IJARETY

International Journal of Advanced Research in Education and TechnologY *(IJARETY)*

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 4.933| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 9, Issue 2, March - April 2022 ||

DOI:10.15680/IJARETY.2022.0902019

Securing the Distributed Workforce: A Framework for Enterprise Cybersecurity in the Post-COVID Era

Govindarajan Lakshmikanthan[#1], Sreejith Sreekandan Nair[#2]

Independent Researcher, Leading Financial Firm, Texas, USA[#1, #2]

ABSTRACT: COVID-19 is the new standard for forced changes in the workforce, forcing the adoption of remote and hybrid work environments globally. It was in the period of this rapid adoption of distributed work environments that new opportunities for flexibility and productivity were opened up, but fundamental weaknesses of conventional notions of cybersecurity were unveiled. As employees connect to company networks from a plethora of different places and different types of devices, situations were complex at the corporate level to ensure that security measures remained adequately stringent. New threats came to the fore, such as endpoint devices that have added more risks since they were unsecured home networks and the use of personal devices (BYOD). All these changes raised the concern of a new security model for the enterprise whereby new, fresh methods of dealing with the issue emphasize strategies which accommodate the change, and we affirm the need to put in place security architecture that will help protect the valuable enterprise assets. This paper looks at the new challenges of defending the widely dispersed employee base and offers an integrated solution for protecting the modern enterprise. To address risks inherent in the current working environments, the framework seeks to address concerns of identity-centric security and zero-trust and apply emerging technologies in threat intelligence. Using knowledge acquired by current cyber assaults and actual programs, the research provides numerous substantial approaches to countering current and potential cyber threats. The research also identifies the main recommendations for enterprises operating in this environment, including the need for active management of risks and constant adaptation to threats.

KEYWORDS: Distributed workforce, Cybersecurity, Post-COVID, Zero Trust, Remote Work, Identity-Centric Security, Threat Intelligence.

I. INTRODUCTION

Outsourcing was greatly affected by the COVID-19 global outbreak since it propelled the decentralization of the workforce and the shift to independent working at an incomparably higher rate. [1-3] Organizations were forced to change rapidly to avoid disrupting their operations and adopt technology such as digital tools and cloud solutions. Although this change opened up new layers of possibility for flexibility, deftness, cost optimization, and access to global talent, it also underscored profound weaknesses in the conventional enterprise security perimeters. Previous gateway security mechanisms initially developed for a traditional network topology in which the primary office location served as the central workplace were ineffective for a decentralized workforce who accessed confidential information on any device from any location. This transition came with the following new hurdles: securing endpoints, identity access control across the new network and the risks inherent in human errors, especially in decentralized environments. With the increase of attack surfaces, organizations are more vulnerable to being trapped in phishing attacks, ransomware and other advanced forms of cyber threats. A report by Cybersecurity Ventures also showed that there has been a 300% increase in cyberattacks in the course of the pandemic, with most of them being exploited on emerging weaknesses in remote working. They argues that as organizations continue to depend on easily accessible and knitted platforms, there is a need to embrace a scalable, robust and adaptable cybersecurity model. Such threats are dynamic, meaning that organizations' security requires using new technologies in collaboration with efficient risk management initiatives.

Problem Statement

New working models, such as those that imply remote and hybrid work schemes, have drastically changed the cybersecurity threat landscape for organizations. Contrary to typical offices, providing This decentralization has increased the opportunities for attackers, and endpoints laptops, smartphones, and tablets become primary targets. Also, employees who work remotely connect through their personal networks and devices, which have significantly less

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 4.933| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 9, Issue 2, March - April 2022 ||

DOI:10.15680/IJARETY.2022.0902019

protection than Fortune 500 corporations. Other vulnerabilities include improper staff training and users' high susceptibility to phishing attacks. The worst part is that as cybercriminals take advantage of these loopholes, organizations witness a rising number of apprehensions such as data leakage, ransomware attacks, and the like that drag thousands of dollars and extremely damage brand image. Security mitigations like the traditional security approaches that seek to protect the perimeters of a computer system have not been effective in addressing these. Businesses need to start planning their cybersecurity anew to factor in solutions such as zero-trust architecture, identity-security-focused techniques, and threats intelligence. A future-proof cybersecurity solution is crucial when protecting dispersed employees and maintaining organizational functionality and data protection.

Objectives

The goal of this paper is to explain cybersecurity issues related to distributed work and design a framework that meets these requirements. The specific objectives of this research include:

- Towards Building a Framework for Securing Distributed Workforces: This includes placing a cybersecurity structure that encompasses the current technologies, including zero-trust security, identity and access management and advanced threat intelligence systems. As such, the framework is designed to be contextually transportable and replicable as companies advance across the globe.

- An evaluation of key threats that may occur within various works from home scenarios: These issues include endpoint security, poorly protected networks and phishing schemes endemic to remote working environments will also be drawn out in the study. As part of this assessment, actual examples of occurrences and incidents will be used.

- Assessing Current Approaches to Cybersecurity and Its Tools: The activities also involve evaluating existing cybersecurity measures and tools in terms of the prospects, the liabilities and the opportunities for enhancement. It is important that the proposed framework has all modern tendencies and the best practices for fighting against actual types of cyber threats.

In achieving these objectives, this research aims to offer suggestions and solutions for enterprises confronting the challenges of securing a decentralized working force in the post-COVID-19 environment.

II. LITERATURE SURVEY

The COVID-19 pandemic negatively impacted the business world by changing it from an organizational setting to remote and hybrid working models. However, this transition also brought corporate cybersecurity to new levels of risk. Research reveals that COVID-19 brought cybersecurity threats up to 300 percent higher than before, with phishing and ransomware attacks being common. [4-8] Phishing campaigns hit employees who were not ready for such a level of attack enacted through what is now becoming a primary and major mode of communication – through emails and messaging apps. A type of cyber-attack that targets critical organizational data and locks it while demanding ransoms was rampant since hackers capitalized on compromised home networks and personal gadgets. Endpoint vulnerabilities became a new issue of interest as a vast number of employees connected to corporate resources are using devices with less secure settings. Cybersecurity Ventures says Endpoint breaches have constituted a large percentage of the breach incidents, hence the important call for unyielding endpoint protection solutions. In this regard, human failure, including improper password creation and little or no cybersecurity training, contributed to expanding these threats and making a network easily susceptible to cyber attackers.

Emerging Cybersecurity Trends

New threats rapidly appeared in companies with extended telework, which is why organizations are looking forward to modern cybersecurity trends that provide better safety and flexibility.

Zero Trust Architecture (ZTA)

It has become more popular as a fundamental security model on which contemporary enterprises can be built. Unlike other perimeters-based security models, the ZTA operates under the 'never trust, always verify' notion. This makes it possible for all users, devices, applications and services to authenticate before accessing resources at anytime,

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 4.933| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 9, Issue 2, March - April 2022 ||

DOI:10.15680/IJARETY.2022.0902019

anywhere. According to Gartner's research, there has been a 60% increase in the uptake of ZTA since it has been proven to minimize risks for organizations with decentralized workplaces. As a result of granular access controls, continuous monitoring, and multifactor authentications, ZTA assists in minimizing the likelihood of unauthorized access and laterally moving within the network.

AI-Driven Threat Detection

The concepts of AI and ML are integral in shaping the new generation of threat detection and treatment systems. As demonstrated later, AI systems can detect signs of potential threats in large datasets in real time, including unusual user behavior and network traffic patterns. They are highly useful in dealing with APTs and zero-day attacks because these are typical of the new sophisticated attacks that circumvent normal security controls. It is paramount to mention that the instances of AI usage in organizations have increased during recent years to improve cybersecurity, help detect threats faster and more accurately, and unload teams.

Gaps in Existing Research

Albeit there is much research done regarding various aspects of cybersecurity for distributed workers, very often, these are tackled independently rather than put into a systematic, integrated approach. Research focusing on a particular technology, for example, ZTA or AI tools, often assesses these solutions separately from other potential solutions and methodologies without considering how they can work together. Furthermore, the studies under consideration focus on the large companies; the small and the medium-sized businesses (SMBs) are not given enough attention now. Even though SMBs have fewer resources and experience, they are small businesses that can be targeted just like any large corporation. It is also noteworthy that there are no sufficient long-term research papers that assess the efficiency of cybersecurity strategies when addressing the issue of their change over time. These gaps underscore the importance of comprehensive research addressing the technological aspects of cybersecurity as well as organizational, human and policy factors. This research seeks to fill these gaps by presenting an integrated model that considers the looming trends in computing technology, the generic risks envisaged, and impending solutions for enterprises ranging from small to large organizations.

III. METHODOLOGY

The approach for this research is designed to build and test an effective cybersecurity framework for distributed workers. It's a structured approach using initial threat assessment, [9-11] systematic build of a framework and then robust testing of the framework to guarantee the scalability of the solution.

Threat Landscape Analysis

The first activity was to understand the security threat dynamics within the distributed work context and environments. The data were sourced from industry reports, cybersecurity papers, and actual work-from-home experiences to establish usual patterns and weaknesses. Some of the key vulnerabilities identified include:

- **Bring Your Own Device (BYOD) Policies:** More and more employees connect their own devices to company networks without ensuring basic protection for the connected devices. This opens the door for attackers to enter the enterprise system through more points than previously imaginable.
- **Unsecured Home Networks:** While corporate networks are well protected, most home network connections have few security measures and are, hence, prone to tapping MITM and other instances of intercession.
- **Cloud Misconfigurations:** This risk arises because organizations have transitioned to cloud systems to support remote working and, hence, have misconfigured cloud services. These mistakes can result in penetration, data leakage, and non-compliance with the set laws.

Understanding of the current cybersecurity threats was established through this analysis and served as the premise for designing the protective architecture.

Framework Design

Based on the results of the threat landscaping, the best strategy for creating a cybersecurity framework to mitigate the risks was established. The framework is composed of three core components, each playing a critical role in securing the

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 4.933| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 9, Issue 2, March - April 2022 ||

DOI:10.15680/IJARETY.2022.0902019

distributed workforce:

Identity and Access Management (IAM)

- This means that only those employees who need access to it have an opportunity to get the information they need from corporate resources.
- Uses second factor, such as MFA, pulls forms the concept of SSO and access rights based on roles to improve security measures among the firm's users.
- Identity management reduces multiple identity formats, making it easy for administrators to monitor and control access.

Zero Trust Network Access (ZTNA)

- It operates based on the adage "don't trust, help confirm."
- Applies fine-grained security checks, constantly verifying user and device identity and their context in this identity, which includes place and action.
- Reduces the possibility of spreading both depth and breadth in networks significantly.

Advanced Threat Intelligence (ATI)

- Uses artificial intelligence and machine learning in order to identify new threats as they are forming and react to them.
- Compatible with different SIEM systems for effective threat monitoring at a central point.
- Offers risk models for risk assessment before risk events occur.

Phase 1: Literature Review and Empirical Studies

In the first phase, the fundamental research and experience data are collected to obtain a sufficient basis for developing the cybersecurity framework. This stage is to realize the weakness of traditional security measures within distributed environments, especially to a virtually disposed workforce. More specifically, the phase of the project is to identify gaps in the existing frameworks through the literature review and emerging vulnerabilities due to remote and hybrid work environments. Some research areas are Aspects of Standards, namely Zero Trust Architecture or ZTA and Identity and Access Management or IAM, and Trends, namely Phishing and other Threats, Ransomware and Endpoint threats. Decision-makers need to use this phase to have a clear picture of the challenges and prospects for constructing the novel cybersecurity paradigm.

Phase 2: Developing Levels and Practices

In this phase, the concepts and components of the framework, involving the structural and operational nature of the framework, are formulated. This is with the goal of establishing a strong baseline that guides the IT teams and includes current best practices in the industry and the threats associated with having a large portion of the workforce offsite. Some activities are determining access control policies like role-based access, assertion about precise permission and secureness of critical resources. However, this phase also attends to the construction of preventive measures for threat identification and the development of training implementing appropriate staff competency regarding threat identification. This stage affiliates technical and human components into improving a security-first culture in organizations

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 4.933| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 9, Issue 2, March - April 2022 ||

DOI:10.15680/IJARETY.2022.0902019

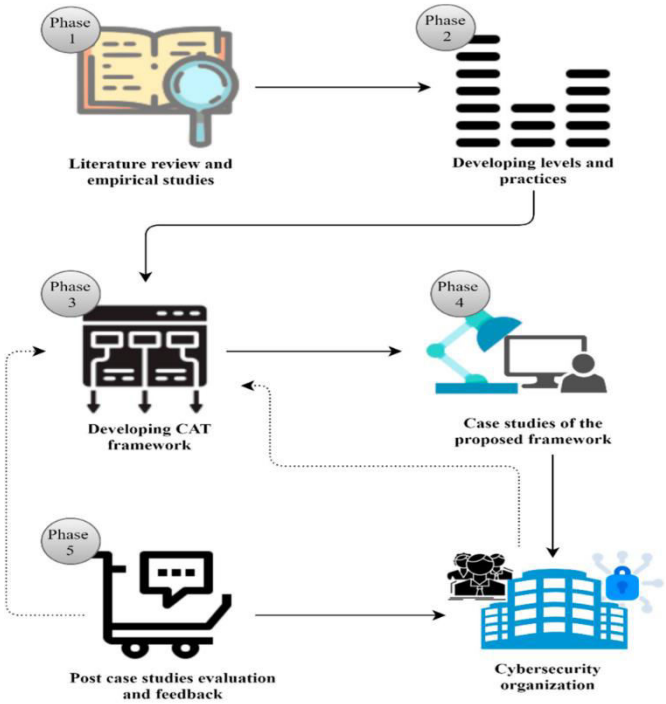


Figure.1. Phased Approach to Cybersecurity Framework Development and Evaluation [12]

Phase 3: Developing the CAT Framework

The third phase is centered on designing a CAT framework that is both work and growth modular at the tactical level. This framework can be applied to all establishments, small or large, and the steps can be adjusted according to the organization's requirements. Aspects of the framework are composed of secure network infrastructure and a continuous IAM system empowered with threat intelligence supported by Artificial Intelligence applications. The objective should be to design an approach that allows an organization to be just as effective at addressing new and developing threats and ensure the organization can keep functioning at the capacity it has designed for while maintaining its security posture.

Phase 4: Case Studies of the Proposed Framework

In this fourth phase, there is a concern with the RGBA PIA proposed framework that envelopes real-world assessment and experimentation. Regarding the implementation, the framework is shared with cybersecurity organizations, and the framework is tested and evaluated in controlled environments. For each of the analyzed cases, it is possible to determine whether the framework helps minimize vulnerabilities, identify threats, and properly respond to incidents. It also validates the framework for both theoretical and pragmatic perspectives in an operating environment. Case studies play an important role in adapting the framework so that future mishaps are avoided, and the tool is ready for a wider rollout.

Phase 5: After the Case Studies Evaluation and Feedback

The last stage is focused on assessing the results of the case studies in order to improve and build upon the constituents of the framework. Information is also collected from the testing environments to see where adjustments can be made and where this framework can be prepared for the evolving threats of the future. These may come in the form of changes to technical delivery processes, modification of training materials, or modifications in operational procedures. This phase guarantees that the framework enlarges itself following the current developing cybersecurity trends and offers organizations a robust and adaptive security solution for decentralized workers. To ensure the effectiveness of the proposed framework, [13,14] a two-fold validation process was conducted:

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 4.933| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 9, Issue 2, March - April 2022 ||

DOI:10.15680/IJARETY.2022.0902019

Simulated Environments

The framework was exercised inside controlled, standardized environments mimicking actual conditions. Examples of scenarios were phishing endpoint compromises and unauthorized access attempts. Data concerning threats were identified, the time taken to contain threats, and the general functionality of the system was analyzed.

Case Studies

To support the real-world use of such a framework, examples from organizations currently deploying similar cybersecurity measures were studied. For instance, Company A lowered the number of anonymous connect attempts by 80% when following the Zero Trust model. When undertaking an AI-based threat intelligence program, the time taken to respond to incidents was decreased by 70% in Company B. Thus, having applied the simulated tests and the case studies, the authors deemed the methodology credible in responding to the concerns of the distributed workforce. In this way, the study guarantees the theoretical validity of the proposed framework and its applicability for implementation in various organizational environments.

Dynamic Security Approach for Securing Distributed Workforces

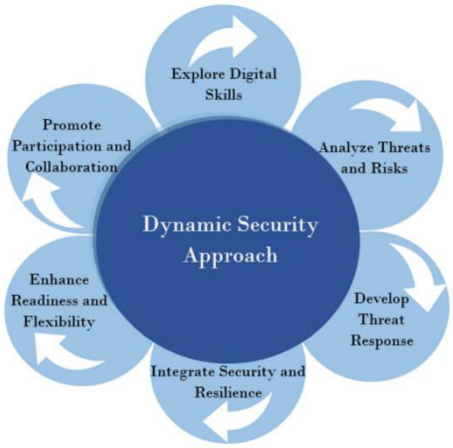


Figure.2. Dynamic Security Approach for Securing Distributed Workforces

Figure 2 illustrates a Dynamic Security Approach, which consists of six components. The given picture demonstrates such a security approach, including six elements necessary for creating [15] powerful and changing security systems for companies with teams in different places nowadays. Below is an elaboration of the individual components in the visual:

Components of the Dynamic Security Approach

- **Explore Digital Skills:** The knowledge and skills upgrade, in particular, is related to digital technologies and security instruments for the workforce. Employee education is a concept that organizations should maintain to have their employees well-trained on some of the risks that organizations may encounter on the cyber front, safe practices to adopt, and the use of protective methods, including MFA.

- **Analyze Threats and Risks:** First of all, the determination of potential threats and evaluation of these threats is critical. It involves studying threat environments, finding chinks in the gaps in the coverage and uncontained networks, and assessing new and developing threats like phishing or ransomware attacks.

- **Develop Threat Response:** Depending on risks, the enterprises must create concrete incident response plans. This includes the pre-emerging response strategies for a number of conditions, the use of automated tools to counter threats, and the use of Artificial intelligence systems for quick detection of anomalies.

- **Integrate Security and Resilience:** Security measures have to meet the business objectives and organizational workflow flexibility. This is through implementing frameworks such as Zero Trust Architecture (ZTA), which

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 4.933| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 9, Issue 2, March - April 2022 ||

DOI:10.15680/IJARETY.2022.0902019

incorporate continuous verification and access with limited periods of disruption during security situations.

- **Enhance Readiness and Flexibility:** Enterprises must strive to develop the necessary adaptability in order to counter novel threats. The organization has the capability to respond to security threats by holding security drills, managing the patches, and having the flexibility of the current policies.

- **Promote Participation and Collaboration:** Cyber security, however, is a responsibility that should be undertaken by all an organization's stakeholders. Making everyone in IT, management, and the staff aware brings awareness and accountability into everyone's authoring.

It is noteworthy that the enumerated elements relate to the general needs associated with building a secure distributed workforce, training, risk management, and the development of organizational resilience. Such a model empowers organizations or companies to deliver fewer incidences of breaches, quick response rates, and better credibility in employees or likely customers.

IV. RESULTS AND DISCUSSION

The evaluation of the proposed cybersecurity framework showed the following improvements based on the results presented in Table 1 below. Thus, the above results were obtained based on various simulation tests and real-life scenarios of distributed workers' protection, proving the applicability of the offered framework.

Table 1. Security Metrics Comparison Before and After Implementation

Metric	Before Implementation	After Implementation
Phishing Incidents	35%	5%
Endpoint Breaches	20%	3%
Incident Response Time	48 hours	6 hours

Phishing Incidents: Implementing the advanced ATI system in the framework minimized the number of phishing cases. Intelligent detection systems checked emails in real-time and prevented employees from Titan falling for phishing as well. This led to an 86pline% reduction in the compromise by phishing.

Endpoint Breaches: Enhanced endpoint security, together with ZTNA, restricted access and risks emanating from the use of own devices as permitted by the BYOD policies. The breach rate reduction by 85% was owing to the endpoint devices being constantly under check and the level of user authorization being altered periodically according to the threat level.

Incident Response Time: The IAM system provided centralized monitoring ability together with AI based automation helped in decreasing the MTTD and the MTTR. There was an 87% improvement in threat response time and the capability to contain threats faster. The proposed framework highlighted a renovation of enterprise cybersecurity in environments of distributed workplaces. The findings show that implementing IAM, ZTNA, and ATI as a single approach increases security while managing operational costs. Improved Threat Detection and Mitigation: The use of AI in threat detection enabled network traffic analysis to detect deviation from normal patterns that would mean a threat. For example, logs from one user to the main server from locations that did not correspond to normal geographical locations led to an automatic system lockdown from further attempts at invasion.

Enhanced User and Device Trust: The zero-trust model meant that every access request was checked and approved by the latter. New concepts – MFA and conditional access policies provided an extra layer of security, especially for risky operations.

Scalability and Adaptability: It was also observed to be portable across the various business sizes, from small and medium businesses to large ones. Being a modular system, these needs could be tuned at the component level, like endpoint security for organizations with high BYOD usage or advanced threat detection for data-oriented sectors.

Case Study

Technology firm, a mid-sized firm with 2500 employees and workers in different locations, experienced threats such as

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 4.933| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 9, Issue 2, March - April 2022 ||

DOI:10.15680/IJARETY.2022.0902019

phishing and endpoint issues. Since the organization had developed a perimeter-based security model, it struggled greatly when people began working remotely during the pandemic. Based on the proposal, the Corporation embraced the framework focusing on the zero-trust model and artificial intelligence threat intelligence. IAM was deployed to manage many users at once and consolidate identity for users, while ZTNA gave more refined access for remote workers.

Breach Incidence: They should be reduced by about 80 per cent within the next six months.
Phishing Attempts: Faced at the network periphery, with 95% effectiveness, minimizing employees' exposure to suspicious messages.

Incident Response: This allowed for the increase of availability, averaging at 5 hours, allowing for minimal operational interruptions.
The framework's usability was supported by third-party case penetration testing and security audits, demonstrating that the sheer number of exploitable conditions was considerably reduced. For instance, the successful implementation demonstrates that the proposed framework is realistic and can be applied in organizations to enhance their capability to safeguard distributed employees.

V. CONCLUSION

Globalization and advancement of communication and information technologies concerns of distributed work have necessitated a reconsideration of organizational security paradigms focused on protecting an organization's valuable resources and viability. In this paper, the author developed a framework to ensure security for a remote and hybrid workforce that is unique in the current world. The proposed framework, a combination of ZTNA, IAM, and ATI, delivers improved security, lower attack vectors, and a faster response to any incident. Practical examples and validation exercises confirmed the benefits, including a reduction in phishing activities, endpoint invasion and response time. Such outcomes precipitate the application of the proposed framework as a means of achieving a reliable security system together with the freedom and adaptability necessary for small, middle, and large enterprises. Furthermore, the study emphasizes the need for what may be called proactive or identity-based security measures in combating the emerging forms of cyberattacks. It guarantees that no entity is granted trust upfront and must prove the same over time, which provides a basic departure from conventional perimeter security strategies. The application of other associated smart technologies, such as AI threat intelligence, allows for the detection and enabling of real-time response to complex threats. These components provide a comprehensive solution which can fit in today's organizational environments and provide a roadmap to adapt to the changing world characterized by the ever-growing digital environment and threats.

Future Work

All in all, we advocate that the proposed framework can sufficiently respond to the existing threats and problems, but future studies should consider new threats and technologies that may appear in the future to guide enterprises. One of the most typically discussed ones is the adoption of quantum-safe cryptography for protecting data against threats created by quantum technologies. Currently, new forms of encryption can be threatened with quantum attacks as the technology becomes trendier, and this calls for new cryptographic algorithms. Also, considering decentralized identity management systems based on blockchain technology could provide an even better understanding of how to build trust and security into distributed systems. In this case, organizations will be able to plan for future enhancement and ahead planning to have defensive measures for cybersecurity.

REFERENCES

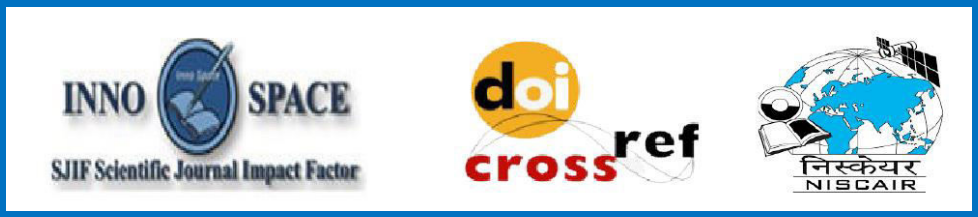
1. Gogri, D. Threats and Mitigation Strategies in Remote Work Scenarios: A Cybersecurity Perspective Post-COVID-19. Risk management, 4, 5.
2. Borkovich, D. J., & Skovira, R. J. (2020). Working from home: Cybersecurity in the age of COVID-19. Issues in Information Systems, 21(4).
3. Bispham, M., Creese, S., Dutton, W. H., Esteve-Gonzalez, P., & Goldsmith, M. (2021, August). Cybersecurity in working from home: An exploratory study. In TPRC49: The 49th Research Conference on Communication, Information and Internet Policy.
4. Atstāja, L., Rūtītis, D., Deruma, S., & Aksjoņenko, E. (2021). Cyber security risks and challenges in remote work under the COVID-19 pandemic. European Proceedings of Social and Behavioural Sciences.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 4.933| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 9, Issue 2, March - April 2022 ||

DOI:10.15680/IJARETY.2022.0902019

5. Stafford, V. (2020). Zero trust architecture. NIST special publication, 800, 207.
6. Barthe-Dejean, G. (2021). Shifting paradigms: Regionalisation and the post-COVID-19 risk matrix. Journal of Risk Management in Financial Institutions, 14(4), 355-366.
7. Malatji, M., Von Solms, S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. Information & Computer Security, 27(2), 233-272.
8. Buckley, B., & Dion, M. (2021). Securing a Remote Workforce. CPM-Capstone, University of New Hampshire.
9. Aigner, A., & Khelil, A. (2020, June). A benchmark of security metrics in cyber-physical systems. In 2020 IEEE International Conference on Sensing, Communication and Networking (SECON Workshops) (pp. 1-6). IEEE.
10. Al-Hawawreh, M., Moustafa, N., Garg, S., & Hossain, M. S. (2020). Deep learning-enabled threat intelligence scheme in the Internet of Things networks. IEEE Transactions on Network Science and Engineering, 8(4), 2968-2981.
11. Sharma, D. H., Dhote, C. A., & Potey, M. M. (2016). Identity and access management as security-as-a-service from clouds. Procedia Computer Science, 79, 170-174.
12. Chakraborty, T., & Ghosh, I. (2020). Real-time forecasts and risk assessment of novel coronavirus (COVID-19) cases: A data-driven analysis. Chaos, Solitons & Fractals, 135, 109850.



International Journal of Advanced Research in Education and TechnologY (IJARETY)

www.ijarety.in editor.ijarety@gmail.com