that the cybersecurity process will always improve.  
  
 - Recover: This step makes sure that it’ll return soon back to regular activity after mitigating all the effects of cyber security occurrences.  
   
2) PDCA Cycle: This cycle is based on and works on the Business development method. It’s divided further into 4 steps -   
- Plan: This step focuses on establishing ISMS along with policies, procedures, and objectives for risk management  
  
- Do: This includes implementing the actual functioning of Infosec.  
  
- Check: based on reviewing and monitoring of ISMS, it is used to measure the system process along with the available policies and procedures.  
  
- Act: This used to deal with updating and improving the ISMS. This makes sure used to take all the preventive and corrective measures for the internal management and audits.  
  
**References**  
  
Methodology/Impact  
[**https://en.wikipedia.org/wiki/2021\_Microsoft\_Exchange\_Server\_data\_breach**](https://en.wikipedia.org/wiki/2021_Microsoft_Exchange_Server_data_breach)Breaching Initiation  
<https://auth0.com/blog/the-worst-data-breaches-of-2021-q1-and-q2/>**.**  
  
Exposition Of Data  
<https://www.lifelock.com/learn/data-breaches/microsoft-exposed-250-million-customer-records>Wikipedia Source  
<https://en.wikipedia.org/wiki/2021_Microsoft_Exchange_Server_data_breach#Impact>Mitigation Strategies  
<https://en.wikipedia.org/wiki/2021_Microsoft_Exchange_Server_data_breach>Steps Microsoft had taken before security breach  
<https://www.microsoft.com/en-us/microsoft-365/business-insights-ideas/resources/avoid-security-breaches-how-to-protect-your-data>Security Breach of 2021  
<https://jumpcloud.com/blog/top-5-security-breaches-of-2021>Collision of IT and Security  
<https://www.techtarget.com/searchsecurity/feature/IT-and-security-teams-collide-as-companies-work-from-home>Incident Management Overview  
<https://docs.microsoft.com/en-us/compliance/assurance/assurance-incident-management>