 |  BCIS 5740 Information Security Management

The Case Study of Microsoft Breach Incident

The Case Study of Microsoft Breach Incident

# Introduction

Microsoft was founded on 4 April 1975 by Bill Gates and Paul G. Allen, two school friends from Seattle. Microsoft's headquarters is in Redmond, WA. Microsoft used to own a total number of full-time employees as 1,81,000.

The Chinese hacking group known as Hafnium attacked Microsoft in March of 2021. The attack began when hackers used stolen passwords combined with previously undetected vulnerabilities on Microsoft Exchange software servers. The vulnerability allowed any user who had physical or virtual access to the login time to gain full administrative rights. This way, the attackers logged in and installed malware that created command-and-control proxies for their use.

To help with this kind of attack, Microsoft updates that its customers should immediately install all new software. In this case, the vulnerabilities were discovered, and Microsoft released patches in 2020, but many customers hadn't updated their systems. It was estimated that 2,50,000 people were affected by this attack, and around 30,000 organizations in the United States were affected.

Satya Nadella was the CEO of Microsoft when this incident happened. It was estimated that this incident caused an average worldwide loss of $3.86 million.

# The Incident

## This Microsoft breach incident happens in 3 stages in the year 2021. The incident was first reported in the month of January, then March. Here is how it gets noticed -

- 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. \

On 10 March 2021, security researcher Nguyen Jang intentionally posted a code on GitHub regarding how the exploit words comprised of lots of errors, so that the hackers wouldn't be able to use the code to hack the servers. Later, this code was removed as it requires minimal modification to make the code work.

This attack was planned by the Chinese-based hacking group in which Hafnium is know how to install the web shell on the servers. But the Chinese government is not ready to accept any of these allegations and said that's it all groundless. This incident impacts 30,000 organizations within the US which include the government sector, IT sector, defense, and all educational institutions also.

This incident was first reported at the beginning of Jan 2022. There were some zero-day exploits discovered on the Microsoft campus. 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 ***because of*** the breach. Hackers also have access to all the connected devices that are part of the main affected device. Hackers use the backdoor policy for this attack. So, anyhow they've full access to the system even if Microsoft updates the version or the previous version features will no longer be available.

Hackers used the four separate zero-day policies to access the systems. This targets Microsoft outlook and from here it'll get access to all the calendar invites, passwords, emails and the whole work, and ultimately this will allow access to the entire servers which hackers can use to target. Hackers used to do this process in a very strategic way, using the process of mass scanning to find all the nearby vulnerable servers available, and get the address of the server. Once you get the address of the server, then use the two exploits policy which will work out in 2 steps –

- Connect to the server as a false authenticate user

- exploited standard user access to the admin rights.

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.

## Impact of the Breach

This hacking attack impacts all the data of Microsoft in terms of email communications. Everything communicated over email to an organization or related organization gets exposed.This incident happened because there were some vulnerabilities in the Microsoft system. Though the organization released patches to resolve these vulnerabilities, customers need to update their system to install these patches. Till the time this practice is not performed by people, we're still at risk of any future hijack.The main target of the hacking team is just to get all the email addresses and personal information from all of Microsoft's allied industries also. Further, hackers used to send unwanted emails with phishing links and content and make people foolish. They want to do this to get money, and all banking data from people to access their credentials for their own sake.

Breaching data leads to the flow of information on a massive scale directly from the people to the hackers. This information leads to the sharing of various personal ids starting from an email address, phone number, organizational data, and internal security things, and consequently, it can affect all the personal security of an individual and hackers have all the data. There're several other companies that are owned by Microsoft, their data also gets shared. People start getting unwanted calls, fake job offers, and emails with unwanted attachments that are just spam and don't have any relation to the job. People start getting fake job offers like you're selected for this company with an average package of this. Come and let's join——kind of things. Microsoft lost a million dollars because of this crisis.

The company starts falling to loss and starts firing employees. This leads to so many layoffs. Skilled people suddenly search for jobs and can't find them anymore frequently. A wave of recession starts hitting the market for IT employees. I still remember one of my cousin's brother got fired from Microsoft at that time. I remember that he got placed in his dream company and how badly this thing hurt him! At that moment, I didn't have much awareness of this thing, but when I met him personally, he told me the things that happened with him, it was about various other people that also got fired. Firing from such kind of organization soon after you complete your master's is a kind of shock!People are dealing with this mental pressure along with the hustle of searching for another job.

When this kind of incident happens, social Engineering people and teams start taking advantage of the soft crowd emotionally. They kind of start building the feeling of fear, helplessness, urgency, and neediness. All this will ultimately lead to the people falling prey and the loss of money, and credibility for the previous organization.

## This incident impacted on an overall 250 million customer records. The target population included people from all the majors like government people, non-government organizations, people from the defense, students, IT people everyone. Though Microsoft is such a big organization, it's on the verge of rising all the time. It didn't have much effect on the various factors. I want to list some of them with a comparison from the previous year's data.

## - Revenue

## In the year 2020 - $143.015 billion

## In the year 2021 - $168 billion

## Microsoft has noticed an upgrade in terms of revenue, an increment of 18% noticed in comparison to the previous year.

## - Stock Price Microsoft noticed an Increment in terms of stock price also. There's a bump in the prices of stock compared to the previous year 2020.

## In 2020 - 193.0261

## In 2021 - 275.9408

## - Reputation - Any major breaching incident affects the people working there or want to work there in some or other way. This impacted on the current workers in terms of getting fired from the company and other potential employees who want to work there take a step back because they are also under fear of getting fired. Later, Microsoft is such a big name and makes a strong comeback in the market with better stocks and revenues, and from then till now its stocks and revenue value is increasing every year. Again, the big organization gains the unbreakable trust of people, and it continues to persist.

## Even before this breaching incident happened, Microsoft used a lot of safety precautions to protect the data from any kind of security means. These are some of the processes that Microsoft used to

## - Awareness among the people who're working in the organization. Once employees get to be kind that they've some data that hackers are always in need of. They will access things more diligently and with knowledge. Microsoft used to have some other kinds of training programs within the organization to train the employees on how to deal with data.

## - Classification of data based on sensitivity.

## - Have restrictions of access on the basis and other protected rights should be given based on authority.

## - Store all the necessary information and sensitive content within the cloud.

## - All the devices which have some secure and sensitive information stored should have the capabilities enabled.

## - Access to sensitive information should have individual sensitive credential access.

## - Always emphasize the strength of passwords. - Multi-factor authentication is installed to access almost every sensitive piece of information which is very important and essential for protecting the security of the data.

## - Encryption of security data is very important while storing and transferring it.

## - Back up and production work should be separated.

## - Always make sure that the system is properly up to date. Updating of the system instills the new updated version with a more secure connection.

## - Always have the security and networking team members look over the activities that are happening within the organization.

## And I would like to write that these kinds of incidents are problematic for everyone. When I'm reading it, sometimes I also feel like that if it's someone accessing my information from somewhere. I can also be part of this kind of incident. To be on the safer side, I started using 2-factor authentication on almost all the apps where it's possible. I stopped writing my passwords on the notepad. I started to be more aware of the strength of the password, now I prefer to use passwords that are good in strength, and difficult and try to remember them and learn in my way. And recently, 4 months prior there's a kind of scam happened with me in which I lost my 3250 USD. Being a student, it's a very big amount for me. I still remember how I came out of this fear. It'll take me a month to accept it. it. But this gives me a lifelong lesson on how to be very aware and protective regarding the security of your data.

## Mitigation Strategies

## - 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.

# 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 Key Point Intro

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.

**Case Narrative**

The acknowledgement by Microsoft Corporation regarding an access misconfiguration that led to the exposure of more than 250 million customer records on a public access database that had not password protection caused a global out roar. However, the case prevented an opportunity to analysts and cyber security experts to access the vulnerability of their institutions regardless of size and technical resources. 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.

# Potential Consequences

With Microsoft's recent data breach, many were wondering how the company would deal with this situation and what are the potential consequences for all those who used its service. The data breach involved more than 250 000 individuals' information (Novet, 2021). The lost data include names, email addresses, passwords, telephone numbers, and financial details such as bank account numbers and credit card details.

There are four potential consequences of the data breach for Microsoft customers.

*Outage of company services and passwords*

Microsoft revealed that the data breach could result in the suspension or disorientation of service for the users, and their passwords will automatically be reset. The company is currently working to mitigate the situation. It is unclear how long the users will have to wait before resetting passwords. Some users report that they have already experienced the consequences of the data breach (GAO, 202). Some of them have been unable to access their email or have had their passwords automatically reset. However, those who want to regain access to their account must generate a new password, ideally containing a combination of letters, numbers, and special characters.

*Affected services will be restarted*

As mentioned in the previous point, affected services such as Outlook, Hotmail, and Live Mail will have to be restaffed again as they cannot cope with the number of users due to the data breach (GAO, 202). It will result in the accounts being suspended once again.

*Increase in the number of spam messages*

As a direct consequence of the previous two points, Microsoft users could receive up to 30% more spam messages in their mailbox after their accounts are reinstated (Chance, 2021). It is because spammers can access the users' previous email addresses. The users will have to spam their mailbox to prevent this from happening. It is recommended that the users keep their spam filter enabled to decrease the chances of getting emails from spammers. Most spam filters can detect emails sent from known senders and can be set up to not allow emails from these senders to be classified as spam (GAO, 202). It is because some third parties will have access to their online address and email passwords.

*Possible identity theft*

Some hackers will likely be able to access Microsoft users' information after the data breach. Once they have access to their details, they can use them to create fake accounts and steal money from these users (Chance, 2021). To avoid being a victim of identity theft, Microsoft customers should be extra careful with their accounts and ensure strong password combinations and 2-step verification protects them, preventing hackers from accessing their accounts. After the data breach, users also had to deal with the possibility of phishing emails. Since their accounts were suspended, they received messages from other third-party services, and all those who clicked on them had a big chance of suffering from severe identity theft.

## Action Plan

The data breach will cause some losses to the company. The number of users that will stop using Microsoft services is still unknown, but it is certain that the firm will have to deal with a lot of criticism from consumers and must pay fines for failing to protect their accounts and data. Microsoft services must bear the cost of account suspensions and anticipate growth in spam emails. However, to ensure that the company could deal with these losses, Microsoft decided to acknowledge this incident and acted by informing all those who were affected (Chance, 2021). It has helped them gain some trust from their customers and made them able to handle this situation better than it could have been if we had not admitted the data breach.

Four action plans may handle the security breach for the affected enterprises and Exchange Server users

*Consumer Notification*

After the data breach was announced, Microsoft started to send emails to those who had been affected. For those who do not use Microsoft services, their service providers will also send them emails with information about the breach and how they should check if they have been affected. As per the GDPR guidelines, all affected users must be notified of the security breach within 72 hours of the data breach. Notifying both the affected users and unaffected consumers can help both parties prepare. The notifications can be done via email, SMS, or phone. Per the GDPR guidelines, anyone receiving this notification can choose to keep it private.

*Checking for Compromise Indicators*

After such a data breach is detected, the affected users need to check for any indicators that suspicious emails could have been sent from their accounts. These indicators are usually called compromise indicators and include a sudden increase in the number of messages from the same sender, more than one email account created with their account, unusual behavior of accounts, and some other measures that may cause alarm in an incident like this. The users should be on the lookout for any suspicious activity resulting from the data breach. For example, they should notice odd behavior in their accounts, such as sending unusual amounts of money to other users or receiving strange emails from third parties. Their service providers should also be able to detect any unusual activity in their accounts and notify them. Compromise indicators include the presence of unknown incoming mails, unusual login activity, the presence of unusual files in their account, etc.

*Creating a Forensic Image*

To create a forensic image of an affected user's mailbox is just like comparing it with a "snapshot" or a "digital footprint." It can help in solving the problem and recovering data from the compromised account safely and quickly. The system would take a snapshot of all data stored in the operating system and compare it with what is stored on the server to ensure all data has not been lost (Chance, 2021). The company should create a forensic image of all the data stored on their servers and ensure that they can provide this image to all users affected by the data breach. The user should not delete any information stored on their account but can use this image to check if all their account data has been compromised. The user will also have information about how much is being stolen and how many users are affected by the security breach. It will help them decide what action to take and prevent identity theft. A forensic image can also ensure business continuity and act against the person or group responsible for the data breach.

*Security Patches*

Microsoft has regularly released patches throughout the security breach to improve its security measures. These patches should be applied to all systems connected to Microsoft networks and protect them from data breaches (Chance, 2021). However, users must ensure that they apply all the necessary patches on their computers and do not install any applications or updates from third parties. The security patches the company implemented should be checked regularly to ensure they can protect the data stored on their servers. All users and their providers should regularly check if they can receive emails from third parties. If suspicious activity is detected, they must report this to their providers, who will then report it to Microsoft.

The security patches that have been released will only work if installed. To ensure they are, the user can check immediately after their account has been suspended if the latest security patches have already been installed on the device they use. Then, they can reinstall the patches to ensure all their data is safe. Patches that safeguard vulnerabilities should be available worldwide against zero-day exploits. Some of the patches are applying to all Exchange servers. It may include Microsoft's best practices, such as transit encryption or proper authentication steps.

Despite the disastrous impact of this data breach, Microsoft has been praised for acting against it and has tried to resolve this incident as quickly as possible by informing those affected about the security breach immediately after it was discovered (Chance, 2021).

# Preferred Course of Action

Companies need to take measures when dealing with a data breach as otherwise, users will lose trust in them and may even stop using their services. Advanced Detection and Response Cloud software is an Artificial intelligence approach to improve the response to cyber-attacks. This new solution provides organizations with improved protection against unauthorized access and use of their cloud infrastructure. It also extends its protection against remote and on-premises devices.

As organizations move their operations and applications into the cloud, they face increasing complexity in monitoring and securing their infrastructures. Existing solutions are not designed to address these challenges effectively and are not easy to deploy and manage. The Cloud Advanced Detection and Response solution provides a comprehensive view of all threat surfaces, allowing organizations to manage their cloud operations confidently (ARIA Cybersecurity Solutions, 2021). The Cloud ADR solution uses a threat modeling approach to analyze and detect threats by their behaviors. It then uses machine learning to find these behaviors in the network data and threat analytics. Its AI-driven approach eliminates human intervention and allows IT staff to deploy and operate the solution quickly.

Cloud ADR is a software-defined approach that combines the capabilities of the application-based solution with the latest threat detection and response capabilities. It enables organizations to improve their protection against unauthorized access and use of their cloud infrastructure. It also extends its protection against remote and on-premises devices. The seven security tools included in the product are designed to provide a comprehensive view of their environment. The Advanced Detection and Response (ADR) solution would provide a virtual AI-SOC that automatically detects and stop cyberattacks without requiring highly trained security personnel (ARIA Cybersecurity Solutions, 2021). It works around the clock and is powered by a big data approach that combines machine learning and advanced analytics. The solution takes advantage of the data collected from various security devices and applications, such as firewalls, operating systems, and cloud services.

The solution takes advantage of the built-in models in SIEM to analyze and visualize every known threat. Its AI capabilities can identify and prevent attacks by analyzing their behavior patterns. It eliminates the need for daily alerts and significantly reduces attack risk. It is a type of security that can help organizations protect themselves from various attacks, such as ransomware, malware, and DDoS attacks. It can also help prevent data loss, policy violations, and other hidden threats. The Cloud ADR solution is a variant of an application-based ADR that can be deployed within a VM infrastructure (ARIA Cybersecurity Solutions, 2021). The threat surface covers the full spectrum of threats, including the cloud, remote devices, and on-premises infrastructure. With machine learning, you can find and analyze threats through their tell-tale behaviors. Automatic stopping of attacks is also built into the platform, which can be used to prevent attacks from happening immediately.

## Steps to integrating an ADR into a server

The Advanced Detection and Response (ADR) system should be fully implemented with all the resources needed to ensure it functions correctly. It will include deciding who will be part of the response team and hiring outside contractors to get expertise in the area. The system should also address security concerns of confidentiality, integrity, and availability to ensure that the system addresses these concerns. The technical staff should be involved in training the incident response team and informing them of what resources they will need to operate the system. It can be done by integrating security controls into the system so that there are some built-in checks and balances when performing the detection process. Reporting security incidents and carrying out investigations is important for any organization; it is always better to report a breach of confidentiality or integrity immediately so that immediate action can be taken to stop further damage from being caused before it spreads further.

***Create an Incident Response Team*:** When developing an Advanced Detection and Response (ADR), it is important to have a team of people who can respond to a breach. This team should contain Incident Response personnel, Person Responsible, Legal Department, and technical experts organized under the Incident Response Team. This team is responsible for keeping security controls in place and ensuring that they continue working properly; they should be responsible for evaluating the effectiveness of security controls and creating an incident response plan in the case of a security incident.

The Incident Response Team should work with security engineers to create a detection plan for their Advanced Detection and Response (ADR) system. They should be able to detect and respond to security incidents as soon as possible to mitigate the damage before it spreads further. The incident response team will also have to help develop a plan for legal issues arising from the breach of personally identifiable information, trade secrets, or intellectual property; this could include informing customers of the breach, monetary compensation, and consultation from legal experts.

***Automate the Incident Response Process*:** By automating this process, you can improve your response time and reduce the human error aspect that may occur by having humans carrying out manual procedures. When the Advanced Detection and Response (ADR) system is being developed, it is important that it can be easily configured and adapted; this can be done using an API to integrate security controls into the incident response process. The incident response process should be automated to continue working properly in the case of a breakdown; this allows for an Advanced Detection and Response (ADR) to function in an environment that may have damaged or compromised hardware and software. All security controls should have a set time frame to work when installed. It can be achieved by using clear instructions to ensure the system is set up correctly.

***Integrate Security Controls into the Incident Response Process***: All security controls should be integrated into the Advanced Detection and Response (ADR) process to ensure that they work together; this can be done by developing a well-structured API to integrate security controls into the incident response system.

***Make sure that the incident response process is communicated to staff members:***

All staff members should be informed and trained on what to do in the case of a security incident; this can be done using written procedures and training sessions that staff members conduct.

***Establishing partnerships with other organizations and agencies to share information, expertise, and experience:*** The response team will need communication channels open with other organizations to share information, expertise, and experience in handling security incidents that could occur within their organizations. They should be able to share information on breach incidents, new security controls, training, and development. New security controls should be brought forward so the team can evaluate them before implementation. They should also be able to recommend any new security controls that may affect the incident response process.

***Developing a plan for handling breaches of personally identifiable information, trade secrets, or intellectual property with an Advanced Detection and Response (ADR):***

The Advanced Detection and Response (ADR) system should be able to notify the incident response team as soon as possible so that they can begin working on the problem and implement their plan. This plan should also include contacting outside parties to ensure that incidents are handled properly. This process can be further improved by integrating an Incident Handling System into the Advanced Detection and Response (ADR) system, whereby all information is logged and can easily be acted upon by the response team.

***Establishing a service level agreement with the information technology staff:***

All staff members should be informed and trained on what to do in the case of a security incident; this could include informing customers of the breach, monetary compensation, and consulting with legal experts. This process can be further improved by integrating an Incident Handling System into the Advanced Detection and Response (ADR) system, whereby all information is logged and can easily be acted upon by the response team.

***Having Response and Notification Procedures from the Advanced Detection and Response (ADR) for Breaches of Personally Identifiable Information, Trade Secrets, or Intellectual Property with an Incident Handling System:***

Formal written procedures should be prepared and distributed to all staff members and kept updated in case of any changes. The Incident Handling System should be able to notify the Advanced Detection and Response (ADR) Service when an incident has occurred. It should also log all security events to allow for analysis. All the Advanced Detection and Response (ADR) team members should evaluate their response plan regularly to prevent human error within the process. Advanced Detection and Response (ADR) can help organizations improve their detection capabilities; by integrating security controls into the system, they can detect attacks more easily before they cause further damage.

***Developing a relationship with outside contractors for an Advanced Detection and Response (ADR)***

The incident response team will need to establish a relationship with outside contractors for the Advanced Detection and Response (ADR) to gain access to their expertise and analyze their findings. It can be done by sharing information and trial runs on the incident response process. These trials could be with other organizations to test it out before it is fully implemented by the Advanced Detection and Response (ADR) team. It can also be done by starting with a trial run in the strategic plans department before adding it to the incident response process.

***Establishing a Service Level Agreement with the information technology staff:***

When developing an Advanced Detection and Response (ADR), an agreement must be established between the team and the Information Technology Department. It will help them determine how they can help each other when different incidents occur. This agreement can be generated during the development of an Advanced Detection and Response (ADR) system so that there is clear communication between both teams. The Incident Response Team should work with security engineers to create a detection plan for their Advanced Detection and Response (ADR) system. They should be able to detect and respond to security incidents as soon as possible to mitigate the damage before it spreads further. The incident response team will also have to help develop a plan for legal issues arising from the breach of personally identifiable information, trade secrets, or intellectual property. It could include informing customers of the breach, monetary compensation, and consultation from legal experts.

***Developing a set of procedures for detecting and responding to security breaches:***

A procedure is needed to ensure consistency between these different detection mechanisms. The procedures will also explain how to follow up on a security incident and what to do in a major incident. The Information Technology Department has to ensure that all security controls are set up correctly for the Advanced Detection and Response (ADR) system to function.

***Gaining approval of this process from the organization's senior management to ensure that it will be implemented correctly:*** The Senior Management has to be involved in developing this plan to clearly understand the Advanced Detection and Response (ADR) system will be doing for them. Developing the plan is also a good time to communicate any concerns they may have with their staff. Senior management must give the go-ahead for this new procedure to ensure there is support from the organization's top. It will help reduce any barriers or opposition when implementing this process.

***Performing testing and training to ensure that the response procedures work correctly:***

The response team should test this process in the strategic plans department before fully implementing it in the Advanced Detection and Response (ADR) system. It can be done by performing a trial run in this department first and then expanding it to other departments as time goes on. Training for the team should include how it will be implemented, what resources they will need, how to use them, and how to develop their skills to deal with any security incidents that may arise within their organization. Performing testing and evaluation is a crucial part of an Advanced Detection and Response (ADR) system; it can be done by performing tests on security breaches within the Strategic plans department before expanding it into other departments.

.

# References

Methodology/Impact

<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>

Novet, J. (2021, March 10). Microsoft's big email hack: What happened, who did it, and why it matters. CNBC. Retrieved August 6, 2022, from <https://www.cnbc.com/2021/03/09/microsoft-exchange-hack-explained.html>

Chance, C. (2021, March 17). Microsoft Data Breach: Risk, regulation and managing a crisis. Clifford Chance. Retrieved August 6, 2022, from <https://www.cliffordchance.com/briefings/2021/03/microsoft-data-breach--risk--regulation-and-managing-a-crisis.html>

ARIA Cybersecurity Solutions. (2021, December 23). Best of 2021 - what we can learn from the 2021 Microsoft Data breach. Security Boulevard. Retrieved August 6, 2022, from <https://securityboulevard.com/2021/12/what-we-can-learn-from-the-2021-microsoft-data-breach/>

GAO. (202AD, January 13). Federal Response to SolarWinds and Microsoft Exchange Incidents. U.S. Government Accountability Office. Retrieved August 5, 2022, from <https://www.gao.gov/assets/gao-22-104746.pdf>

***My Learnings***

At the end of this assignment submission, I have learned a lot about my chosen organization Microsoft. I never thought that the scope of security and its allied industries is such impacting. I feel the presence of this subject in the curriculum should be must, because being an IT people, our most of time got consumed on our laptops. Most of the major and important data is stored in it, and if we aren’t aware about the security and safety of our machines, it’ll really be disastrous. I’ve noticed a very special change in me in the form of awareness for my own devices -  
  
- I never used to lock my laptop when I take a break between my work. I usually leave it as is, now I never leave it without locking even for a min.  
- I’ve a habit of writing things. I used to write my passwords in the notebook. This thing is completely removed from my routine.  
- After I’ve done with this subject, I checked every app on my phone ranging from social media to LinkedIn to Gmail. I applied 2 step factor authentication everywhere. I’ve changed all my passwords. In my views, I didn’t leave a space of mistakes in it.

I learnt a lot about various aspects of information security. I learnt about all the technical terminologies, learn about different acts. As in short, information security is very vital part of study and learning in today’s era. I know various thefts, main key constraints and a lot more. I got confidence that if someday someone asks me or discuss about any of these, I can surely have something to answer on every topic.

I always heard a lot about the breaches within the company in news, media etc. I always like okay, something happened, never try to learn, and get into it like why it happened and how it happened. I was in a kind of impression that it’s okay breaches usually happened. After doing an entire case study on the breaching, I’m really in Awe like this much. I get the whole idea like bow it starts, what are its after-effects both on society and individual organization. And after a long while I literally write something. Being a masters’ student here, all our courses and tests, everything is so consolidated into less writing. And, writing is a work of patience. After writing these elaborated 5 assignments, I would surely say that this squeeze my writing laziness away from me.

Only because of this study can relate when employees used to get fire from the organization, and the reason was that company went in loss. I get to know the logic behind this now, that these breaches are the only reasons of all this movement. It’s interesting to know how hackers hijacks the system, I start thinking that those people are like far more intelligent even from our top Microsoft brains. They have that much knowledge that can break such organization security also, it’s interesting. Sometimes, I would think if this much of energy gets utilized in some productive work, don’t know how many more inventions we can do as a society. It was interesting to read about the Chinese Hafnium group, the strategy they used to take a control. They start from the key source Outlook, powerhouse of most of information.