A Review: Insider Attack in New Normal

Mrs. Divya Chitre, Mr. Ashish Dhoke, Mr. Atish Shriniwar

Abstract: *Technology brings comfort and makes our work easy, but it may come with a cost of your data breach. The Covid-19 crises have fundamentally changed ways of working as many companies are extending the remote working policies that become necessary during the pandemic. Static, network-based security parameters will no longer be sufficient. The security dynamic among users, assets and resources must be protected.*

Keywords:-

Insider attack, new normal, cyber security

Introduction:-

The Covid-19 Pandemic has affected the world and brings massive change to the way we work. Most organizations make a quick transition to remote work force and a more intense focus on serving customers through digital channels.

You've probably heard how Facebook expects half of its workforce to keep working remotely over the next five to ten years. And the twitter told his staff that they can work from home "forever" if they wish.

This is a new model what we're used to. And it's here to stay. But moving to this model is not so simple. While digital transformation and remote accessibility have been increasingly adopted over the past decade. Although there were very few organizations that were prepare to go 'fully remote' and do so practically overnight[2].

Insider Threat(IT) is a Growing cyber security issue. ITs are trusted individuals who have legitimate access to an organizations data or network structure including employees, contractors, vendors and consultants. Insider threats are hard to identify because of their knowledge of the organization and motivation to avoid detection[1].

In the new normal working environment insider threat is one of the most concerning cyber security threat for most of the organizations.

Understanding Insider Attack:-

An insider threat is that the threat of a malicious data attack for a corporation. It usually suggests that the company's security is compromised, and sensitive company information could be stolen and used for personal, malicious, or financial gain.

Unlike an external data breach, an insider threat comes from someone who is inside the corporate and is either malicious or a vulnerable employee [5].

Categorization of insider attacker:-

Malicious insider:

A malicious insider is a person inside your company who exploits the company's vulnerabilities for personal gain. A malicious insider threat may seek an economic reward for the info breach and typically aims to deface the corporate.

A malicious insider is often an individual who came into a corporation (as a contractor, part-time, or full-time employee) for the precise purpose of a knowledge breach. A malicious insider may additionally be a third-party contractor, like a business or partnership [5].

Negligent insider:

A negligent insider is, someone who is tied to a corporation and since of some vulnerability, a malicious attacker was ready to infiltrate privileged accounts within that company. A recent report found that 63% of insider threats were caused by negligent employees.

The negligent insider could be someone who doesn't lock their computer once they walk off from their desk, or it also can be someone who fails to patch a fatal security error in the computer system.[5]

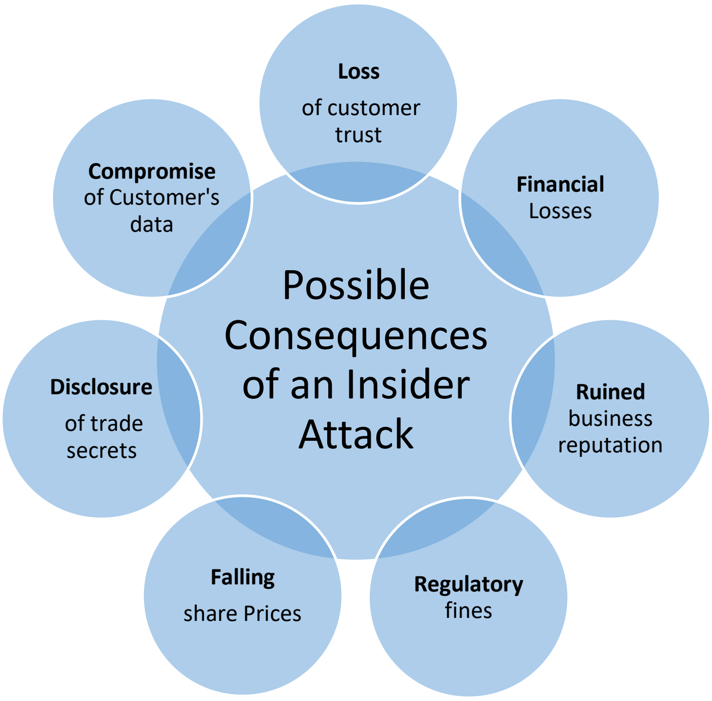
In order to understand how to detect malicious insider actions we have to understand many forms of attack that have been reported like [3]

1) Unauthorized exfiltration, extraction or duplication of data.
2) Data Tampering
3) Misuse of resources for unauthorized activities
4) Intentionally installing malicious software
5) Spoofing and impersonating other users.
6) Destruction and deletion of critical assets

All of these actions can be considered malicious but not every one of them is easy to trace. Some of these actions do leave some trail in some log files, which will help to identify the user but in new normal where actually the attacker is working remotely using organizational resources from not from organizational network but some other public network. It became more challenging for organization to face such concerns.

Organizations used to adapt filed monitoring systems to automatically and reliably detecting and deterring, insider attack but that is too has limited scope in new normal.

The figure below shows major seven consequences of an insider attack. [4]


Possible Consequences of an Insider Attack
Loss of customer trust
Financial Losses
Ruined business reputation
Regulatory fines
Falling share Prices
Disclosure of trade secrets
Compromise of Customer's data

Some more focus on Insider Attack:

Malicious Insiders in Cloud Computing

Nowadays, attacks on the services based on Cloud Computing are more predominant almost in all the sectors and even the big giants are victim of it such as Tesla, Aviva Insurance, Gemalto(SIM card manufactures), Waymo (Google’s selfdrive car company) and many others. Organizations are trying to detect and overcome the threat posed to them by malicious insiders with investing in hardware, software and recent new processes. For all types of attacks, there are some to which we are unware of and rest are known but difficult to detect and counter esp. with respect to the time. So, cloud service providers should enhance their ability and technical security to detect insider malicious attacks through indirect detection.

Organizations assets going to reside on cloud in abundance and as increasingly our lives, enterprises and prosperity may depend upon cloud, we need to understand the threats and scope for the insider attacks and we must be capable to such threats with our technical shields. Everyone need to understand whether the cloud may expose their assets to the increased threats in terms of both – actors and attack surface. So, there should be some mechanism and assessment to tackle with such attacks and hence here we present an assessment of current insider threat definitions and classifications, and their applicability to the cloud. We clarify the nature and state of the insiders with respect to and with reference to the cloud ecosystem. [7]

Symptomatic Insider:

In today's technical era, it's a very common that in every successful business operations and organizations require their employee to access their resources and critical assets such as systems. So, persons working on contract and on roll in any organization are considered as insiders. Knowingly or unknowingly, directly or indirectly, intentionally or unintentionally these insiders may misuse this access in a harmful manner that may affect either the Confidentiality, Integrity, or Availability (CIA) of organisation's Information System Security (ISS). As the critical infrastructure is broader its crux and essence, it covers lot with respect to the infrastructure spectrum compared to critical infrastructure organizations. So, keeping this in mind, assessing the risks of malicious insider threat in critical infrastructure organisations helps in developing a realistic risk assessment methodology for Insider Threats of Information Misuse. So, with an objective to determine and detect the insider threat by computing scores based on a defined metric, this is going to serve as a risk assessment methodology. [6]

INSIDER ESPIONAGE:

According to the Computer Emergency Response Team(CERT) statistics, espionage using organization's information systems (referred as an insider espionage) is the rarest internal IS threat [3].

According to the CERT statistics, espionage using organization's information systems (referred as an insider espionage) is the rarest internal IS threat [3].

This sort of espionage is not defined in the well-known study. Let us describe espionage as an IS threat consisting of the use of insider's organization's information systems for the acquisition, theft, or storage of information for future transfer to external rivals, as defined by the Russian Federation's Criminal Code. The term "industrial espionage" is used when the external party is a competitor. The phrase "international espionage" is used when the external party is a foreign country. The PERSEREC Research Center of the US Department of Defence is another entity that studies insider espionage alongside the CERT. The impact of the parameters of a given insider's position on the threat execution is investigated. The authors present examples of insider espionage in the US government and law enforcement agencies. CERT collaborates with PERSEREC to research and develop the behavioural insider spy model, which is based on PERSEREC's espionage statistics for US government institutions (9 cases of insider espionage). As a priority strategy for forecasting the internal IS threat, system-dynamic modelling can be advised. Because there are no predictive models for specific IS threats among the existing models, the creation of system-dynamic models of internal IS dangers based on insider behaviour and statistical data is clearly in high demand. There is currently no solid quantitative approach for assessing potential internal IS dangers, and existing research solely use behavioural indications for all IS threat types. As a result, it's a good idea to concentrate not only on behavioural, but also technical indicators of internal IS risks, and to use them in mathematical modelling. [8]

Smart Insiders with respect to Internet-of-Things

The Internet-of-Things (IoT) is poised to be one of the most transformative technological concepts since the Internet's inception. According to Gartner, there will be roughly 4.9 billion connected items in use in 2015, and around 25 billion by 2020. While there are numerous benefits to IoT, ranging from healthcare to energy, there are also numerous worries about the security and privacy of this vast network of connected devices. In this position paper, we take a different approach to security and privacy in IoT than previous research by evaluating the influence that IoT could have on the growing problem of insider threat within businesses. Our specific goal is to investigate the extent to which the Internet of Things (IoT) may increase the insider-threat problem for businesses, as well as to examine the variety of new and adapted attack vectors. Insiders' (personal) devices that they carry and use within their employer's organisation are the focus of this article. We present a broad research agenda to stimulate more research in this field as a first step in addressing these concerns. [9]

Unsupervised Learning Approach for Insider Threat

Insider Threat is becoming a major worry as internet becomes increasingly connected. Human analysts face a huge hurdle in detecting insider threats from system records. An insider threat detection and mitigation programme must include an analysis of an organization's log files. Emerging machine learning techniques have a lot of promise for completing complicated and difficult data processing tasks, which will help the next generation of insider threat detection systems. However, with such large volumes of heterogeneous data to evaluate, applying machine learning techniques to such a complicated problem effectively and economically is not easy. [10]

Insider threats vs. outsider threats is a contentious topic, but more firms are recognising the dangers that insiders might offer to a company's data security today than in the past. Outsiders have historically been the perpetrators of data breaches that make the news. Outsider risks are often the dangers that have been dealt with traditional security measures, despite the fact that they can cost hundreds of thousands of dollars (or even millions of dollars). Internal attacks are even more difficult to prevent and identify with one-size-fits-all security methods.

Insider threats are more difficult to prevent for a variety of reasons, one of which is that insiders may not necessarily endanger the company's data security on purpose. Many data breaches caused by insider threats are, in reality, wholly inadvertent. In the modern threat landscape, a holistic approach to security is essential to combat these risks, as well as insider threats originating from those who do have malicious intent. One that adequately addresses not only insider and outsider threats, but also effectively manages both unintentional and intentional threats posed by those within your organisation. [11]

Steps to Effectively Identify Insider Threats

It can be distressing to learn that your company has suffered a severe compromise or data breach as a result of rogue, careless, or compromised insiders. Regardless of the type of insider threat, security teams must have a plan in place to detect and mitigate breaches caused by insiders as soon as possible.

This entails more than just selecting the appropriate security solutions. It's also a matter of establishing and implementing a security programme that brings together people, procedures, and technology to successfully protect against these risks, all while maximising the resources already available.

An insider can be any one or more of the following in many circumstances when users have been given unauthorised access rights:

- Current employee
- Business partner
- Supplier
- Former employee
- Temporary worker
- Service provider
- Contractor
- Outsourcer

Insider assaults aren't always planned. It's also possible that the "insider" is someone whose network credentials have been stolen. It could also be someone who has been "deceived into furthering... adversaries' aims without their knowledge," according to the National Insider Threat Task Force (NITTF).
"The last year and a half presented an increasingly challenging risk environment, with significant adjustments to work and home life, disrupted supply chains, financial insecurity, unreliable or overwhelmed technology capabilities, political and cultural fissures, and serious health concerns," the National Counterintelligence and Security Center (NCSC) says of insider threats.

To properly identify insider threats, follow these five steps:
1. Not all users are the same : All of your users should be grouped by their location, role, and function. Regular activities should also be grouped together. Set access levels for each role type. Before allowing access to corporate assets, vet all individuals, regardless of their function. Make it a habit to audit user groups on a regular basis to ensure that no deviation from allowed access has happened for any given user.

2. Get to know normal: According to the NITTF, "detecting possibly harmful activities" entails "approved... people gathering information from a variety of sources and assessing [it] for clues or suspicious behaviour." However, achieving all of this with minimal human intervention is critical. The good news is that technology exists to automate the process of determining what is typical. UEBA (User Entity and Behavior Analysis) is a wonderful approach for security teams to start learning about how user accounts and assets are commonly used.

Use powerful AI and machine learning to your advantage. UEBA can construct a baseline of your people and assets, and then assign risk scores to them as new activities occur, making it simple for security analysts to create watchlists to monitor those who are most essential or who are exhibiting behaviours that may suggest a threat. Security analysts should be able to use the data evaluated by the system to acquire full visibility into the possible threat and, if necessary, execute decisive automated reaction steps once risky users/assets have been identified.

This guide assists SOC managers in determining where automation can be used in their workflows to alleviate staffing and budget restrictions while maintaining the highest level of security for their organisation.

3. Manage wisely:

The majority of the time, a rogue user is created rather than born. While no management wants their employee to lose interest in the company, it is possible. Holding regular check-ins with your team and paying close attention to those who may be exhibiting peculiar behaviours is critical to spotting a potential rogue insider early on, before they fully convert to the dark side. You and your company can avoid the anguish of a successful rogue insider attack if you respond quickly.

While not a rogue insider, a compromised insider may have unknowingly allowed malware or ransomware to infiltrate their own desktop. "By raising awareness, you may help your [users] avoid social blunders and unintentional injury that can lead to an elevated risk of insider threats," says the NITTF.

Prepare to train all personnel on cybersecurity and to challenge them to stay vigilant on a regular basis. Make sure you cover all of the different sorts of insider threat personas in your training. Maintain their knowledge of current rules, security threats, and best practises.

4. If a user looks like they’re making a move, alert the SOC:

Use appropriate security technologies to keep track of employees and assets. Such visibility can uncover actions that indicate a threat and could have a detrimental impact on the company. Examine any unusual activity that was identified during the risk assessment.

Insider attacks can be easily launched by granting unnecessary access privileges. Audit sensitive information entitlements on a regular basis to ensure that they are only available to authorised people, processes, or devices, as well as to permitted activities and transactions. Reduce the number of devices with such access, especially for employees whose contracts have expired (e.g., temporary employees, contractors, and business partners) or who have been fired. According to the NITTF,“A single indicator may say little,” [But] if taken together with [others], a pattern of concerning behavior may arise that can add up to someone who could pose a threat.”

5. A breach occurred…now what?- Even if you try your hardest, an insider may go rogue. Prepare for a breach by putting in place a sound breach plan. If you prepare for the worst-case situation, you'll be ready to act if and when the insider executes their evil plans.

Create repeatable quick-reaction checklists and response playbooks for your team to use in the event of a major danger. By routinely evaluating risks, security professionals may properly determine where an actual threat exists and devote their time to addressing it rather than chasing false positives.

An insider breach has far-reaching consequences for a business, going beyond the loss of data or damage to systems. After such a catastrophe, trust between employees, supervisors, customers, and partners can swiftly evaporate. Building an insider threat programme that transforms your reactive team into a highly effective, proactive one requires a methodical, step-by-step approach. [12]

An insider threat is a current or former employee, contractor, business associate, or other person within a company who has access to sensitive data or IT systems and could harm the company. Policies, processes, and technology that help avoid or mitigate the damage caused by insider threats can be used to manage insider threats. These best practices to prevent insider threats will help you minimize the risk of your sensitive data being compromised.

How to minimize the risk of insider threats:

- **Perform enterprise-wide risk assessments:** Know your most valuable assets, their vulnerabilities, and the dangers that may damage them. Insider threats provide a variety of dangers, so make sure to account for them. Then, based on the risk priority, prioritise the risks and improve your IT security infrastructure as needed. See these IT risk assessment best practises for additional information.

- **Clearly document and consistently enforce policies and controls –**

Each piece of security software or appliance must have its own management policy and configuration documentation. Work closely with your HR department to develop policies that cover nearly every employee interaction with the IT environment.

- General data protection regulations
- An incident response policy
- A third-party access policy
- An account management policy
- A user monitoring policy
- A password management policy

Your legal department must verify all of these policies, and your CEO must sign them. If a policy is broken and your investigation uncovers the perpetrator, it's critical to specify what measures will be performed and what punishments will be imposed.

- **Establish physical security in the work environment.:** Employ a competent security staff that will adhere to your security guidelines to the letter. They should keep suspicious people out of places where sensitive IT equipment is kept (such as server rooms or rooms with switch racks). Have them check everyone for IT devices at the entrance and document anything that deviates from the security baseline. Instruct everyone to turn off their phone cameras when inside the facility. Remember to secure all server rooms.

- **Implement security software and appliances:-**

Deploy and properly configure the following software:

✓ - Active Directory
✓ - Endpoint protection system
✓ - Intrusion prevention system
✓ - Intrusion detection system
✓ - Web filtering solution

- ✓ - Traffic monitoring software
- ✓ - Spam filter
- ✓ - Privileged access management system
- ✓ - Encryption software
- ✓ - Password management policy and system with at least two-factor authentication
- ✓ - Call manager
- ✓ - Data loss prevention system
- ✓ Enable mailbox journaling on your Exchange Server, preferably with e-discovery software installed.

• **Create and follow strict password and account management policies and procedures.** All of your users should log in with credentials that are unique to them; each user should have their own login ID and password. To correctly implement these regulations, use password best practises and account management best practises.

• Remote access from all endpoints, including mobile devices, is monitored and controlled. Deploy wireless intrusion detection and prevention systems, as well as a mobile data interception system, and configure them effectively. Examine whether employees still require remote access and/or a mobile device on a regular basis. When an employee leaves the company, make sure that all remote access is turned off.

- **Harden network perimeter security.** Make sure your firewall is set up correctly. All hosts and ports should be blacklisted, and just the ones you need should be whitelisted. Create a DMZ zone. Do not use VPN or FTP, and make sure no essential systems are connected to the internet directly. To restrict users from freely accessing the network, divide the network into VLANs established by business units. Establish a regular network device behaviour baseline.

- **Enable surveillance**. Video cameras with motion sensors and night vision are used to keep an eye on all of your company's important facilities. Enable session screen-capture technologies on all privileged users' essential servers and devices.

- **Enforce separation of duties and least privilege.** Demand two users' permission to copy data to removable media (and consider requiring the data to be encrypted); require two system administrators' permission to delete essential data or make configuration changes. Set up role-based access restrictions and Group Policy to prohibit employees from accessing information or services that aren't necessary for their professions, and make sure that administrators have separate, distinct accounts for administrative and non-administrative tasks.

- **Recycle your old hardware and documentation properly.** Before destroying or recycling a disc drive, make sure it has been entirely erased and that the data is no longer recoverable. Old hard discs and other IT devices containing sensitive data should be physically destroyed; appoint a dedicated IT engineer to oversee the procedure.

- **Use a log correlation engine or security information and event management system (SIEM) to log, monitor and audit employee actions.** Keep all of your device logs for several years to allow for incident investigation and easy access to historical information. Implement software for log management and change auditing to provide enterprise-wide insight. Every major change made to your IT infrastructure should be tracked and documented; for example, audit permissions on a regular basis to avoid privilege creep.

- **Implement secure backup, archiving and recovery processes:** Implement and configure archiving for files and mailboxes. Create a backup policy that mandates a full backup at least once a month and implement and install a backup system. Create and test a catastrophe recovery plan as well. Consider the possibility that a malicious insider is engaged by a trustworthy business partner if part of the backup and recovery process is outsourced.

- **Identify risky actors and respond promptly to suspicious behavior.:-** Follow your incident response policy when it comes to monitoring your security systems and responding to suspicious or disruptive conduct. Remote access to the organization's infrastructure should be monitored and controlled. Configure alerting on all essential systems and events, and make sure the alerts send you repeated notifications. You can more effectively spot bad actors by deploying user behaviour analytics (UBA) solutions.

• **For any cloud services, define clear security agreements, including access restrictions and monitoring capabilities.** Cloud service providers expand an organization's network perimeter and expose malicious insiders to new attack vectors. Perform a risk assessment of the data you intend to outsource to a cloud service provider, especially if it contains sensitive information such as intellectual property or financial information. Ascertain that the service provider poses an acceptable degree of risk and that their security policies are comparable to or better than your own. Recognize how the service provider handles data security. Determine who is responsible for restricting logical and physical access to organisational assets in the cloud and confirm their identity. All modifications made in the cloud should be monitored and controlled.

• **Create a comprehensive protocol for terminating employees.** Work with HR to build a solid user termination policy to safeguard your company from former employees both legally and technologically. Follow proper procedures for terminating users.

• **Include insider threat knowledge in all employees' regular security training:** Before granting access to any computer system, all new workers and contractors should be trained on security awareness. Prepare your staff for social engineering assaults, active-shooter situations, and sensitive data left out in the open by training and testing them. Perform your own phishing assaults on their mailboxes, for example, or conduct social engineering attacks over the phone. If somebody fails these tests, make sure they receive additional training. Encourage employees to report security vulnerabilities and educate them on how they may help lessen the threat of insiders. Consider providing rewards to individuals who adhere to security best practises. Accept that you won't be able to entirely remove the insider threat, and invest in an insider threat detection system. [13]

Identifying risk & Securing data

The Digital response to Covid-19 crises has also created new security vulnerabilities. Attackers seek to take advantage of the gaps opened when telecommuting employees use insecure devices and networks. Throughout the crises the cyber security leaders respond with attention on three activities as companies shifted to new processes and technologies. [2]

- Identifying and eliminating hot spots
- Fixing and mopping up operations

- Secure incremental gains.

Cyber security teams can fortify initial incremental gains; they'll even have to reevaluate prior efforts as new technologies or processes are introduced.

Assessing and demolition hot spots [2]

As employees began performing from range in less secure environment and with less secure personal equipment. the safety teams need to fix immediate operational process, and technology gaps associated with the pandemic induced response and shift to remote working.

The company's teams leaders need to address training gaps, lead virtual all-hands meetings, and turn workers to take care of digital hygiene, like patching their computers and updating mobile software.

For example, an outsized financial company can support its remote workforce swiftly by distributing Wyse-thin-client terminals to all or any call-center staff for secure remote connections.

Some initial issues with bandwidth and performance were resolved by performing virtual-private-network (VPN) split tunneling also as upgrading firewall infrastructure.

In another scenario, a bank adjusted several security polices in response to the Covid-19 crises. the corporate ran more frequent awareness campaigns.[2]

• **Fixing and mopping up operations**[2]

In earlier phase of pandemic, many companies were forced to simply accept new risks, including reduced control standards, to stay operations going. As employees and customers became familiar with the changes, companies evaluated theses residual risks and tightened controls.

For example adapting various cloud-based collaborations tools, an outsized telecommunications provider accelerated the rollout of latest cloud-aware monitoring capabilities within its security-incident and event-monitoring (SEIM) tool.

Additionally, it reviewed its security and monitoring controls for third-party vendors to make sure that restrictions that had been temporarily lifted were replace in situ.

• **Protect security gains**[2]

As employees became comfortable performing from home, companies began standardizing procedures for remote work environments and explored technologies to scale back long-term risk.

Some companies introduced stronger consumer-security and fraud prevention controls. A bank expanded its biometric and device-based authentication for sensitive customer transactions across new, critical digital channels.

The bank also accelerated implementation of artificial intelligence-based fraud detection platform. As a result, incoming transactions might be analyzed in 300 milliseconds or less, compared with the hours this took before.

In an instance, a social insurance company updated policies and procedures to institutionalize the safety controls required during a remote work environment.

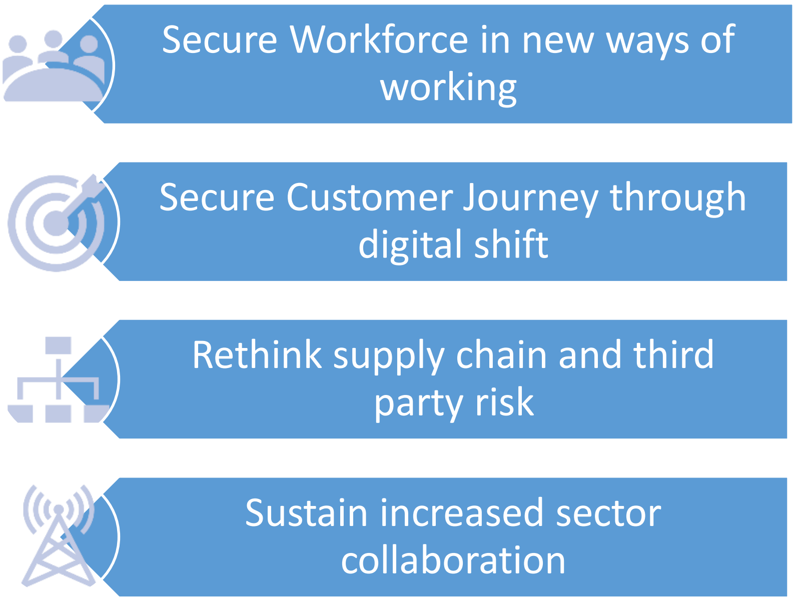
It established a replacement policy and standard to migrate the danger of cybercriminals infiltrating the network through unsecure home printers. apart from approved business cases, all employees were restricted from printing remotely through personal printing devices.

• **Anticipating subsequent normal**[2]

As cyber security leaders are increasingly getting a handle on the primary stage of the pandemic, The CISOs (Chief information security officer) are now shifting to anticipating how the business environment are going to be suffering from new conditions.

They are adapting to include theses expectations of subsequent new normal into both current cyber securities activities and long-term cyber risk strategies.

To secure subsequent normal business environment for value creation and growth, cyber security leaders will got to take effective action in four priority areas.


Secure Workforce in new ways of working
Secure Customer Journey through digital shift
Rethink supply chain and third party risk
Sustain increased sector collaboration

[2]

- **Secure the Workforce in new ways working**[2]

The Covid-19 crisis has fundamentally changed ways of working, as many companies are extending the remote-working polices that became necessary during the pandemic.

Organizations could emphasize the subsequent cyber security initiatives:

1. Dynamic security: Static, network based security parameters will not be sufficient. The dynamic security among users, assets and resources must be the new focus.[2]

Protect end point assets and utilize real-time anomaly detection with end-point-detection and response systems. Protect data assets through enhanced block-mode-data-loss-prevention tools and utilize a model of preapproved sites as a default for external access.[2]

2. Cloud based tools and infrastructure: the necessity for greater agility and adaptability will accelerate the utilization of cloud. Restrict localized data storage for the remote workforce and transform end-user infrastructure through increased adoption of virtual desktop and desktop as service.[2]

Support the increasing shift to a multi-cloud environment and cloud-based services through access controls at points where policy is set and enforced; implement a cloud-access-security broker.[2]

3. Contact aware workforce privacy: Heightened security would require new agreements with employees. think about the implications of workforce privacy and employee consent to introduce contact-aware tools, like contact tracing and temperature taking, within the workplace.[2]

4. Remote Cyber security operating model and talent strategy: The new ways of working will have implications across the enterprise. Rethink the cyber security operating model and continually plans for physical location-constrained operations, including automation opportunities.[2]

- **Conclusion**

The Covid-19 pandemic has changed consumer and business behaviour in dramatic ways. Cybersecurity team have generally performed far above expectations in fulfilling a dual mission of addressing new risks and anticipating the next normal.

Insider threat detection and prevention is challenging in new normal but it is research filed ripe with various opportunities for approaches and methodologies. It is challenging to build effective and highly accurate automated monitoring and analysis system. But with the help of recent techniques like machine learning and artificial intelligence it is not impossible.

Acknowlagement:-

This research review work is majorly based on the findings from article published on "*A dual cybersecurity mindset for the next normal*" *in* https://www.mckinsey.com/

References :

1. Matthews, G., Reinerman-Jones, L., Wohleber, R., & Ortiz, E. (2017, September). Eye tracking metrics for insider threat detection in a simulated work environment. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 61, No. 1, pp. 202-206). Sage CA: Los Angeles, CA: SAGE Publications.
2. *https://www.mckinsey.com/ A dual cybersecurity mindset for the next normal, July 7, 2020 | Article*
3. *Salem, M. B., Hershkop, S., & Stolfo, S. J. (2008). A survey of insider attack detection research. Insider Attack and Cyber Security, 69-90.*
4. *www.ekransystems.com*
5. *https://www.softactivity.com/insider-threat-detection guide*
6. Joris Ikany and Husin Jazri, Department of Computer Science Namibia University of Science and Technology, "Windhoek, Namibia A Symptomatic Framework to Predict the Risk of Insider Threats"
7. Adrian Duncan, Sadie Creese, Michael Goldsmith, Department of Computer Science, University of Oxford, UK, "A Combined Attack-Tree and Kill-Chain Approach to Designing Attack-Detection Strategies for Malicious Insiders in Cloud Computing"

8. Anton Zaytsev, Anatoly Malyuk and Natalia Miloslavskaya National Research Nuclear University MEPhI (Moscow Engineering Physics Institute) Moscow, Russia, “Critical Analysis in the Research Area of Insider Threats”
9. Jason R.C. Nurse, Arnau Erola, Ioannis Agrafiotis, Michael Goldsmith, Sadie Creese Cyber Security Centre, Department of Computer Science, University of Oxford, UK, “Smart Insiders: Exploring the Threat from Insiders using the Internet-of-Things”
10. Maryam Aldairi, Leila Karimi, James Joshi, School of Computing and Information, University of Pittsburgh, USA, “A Trust Aware Unsupervised Learning Approach for Insider Threat Detection”
11. https://digitalguardian.com/blog/insider-outsider-data-security-threats
12. https://www.exabeam.com/information-security/five-steps-to-effectively-identify-insider-threats/
13. https://www.netwrix.com/Insider_Threat_Prevention_Best_Practices.html