Adapting to the New Normal: Management of Security Policy of Organizations during the Pandemic

Bhanuja MK[1], Gopika E[2]

[1]*bhanujamk[at]gmail.com*

[2]*gopikaaessoudasse[at]gmail.com*

Abstract: ***The COVID-19 epidemic has caused substantial changes in the way organizations function, including corporate security standards. Organizations are confronting new problems in securing their networks and protecting their data as remote work becomes the norm and the threat ecosystem develops fast. This paper will look into how the pandemic has affected corporate security policy and the changes that organizations are undertaking to adapt to the new normal.***

Keywords: Organizational Security policy, Cyber security, Pandemic

1. Introduction

The security of an organization's assets and information technology infrastructure is essential for its success. The recent pandemic has had a huge impact on corporate worldwide, requiring significant changes to their business functions and security policies. As work from home became the new normal, organisation's introduced new infrastructure and technologies to keep working smoothly. One of the most significant changes that companies implemented is in their remote access policy. Organizations must maintain the security of their remote work infrastructure when employees work from home. This involves safeguarding home networks and ensuring that employees access business data over secure VPNs. Companies must also implement tight access controls to guarantee that sensitive data is only accessed by authorized.

Organizations must educate their employees about cyber security risks and appropriate practices. Employees must be educated to recognize and report phishing attacks, and also to use strong passwords and secure online behaviour. Employees who are not properly trained may become the weakest link in an organization's cyber-security protection. The requirement for data backup and recovery strategies is another significant need in security policy during the pandemic. With the rise in ransomware attacks, businesses must be prepared to quickly restore their data if an attack occurs. Data backup and recovery methods should be verified on a regular basis to verify that they are effective and can be performed on time. Organizations must also keep their security policies up to date with the most recent security patches and upgrades. This involves upgrading software and systems on a regular basis to fix vulnerabilities and assure their security. Organizations must also utilize multi-factor authentication to guarantee that only authorized individuals have access to sensitive data. Organizations must check their networks and systems for possible security risks on a frequent basis. This involves keeping an eye out for unusual network activities like suspect logins or data transfers. Companies should also undertake security audits on a regular basis to discover weaknesses and opportunities for improvement.

2. Literature Review

In response to the pandemic, many organizations have moved to remote work, which has expanded the usage of internet tools and apps, increasing the danger of cyber-attacks [1] [2]. According to an IBM study, there would be a 6, 000% rise in COVID-19-related spam emails in April 2020. (IBM Security, 2020) [1]. In recent weeks, networks and devices have become vastly more crucial for enterprises. Yet, the majority of these organization's lacked the Technology infrastructure to allow their workers to work from home. Secure access to systems and secure remote access capabilities were important constraints in this league [1]. In the age of software-based applications, the impact of the COVID-19 pandemic is not insignificant. Its impact should be evaluated and quantified to provide a complete grasp of how much this pandemic has damaged software-based systems and their security. The impact of COVID-19 on software systems and their industry has been recognized and classed in order to highlight the software systems and applications that have been seriously impacted.

Organizations have a number of issues when it comes to maintaining secure operations when working remotely. This covers staff training and awareness issues, as well as the necessity to safeguard remote access to organizational systems. As a result, demand for cybersecurity services like virtual private networks (VPNs) and security information and event management (SIEM) systems have skyrocketed. Organizations must make particular improvements to their cybersecurity programs in response to the pandemic. Increased investment in cybersecurity technology and services like as cloud-based security solutions, endpoint protection, and security analytics are among these trends. Furthermore, many businesses have enhanced their cybersecurity training and awareness programs to educate employees about the potential hazards connected with remote work [2] [3]. The rising use of remote work has presented new issues for IT departments, such as managing increased connectivity demand and supporting new devices and apps. In this scenario, IT and cybersecurity teams must collaborate to ensure that security remains a top priority. The pandemic has emphasized the value of cloud-based security solutions, which may give more visibility and control over remote devices and networks [3]. Investment in cybersecurity technology and services, including as cloud-based security solutions, endpoint protection, and security analytics, is increasing. Furthermore, many businesses have enhanced their cybersecurity training and awareness programs to educate employees about the potential hazards connected with remote work.

Employees in the business environment must adhere to a set of cyber hygiene guidelines. Strong passwords, multifactor authentication, secure connections, and frequent software upgrades are examples of these techniques. During the outbreak of corona and after adopting the new normal, there is an increase in several security attacks. During the Covid-19 outbreak, scammers and phishing were the most well-known and effective attacks, although there are other sorts of scams and phishing. Utilizing email, SMS, or voice to target people and systems that entice users by using coronavirus or Covid-19 as a keyword [7]. As the platform’s utilization expanded during Covid 19, so did the number of security problems. There have been allegations of "Zoom bombings, " in which unauthorized individuals enter Zoom meetings and disrupt them with objectionable information [11]. Zoom has issued a number of security patches to address these problems. These enhancements include the option to report people, delete meeting attendees, and restrict screen sharing to the host. Zoom has also added more stringent password restrictions, as well as the possibility for two-factor authentication.

Cybercriminals have been exploiting COVID-19-related baits in their phishing emails, according to TrendMicro’s study, to deceive victims into clicking on harmful links or installing malware [10]. The emails purport to provide COVID-19-related information or items, such as face masks or hand sanitisers, but instead direct recipients to malware websites or download links. According to TrendMicro’s study, fraudsters were also utilizing COVID-19-related terms to increase their presence in search engine results. They were, for example, creating bogus COVID-19 news sites or blogs that contained harmful links or malware downloads. Moreover, cybercriminals were disguising their attacks behind the COVID-19 pandemic. For example, they were initiating ransomware assaults on healthcare facilities that were already dealing with the pandemic. These assaults might interrupt critical healthcare services and harm people’s lives.

Many policies are in place to safeguard the confidentiality integrity and availability of company data and systems. However, the effectiveness of these regulations can be impacted by a variety of factors, including telecommuters’ individual qualities, the security infrastructure in place, and the culture and management of the business. Employees’ personal characteristics, such as their attitude towards security and level of security knowledge, can have a significant impact on the success of corporate security measures. Employees that are casual about security or are unaware of the hazards, may unwittingly expose business information to unauthorized persons.

3. Organisational Security Policies during Pandemic

The Pandemic has also substantial influence on organizational security policies, with many businesses being forced to adjust their policies to handle the pandemic’s new cybersecurity threats. The migration to remote work arrangements has had a significant impact. Organizations have had to re-evaluate their security practices to guarantee that workers can operate safely from distant locations since many employees increasingly work from home. To guard against cyber risks, regulations such as the usage of virtual private networks (VPNs), multifactor authentication, and secure file-sharing protocols must be introduced. Organizations have had to modify their security practices, in addition to technological measures, to manage the growing risk of phishing attempts and other cyber threats. This includes encouraging staff to practice basic cyber-security hygiene, such as using strong and unique passwords, being careful when reading emails or clicking on links, and frequently upgrading software and systems. Another effect of the pandemic on corporate security policy has been the demand to assure regulatory compliance. Several firms have had to immediately adapt to new data privacy and cyber-security policies and standards in order to be compliant while functioning in the midst of the pandemic. The pandemic has also highlighted the importance of good crisis management and incident response strategies for organisations.

Organizations must be prepared to respond quickly and effectively to any security breaches that may occur, given the increased risk of cyber-attacks and other security events. The pandemic has highlighted the need to have effective communication channels in place to ensure that employees are informed of any changes to security rules and standards. Good communication is critical to ensuring that workers understand the importance of cyber-security and the activities they must take to secure company data and systems. In the wide range of priorities, organisations need to be focused on the following areas:

a) Incident Response:

As employees are working from a very different environment during the pandemic, it is important to make sure to modify the incident response plans are in place to make the working effective and secure. Organizations need to revise their incident response plan to reflect the updated operating conditions. This involves recognizing risks and vulnerabilities that develop as a result of remote operations, such as increased phishing attempts and data breaches. Organizations must also implement communication protocols to guarantee that all workers may quickly report security incidents. Another crucial step that firms may take is to ensure that their incident response team is provided with the tools and resources needed to function remotely. This involves granting remote access to critical systems and data, as well as establishing secure communication channels to guarantee that the incident response team can work efficiently together. Organizations must also test their incident response policies on a regular basis to verify that they are effective and can be deployed remotely. Simulated security events are used to assess the performance of the incident response team and the organization's communication protocols. Frequent testing also assists firms in identifying areas for improvement and updating their incident response strategy. Organizations must also verify that their incident response plans are in line with relevant regulations and industry standards. This involves ensuring that incident response protocols comply with data protection laws and industry standards. Organizations must also run an ongoing monitoring program to detect and respond to security problems. Monitoring network traffic, documenting events, and conducting frequent vulnerability assessments to detect possible security issues are all part of this. Organizations can detect and respond to security events before they become critical by continually monitoring their systems.

b) Remote Access and Endpoint Security:

The COVID-19 pandemic has pushed organisations to implement remote work policies, increasing the usage of remote access technologies and endpoints. As a result, the danger of cybersecurity threats has grown, since remote access technologies and endpoints are exposed to various cyber threats. One of the most difficult aspects of remote work is the demand for secure remote access. Workers require remote access to many services and data in order to carry out their responsibilities. Yet, if not adequately secured, remote access might pose a security concern. Remote access should be restricted to those who need it and should be secured using strong passwords, two-factor authentication, and other safeguards. Endpoint security is another vital part of remote work. Endpoint security becomes increasingly important when employees use their devices to access the organization's network and data. Endpoint security entails protecting the devices that connect to the network, such as laptops, desktop computers, and mobile devices. Antivirus software, firewalls, and other security measures must be installed on all devices by organisations. Endpoint testing is one method through which firms may verify the security of their remote workers. Endpoint testing includes evaluating the security of devices that connect to an organization's network. This may be accomplished using a variety of approaches, such as vulnerability scanning, penetration testing, and risk assessments. Endpoint testing can assist businesses in identifying vulnerabilities and security concerns and mitigating them. Organizations must educate their staff on the significance of cyber security in addition to endpoint testing. Those who work from home are more susceptible to cyber security dangers like phishing schemes and malware assaults. Organizations must teach their staff, how to recognize and prevent these dangers, as well as what to do if they are the victim of a cyber-security assault. Firms must have a comprehensive incident response strategy in place to deal with any potential cyber-security problems. This strategy should include what to do in the case of a security breach, including who to call and what procedures to take. It should also contain processes for remote workers to follow if a security problem occurs.

c) Employee Awareness:

The first and most important communication that organisations must convey to their workers is the significance of safeguarding sensitive information. Workers who work from home must be aware of the need of safeguarding sensitive information, such as customer data, financial information, and intellectual property. Employees must be informed on the sorts of information they handle, the dangers of releasing that information, and the impacts of a breach. Employees must be educated on the many sorts of cyber-security risks and how to detect them. Risks including phishing scams, malware, and ransomware attacks can damage an organization's sensitive information, and employees must be prepared to recognize and report such attacks. Employees must be educated on how to utilize secure communication technologies. Employees working from home may need to use numerous communication methods such as email, instant messaging, and video conferencing. To avoid unwanted access to sensitive information, these technologies must be secure. Workers must be educated on how to use these technologies safely, including the use of strong passwords, encryption, and two-factor authentication. Next, employees must be educated on how to use personal gadgets properly. Employees who work remotely may use their personal devices to access business information. These gadgets, however, may not be as safe as company-issued devices, and employees must be aware of the security risks involved with using personal devices. Workers must be educated on the significance of installing security software, routinely upgrading their devices, and protecting their devices with secure passwords. Workers must be made aware of the need for frequent backups. Data loss can be an enormous threat to an organization's information security. Workers must be informed of the need to frequently back up their data as well as the various means of data backup, such as cloud-based backups or external hard drives. Lastly, employees must be educated on the necessity of immediately reporting security occurrences. Employees must be informed of the actions to follow in the case of a security breach, including who to call and what information to supply. Companies must have clear incident reporting protocols in place and ensure that their staff are aware of them.

d) Security Monitoring:

The first step for organisations should be a proper risk assessment of their expanding operational environment. This study should involve a look at the numerous security risks connected with remote work, such as phishing scams, malware, and ransomware assaults. The risk assessment should also take into account the many devices and communication platforms that employees use, as well as the possible dangers connected with each. Organizations may identify possible security weaknesses and prioritise their security efforts by completing a complete risk assessment. The second step is to set up a strong security monitoring program. The program should incorporate continuous network traffic, user activity, and system log monitoring. This monitoring should be carried out with the use of security information and event management (SIEM) solutions, which can provide real-time notifications to possible security problems. SIEM technologies may also analyze user behaviour, finding any odd or suspicious behaviour that may signal a security breach. Establishing a vulnerability management program comes with another step in this category. Vulnerability management includes identifying, assessing, and resolving security vulnerabilities in an organization's systems and applications. Employees who operate remotely may utilize a variety of devices and communication technologies that are not always up to current with the latest security fixes. A vulnerability management program can discover these vulnerabilities and prioritise their treatment depending on the risk they represent to sensitive information inside the company. Organizations should undertake frequent security audits to ensure the effectiveness of their security monitoring capabilities. Potential weaknesses in the security monitoring program, remote access management system, security awareness training, vulnerability management, and incident response protocols can all be identified during a security audit. Organizations may guarantee that their security monitoring capabilities remain effective in the expanded operational environment by conducting frequent security audits.

e) Security Service Vendors:

The first stage is to determine the criticality of each security service vendor. Organizations should identify and prioritise collaboration with suppliers who provide key security services. Network security, endpoint security, and identity and access management are examples of critical security services. Organizations may prioritise their efforts and spend resources accordingly by identifying essential vendors. The second stage is to develop a communication strategy with security service providers. Regular check-ins with suppliers to discuss the effects of COVID-19 on their operations and services should be part of the communication strategy. Companies should also have a strategy for communicating security threat and vulnerability information and updates. Organizations can better understand the effects of COVID-19 on their operations by keeping open contact with security service suppliers. The third phase is to examine the security supply chain's risk. The risk assessment should take into account the possible COVID-19 consequences on each security service vendor, such as supply chain interruptions, staff shortages, and changes in service delivery. Companies should also examine the potential consequences of a security service vendor's inability to offer vital services. Organizations may identify possible vulnerabilities in their security supply chain and take actions to reduce those risks by performing a risk assessment. Organizations should assess each vendor's security controls to verify they comply with the organization's security policies and requirements. Access restrictions, encryption, data protection, and incident response skills should all be considered throughout the examination. Organizations may verify that they are obtaining the essential security services to secure their sensitive information by analyzing the security controls of security service suppliers. Preparing an SLA should outline the vendor's services, the expected level of service, and the penalties for failing to satisfy the SLA. Provisions for reporting security events, breach notifications, and service-level credits should also be included in the SLA. Organizations may guarantee that they obtain essential security services from their suppliers by creating SLAs and holding them accountable for fulfilling the agreed upon service levels. Organizations should undertake security audits of their security supply chain on a regular basis. Security audits can detect possible risks and gaps in the security supply chain and make recommendations for improvement. Regular security audits can also ensure that security service vendors are meeting their contract agreements according to SLA and providing the security services required to protect the organization's sensitive data.

4. Conclusion

The COVID-19 pandemic has caused organizations to adjust to a new normal, which includes remote work, increasing reliance on digital technology, and higher security threats. Security policy management is more important than ever to secure the confidentiality, integrity, and availability of company information and systems. Organizations have had to review their security policies and architecture as they have migrated to remote work in order to safeguard their assets from new and developing threats. The pandemic has underlined the significance of employee training and awareness initiatives in ensuring that employees understand the risks of remote work and follow to security rules and best practices. The pandemic has highlighted the importance of corporations implementing a comprehensive security policy and continuously evaluating and adapting it to handle new threats and changing situations. so that they can function securely and effectively.

References

[1] Mohammed Baz1, Hosam Alhakami, Impact of COVID-19 Pandemic: A Cybersecurity Perspective

[2] McKinsey & Company, "COVID-19 Crisis Shifts Cybersecurity Priorities and Budgets. " 2020 [Online]. Available: https: //www.mckinsey. com/business-functions/risk/ourinsights/covid-

[3] 19-crisis-shifts-cybersecuritypriorities-and-budgets#

[4] TCS Worldwide, "How COVID-19 is Dramatically Changing Cybersecurity. " 2020. [Online]. Available: https: // www.tcs. com/perspectives/articles/how-covid-19-is-dramatically changing-cybersecurity.

[5] Arnold Mashud Abukari and Edem Kwedzo Bankas, Some Cyber Security Hygienic Protocols For Teleworkers In Covid-19 Pandemic Period And Beyond.

[6] Cyber security threats during the pandemic Hassan Aljohani

[7] Factors Affecting Corporate Security Policy Effectiveness in Telecommuting Chulwon Lee 1 and Kyungho Lee

[8] Organizational Security Policy and Management during Covid-19 Ayla Al shammari, Richard Rabin Maiti and Bennet Hammer

[9] Ahmad Kamal, A. H.; Yi Yen, C. C.; Ping, M. H.; Zahra, F. Cybersecurity Issues and Challenges during Covid-19 Pandemic. [Online] https: //www.preprints. org/manuscript/202009.0249/v1/dow nload

[10] J. G. Ronquillo, J. W. Erik, K. Cwikla, R. Szymanski and C. Levy, "Health IT, hacking, and cybersecurity: National trends in data breaches of protected health

information, ” JAMIA Open, vol.1, no.1, pp.15–19, 2018.

[11] "Developing Story: COVID-19 Used in Malicious Campaigns-", Trend Micro, 2020. [Online]. Available: https: //www.trendmicro. com/vinfo/us/security/news/cybercrime-and digital-threats/coronavirus-used-in-spammalware-file-names-and-malicious-domains.

[12] K. Paul, "Zoom releases security updates in response to 'Zoom-bombings'", The Guardian, 2020. [Online]. Available: https: //www.theguardian. com/technology/2020/apr/23/zoom-update-security-encryption-bombing. [Accessed: 06-Jul-2020].