Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, **Number** 2, November 2024
https://doi.org/10.47709/brilliance.v4i2.4759

Cyber Pandemic – The New Cybersecurity Risks

Sukenda[1*], Ulil Surtia Zulpratita[2], Helmy Faisal Muttaqin[3], Ari Purno Wahyu[4], Benny Yustim[5]
[1,2,3,4,5] University of Widyatama, Bandung, Indonesia
[1]kenda@widyatama.ac.id, [2]ulil.zulpratita@widyatama.ac.id, [3]helmy.faisal@widyatama.ac.id, [4]ari.purno@widyatama.ac.id, [5]byustim@widyatama.ac.id

open access

***Corresponding Author**

Article History:
Submitted: 01-10-2024
Accepted: 05-10-2024
Published: 21-10-2024

Keywords:
COVID-19; cyber attacks; cybercrime; cyber pandemic; cyber security; cyber resilience

ABSTRACT

The main focus of this study and a large group of other alarming possibilities is that being prepared for any type of digital emergency regardless of the level of association is critical. Top-level administration, trained network protection professionals, and every representative must know how to handle an emergency attack. We are in the midst of a digital pandemic. This research method uses literature studies and various sources. COVID-19 accelerated the shift to remote work and the products used for these attacks became easier to carry out, ransomware attacks increased rapidly and will continue to increase in 2021. The COVID-19 pandemic has changed the real world and the computerized space, where organizations and associations are faced with extraordinary online protection challenges that many were not prepared or ready to face. Due to the extreme changes in working conditions, cyberattacks and information extortion are now ranked third among business leaders' top concerns, as detailed in the World Economic Forum's COVID-19 Risk Outlook. The results of this study are expected to make the possibility of a vicious digital movement even more alarming considering that 53% of organizations have never tested their systems through force. Cybersecurity is centered on securing information, but it is currently inadequate; organizations need cyber resilience.

INTRODUCTION

The world changed in 2020 with the flare-up of Covid-19. Nations shut their lines, forced separation on their kin, depleted their monetary assets to help their economies. The work life was changed too, with a greater part of the work power progressing to workspaces to proceed with their work while keeping up with the limitations. The generally developing internet-based life had a significant blast during this time.

Yet, 2020 will likewise be recognized as the year that society was changed with the blast of network protection occasions. Digital aggressors consider the pandemic to be a chance to move forward their crimes by taking advantage of the weakness of representatives telecommuting (Check Point. 2020). The negative network protection effects of these internet-based changes have come about in a digital pandemic. With a more extensive spread of digital episodes, securing resources and framework has become really testing. Organizations are speeding up their advanced change, and online protection is currently a main issue.

As COVID-19 spread across the globe, it additionally prompted an optional critical danger to an innovation driven society, i.e., a progression of aimless, and furthermore a bunch of focused on, digital assaults and digital wrongdoing efforts. Since the episode, there have been reports of tricks imitating public specialists (e.g., WHO) (Malware Bytes, 2020) and associations (e.g., grocery stores, airlines) (Bryan, Kenza (2020), focusing on help stages, directing Personal Protection Equipment (PPE) misrepresentation, and offering COVID-19 (Paul, Kari. 2020) These tricks target individuals from the public for the most part, just as the large numbers of people telecommuting.

Working at home altogether has understood a degree of digital protection concerns and difficulties never looked before by industry and populace. Digital hoodlums have utilized this amazing chance to develop their assaults, utilizing conventional deceit which additionally supplicates on the uplifted pressure, uneasiness, and stress confronting people. Likewise, the encounters of working at home uncovered the overall degree of ineptness by programming sellers, especially to the extent the security of their items was concerned. Understanding cybersecurity and the dangers associated with various threats that could compromise or steal personal data while using the internet could be helpful in reducing the likelihood of threats and protecting data from malware and bots (Sadaghiani-Tabrizi, A. 2022).

LITERATURE REVIEW

The COVID-19 pandemic has affected our whole working society. A new overview shows that 95% of safety experts are confronting added IT security challenges due to the Covid (Check Point. 2020). The movements were worldwide, quick, and far reaching. Similarly, as a viral pandemic was inescapable, a digital pandemic in what's to come is likewise unsurprising. As innovation is internationally interconnected, a digital infection could move from one gadget to another, similar as Covid-19 among people. An infection spread through an application could have destroying results, with the chance of a worldwide web lockdown. The World Economic Forum has anticipated that a solitary day without the web could cost more than $50bn internationally, even prior to considering the cultural harm connected with closure of fundamental administrations (Davis, N. 2020). Similarly, as we should plan to get ready for the following pandemic, so too should we investigate our worldwide readiness for digital protection dangers.

With a cyber pandemic, cybersecurity requests that we comprehend the cyber dangers with our changed computing environment. Table 1 shows security challenges of COVID-19 threats and mass remote working and gives a beginning stage as we re-evaluate our cybersecurity procedures.

Table 1. Security challenges of COVID-19 threats and mass remote working))

Transition	Outcome	Threat	Top Procedure and Technology
Working from home	Personal versatile and PCs gave admittance to corporate networks	Data break (for example key lumberjack, screen lumberjack on pc/mobile)	1. Execution of endpoint security and cleanliness with consistence check (most recent patches, AV) 2. Client preparing mindfulness (for example phishing reproduction) 3. Portable danger protection on versatile
Swift move to cloud	Speed of arrangement on the cost of security	Basic security controls can prompt information misfortune and manipulation	1. Put resources into Cloud Security pose the executives 2. Send responsibility security for compartments and serverless applications. 3. Ongoing avoidance of dangers with IaaS security
Essential infrastructure	Allowing essential framework distant access	Essential foundation breach	1. IoT security for IoT gadgets 2. support network security pose with red group 3.Operational Technology (OT) security with Scada requirement
Expanded organization capacity	More throughput is expected to address information in motion	Inadequacy of service Network is down	1. Put resources into network security that scales as indicated by needs 2. All assurances should be empowered while keeping business congruity 3. Versatile secure remote access

The COVID-19 pandemic has affected our whole working society. A new overview shows that 95% of safety experts are confronting added IT security challenges due to the COVID (Check Point, 2020). The movements were worldwide, quick, and far reaching. Similarly, as a viral pandemic was inescapable, a digital pandemic in what's to come is likewise unsurprising. As innovation is internationally interconnected, a digital infection could move from one gadget to another, similar as Covid-19 among people. An infection spread through an application could have destroying results, with the chance of a worldwide web lockdown. The World Economic Forum has anticipated that a solitary day without the web could cost more than $50bn internationally, even prior to considering the cultural harm connected with closure of fundamental administrations (Davis, N. 2020). Similarly, as we should plan to get ready for the following pandemic, so too should we investigate our worldwide readiness for digital protection dangers.

With a cyber pandemic, cyber security requests that we comprehend the cyber dangers with our changed computing environment. Table 1 shows security challenges of COVID-19 threats and mass remote working and gives a beginning stage as we re-evaluate our cyber security procedures. Organizations and governmental bodies' cybersecurity skills are still not up to date with the threats. In light of the current circumstances, these organizations have prioritized cybersecurity education once again. But in most contexts, education seems to fall short of its potential (Workman, M.D. 2021).

METHOD

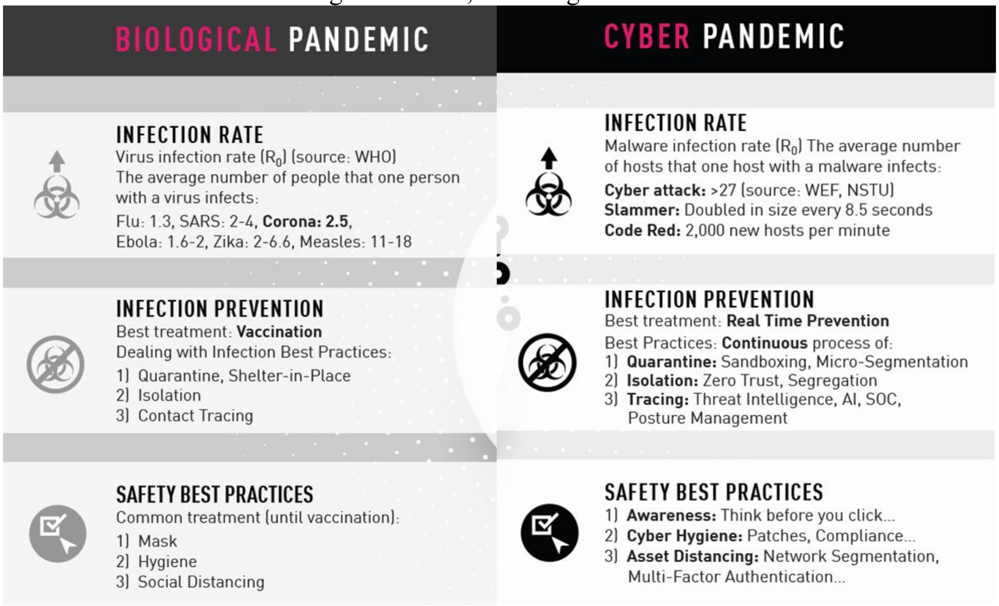
For quite a long time, alarms about the disastrous impacts that a pandemic could produce have been declared by specialists regarding the matter. One such master, Bill Gates, in 2015, tended to this subject at a TED Talks gathering (Gates, B. 2005). Notwithstanding, at that point, neither legislators nor pioneers gave a lot of consideration or focused on mainstream researchers' sobs for activity. Assets, mechanical apparatuses, prescient investigation, and prepared work force were not ready to screen the issue appropriately. It was not until 2020-when the staggering blow of the pandemic's impact on general wellbeing, the wild spread, and the never-before-expected harm to the economy was felt-that the cautions were behind schedule initiated. An entire series of receptive measures were released looking to settle and cushion the blow got, (Ceballos, G.A, 2021). Few empirical studies have systematically tested the efficacy of various training methods and modes, and those that have been conducted have yielded inconsistent findings.

Characterizing a cyber pandemic is a piece like characterizing a "perfect storm" - just this tempest is in the cyberspace. The Coronavirus pandemic has broug ht maybe the quickest, starkest change to working examples all over the planet in living memory. While laborers in medical care, policing, retail, conveyance, cleaning, and a large group of other fundamental forefront administrations wrestle with unfathomably expanded interest and testing working conditions, a larger part of office staff around the world are having to rapidly acclimate to all day, everyday home

E-ISSN : 2807-9035
Volume 4, **Number** 2, November 2024
https://doi.org/10.47709/brilliance.v4i2.4759

working. Furthermore, IT and security groups are confronting numerous difficulties in conveying and tying down this mass movement to distant network.

The pandemic constrained an immense shift - requiring many individuals to work or go to class from home and leading to a detonating number of online stages and gadgets to help a change that has drastically expanded security chances. Cyberattacks become more forceful and inescapable, as hoodlums utilize harder strategies to follow more weak focuses on, the report said. Malware and ransomware assaults have blast, while the ascent of digital forms of money makes it simple for online hoodlums to conceal installments they have gathered. With the Covid-19 flare-up, digital hoodlums have held onto this worldwide emergency to send off slippery digital adventures. The new typical scene has created a flood of modern Gen V digital assaults, including focused on ransomware.



BIOLOGICAL PANDEMIC	CYBER PANDEMIC
INFECTION RATE Virus infection rate (R_0) (source: WHO) The average number of people that one person with a virus infects: Flu: 1.3, SARS: 2-4, **Corona: 2.5,** Ebola: 1.6-2, Zika: 2-6.6, Measles: 11-18	**INFECTION RATE** Malware infection rate (R_0) The average number of hosts that one host with a malware infects: **Cyber attack:** >27 (source: WEF, NSTU) **Slammer:** Doubled in size every 8.5 seconds **Code Red:** 2,000 new hosts per minute
INFECTION PREVENTION Best treatment: **Vaccination** Dealing with Infection Best Practices: 1) Quarantine, Shelter-in-Place 2) Isolation 3) Contact Tracing	**INFECTION PREVENTION** Best treatment: **Real Time Prevention** Best Practices: **Continuous** process of: 1) **Quarantine:** Sandboxing, Micro-Segmentation 2) **Isolation:** Zero Trust, Segregation 3) **Tracing:** Threat Intelligence, AI, SOC, Posture Management
SAFETY BEST PRACTICES Common treatment (until vaccination): 1) Mask 2) Hygiene 3) Social Distancing	**SAFETY BEST PRACTICES** 1) **Awareness:** Think before you click... 2) **Cyber Hygiene:** Patches, Compliance... 3) **Asset Distancing:** Network Segmentation, Multi-Factor Authentication...

Figure 1. Biological pandemic vs Cyber pandemic Check Point. (2020)

An ideal objective for cybercriminals has been the Operational Technology (OT) networks which interconnect the Industrial Control Systems (ICS) that deal with our basic framework. As administrations like power frameworks, water treatment offices, transport and medical care frameworks progressively incorporate their functional innovation frameworks with the Internet of Thing (IoT) - for instance through distant sensors and observing - this makes another outskirt of dangers where millions greater weakness focuses, and new vectors can be taken advantage of by programmers. So now, there is a cyber pandemic, not only a biological pandemic. Fig 1 shows the difference between a biological pandemic and a cyber pandemic.

Digital assaults have likewise designated basic framework, for example, medical care administrations. Because of this, on April 2020, the United Kingdom's National Cyber Security Center (NCSC) and the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) distributed a joint warning on how digital crook and progressed industrious danger (APT) bunches were taking advantage of the current COVID-19 pandemic. These warning examined issues, for example, phishing, malware and interchanges stage (e.g., Zoom, Microsoft Teams) compromise. What is ostensibly missing here and in research, nonetheless, is a more extensive evaluation of the wide scope of assaults connected with the pandemic (CISA, 2020).

The present status of the workmanship is incredibly scattered, with assaults being accounted for from legislatures, the media, security associations and occurrence groups. It is in this manner very moving for associations to foster proper security and reaction estimates given the powerful climate. Results Organizational resilience is impacted by organizational learning. Organizational resilience is not directly impacted by environmental scanning. The association between environmental scanning and organizational resilience is fully mediated by organizational learning, though. Additionally, the indirect association between environmental scanning and resilience is not moderated by environmental uncertainty (Yahia Marzouk, Y,and Jin, J. 2022). When considering the heights of the health crisis, one could argue that the pandemic was a "stress test" of a kind never seen before, testing the resiliency of interconnected systems, corporate models, societal institutions, and even entire economies (Tressel T, Ding X, 2021).

RESULT

The pandemic and a scourge of ransomware assaults uncovered the requirement for another way to deal with big business security. There must now be an alternate way to deal with cybersecurity. Our present methodology is unsustainable. Cybersecurity is about responding, while cyber resilience is tied in with anticipating. This system features the essential and ceaseless activities needed to accomplish cyber resilience. Table 2 shows the differences

E-ISSN : 2807-9035
Volume 4, **Number** 2, November 2024
https://doi.org/10.47709/brilliance.v4i2.4759

between cybersecurity and cyber resilience. What's the challenges of cyber resilience? The basic innovation changes on which future thriving depends - universal network, artificial intelligence, quantum computing and cutting-edge ways to deal with personality and access the board - won't simply be steady difficulties for the security local area.

Except if move is made now, by 2025 cutting edge innovation, on which the world will progressively depend, can possibly overpower the safeguards of the worldwide security local area. Cutting edge advancements can possibly create new network protection hazards for the world, and at this stage, their full effect isn't surely known. There is an earnest requirement for aggregate activity, strategy mediation and further developed responsibility for government and business. Without these mediations, it will be hard to keep up with honesty and confidence in the arising innovation on which future worldwide development depends.

Table 2. Differences between cybersecurity and cyber resilience

Cybersecurity	**Cyber Resilience**
Definition: techniques followed, or gauges taken to guarantee the security of a state or organization.	Definition: the ability to recuperate rapidly from challenges; strength.
Innovations and cycles intended to shield an association from cybercrime	Technologies and cycles intended to continue to convey expected administrations despite digital occurrences.
Attempts to decrease the danger of cyberattacks and to shield the association from espionage.	Works to guarantee progression on a more extensive degree, containing network safety and business necessities.
Can work adequately without compromising the convenience of other systems.	Requires association wide culture shift the standardizes and inserts security best practices.
Includes a business plan to continue tasks for the occasion of a fruitful attack	Requires the association to become agile and versatile in the face of cyberattacks and occurrences.

Cyber resilience expects associations to contemplate their way to deal with dangers and become more dexterous in their taking care of and reaction to assaults. Cyber resilience begins with nailing the network protection essentials; at Salesforce, we refer to it as "doing the normal remarkably well." This incorporates fixing weaknesses, recognizing, and moderating dangers, and teaching workers on the best way to guard organization security. Yet, we should do these things constantly, not simply one time per year.

Past that, organizations need to develop resilience into all aspects of the business, from business process planning to designing help accessibility to basic seller reliance. They need to restrict the effect of cybercrime to an organization's image, finance, lawful, and client trust commitments. While these areas normally get restricted consideration, assets, or chief concentration, they are huge components on account of a genuine danger. Cyber resilience is not the same as security protection. It is tied in with realizing terrible things will occur. The inquiry isn't about if however, when. To become digital tough, the extent of assurance would be more than the "Royal gems." It includes a broader inclusion: the environment of the business or association. Being ready for anything is at the heart of cyber resilience. Fig 2 and Table 3 show the six critical factors of cyber resilience and the description of each term.

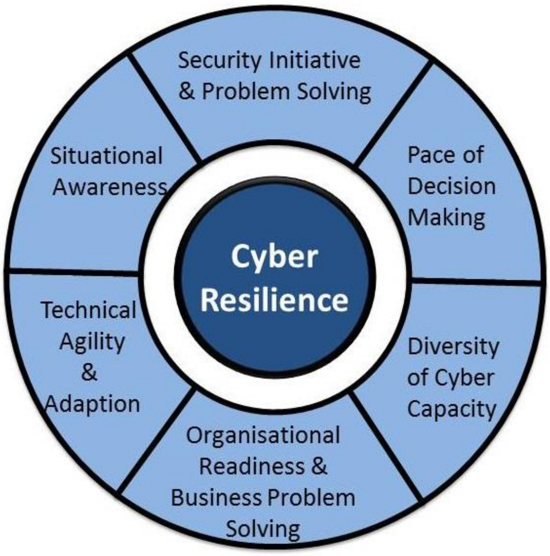

Security Initiative & Problem Solving
Pace of Decision Making
Diversity of Cyber Capacity
Organisational Readiness & Business Problem Solving
Technical Agility & Adaption
Situational Awareness
Cyber Resilience

Figure 2. The six critical factors of cyber resilience (Phil, 2016)

Table 3. Description of cyber resilience's critical factors (Phil, 2016)

Term	Description
Pace of Decision Making	The all-out time it takes top administration and the Board to gather undertaking wide, impromptu dynamic gatherings, give input to these gatherings; for these gatherings to settle on basic choices; and for the association to execute these choices. This is fundamentally critical to guaranteeing the business can keep on working in a corrupted state. This likewise requires CISOs to work with more extensive IT and activities authority to draw in top administration, including CEOs and Boards.
Organizational Readiness and Business Problem Solving	The capacity of the association to prepare able assets and adjust business cycles and activities to oblige startling occasions during an emergency, across the whole endeavor. This plainly requires CISOs to work with more extensive IT and activities authority to draw in top administration, including CEOs.
Diversity of Cyber Capacity	The overt repetitiveness and profundity of limit yet in addition a proportion of heterogeneity in the association's computerized business and expanded undertakings. This spotlights on the versatility of the data frameworks and abilities to digital shocks that might target explicit frameworks, innovations, or staff. Once more, this requires CISOs to work with other IT partners to work in adaptability - and, basically, secure vital venture to go past cost minimization or potentially business usefulness targets.
Technical Agility and Adaption	The capacity of the association to change specialized frameworks and cycles considering new dangers or occasions. This requires CISOs to work with other IT partners to work in adaptability - and, fundamentally, secure important speculation to go past cost minimizations or potentially business usefulness targets. This is a critical cross-over with digital obstruction.
Situational Awareness	The comprehension of the association's own assets, resources, and shortcomings; just as reasonable foe strategies, targets and capacities. In such manner CISOs should guarantee that associations can constantly ingest and survey new data and invigorate this arrangement. This is a basic cross-over with Cyber opposition and underlines the significance of situational attention to digital protection in general.
Security Initiative and Problem Solving	The capacity of online protection experts inside the business to distinguish and react adequately to startling circumstances, including the capacity to help the business 'bomb securely' when assaulted. This ought to be a center skill for CISOs.

The point of cyber resilience is sufficiently clear: to guarantee functional and business coherence with insignificant effect. Be that as it may, the truth can be more earnestly to nail down since there's presently nothing but bad method for estimating digital resilience. As pioneers, we want to have a specific degree of trust in our capacity to react to an assault, to keep up with our clients' trust, to assimilate the monetary, lawful, and brand sway and return to business. However, there is no generally acknowledged cyber resilience system, no development model. Aside from hoping that the thorough presentation will encourage other academics and professionals to try their hardest to continue with research, this aspect of the crucial complexity in these problems demands more thought. Trends like the emphasis on human-centric security measures and the intricate role of AI in cyberwarfare are shaping the future of cybersecurity (Albahri1, A.S. 2024)

DISCUSSION

The present powerfully advancing cybercrime expects us to raise our security propensities, practices, techniques, and conventions. There is presently a requirement for the security practices to be custom fitted and tweaked to ensure against assaults of the new world. To close, we have recorded a portion of the security practices to continue in this digital pandemic.

a. Secure your remote access - Employees working remotely ought to have against infection and malware securities on all frameworks; Employers ought to consider giving these assurances to individual worker frameworks getting to corporate assets to keep their own foundation secure. Multifaceted verification ought to be implemented for all remote access, where conceivable.

b. Further develop security instruction and mindfulness - There is an expanding need for us to keep awake to date with the advancing and changing nature of cyberattacks. Organizations should execute security mindfulness programs and furthermore consider mimicking phishing lobbies for their workers to get more point-by-point results on their human security pose.

c. Secure your home organization - More individuals than at any other time are telecommuting, and it is fundamental for keep our home organization secure. We ought to guarantee our home Wi-Fi network is ensured with a solid secret phrase and appropriate securities are set up on every single home gadget. Think about utilizing a VPN.

d. Foster a weakness the board program - An authority weakness the executives program itemizing resource stock, fix status and insurance levels can go quite far in a digital pandemic. Organizations ought to recognize IT framework shortcomings and fix the most basic weaknesses as quickly as time permits. Analyst and insightful insurances like SIEM ought to be set up.

e. Plan for assaults; consider infiltration testing - It is prudent for organizations to consider going one stage forward and run entrance tests on their resources for get a more exact understanding into their security pose. In these high-hazard times, organizations should complete incessant digital emergency recreation activities to set up their reaction to a cyberattack.

f. Influence insight strategies - Businesses ought to energize proactive utilization of digital danger knowledge to distinguish pertinent signs of assaults and address known assaults.

g. Recharge business progression and emergency plans

h. Organizations are urged to refresh their business congruity plans as indicated by cutting edge work and cyberattack situations.

CONCLUSION

Today, we work from anyplace, on more gadgets, more organizations, confronting more danger than any time in recent memory. Inescapable phishing, malware, ransomware assaults, and different fakes represent a danger to people or stages, yet to whole economies, states, and our lifestyle. The hours of worldwide pandemic created an incredible open door for advanced persistent threat gatherings to target representatives working somewhat in workspace climate where security capacities are no place near the ones conveyed by framework directors in corporate organizations.

As we've learned, vaccination is much better than treatment. A similar applies to our digital protection. Ongoing anticipation puts our association in a superior situation to safeguard against the following cyber pandemic. We have to do the real time prevention. Each part in the chain matters. Our new ordinary necessitates that we return to and check the security level and pertinence of our organization's foundations, processes, consistence of associated portable, endpoint gadgets, and IoT. The expanded utilization of the cloud implies an expanded degree of safety, particularly in innovations that safe responsibilities, holders, and serverless applications on multi-and mixture cloud conditions. That is the reason why we must secure our everything.

Climactic changes in our organization's framework presents an exceptional chance to survey our security ventures. Is it true or not that we are truly getting what we want and are our point arrangement ensuring the right things? Might it be said that there are regions we've disregarded? The most elevated level of perceivability, came to through solidification, will promise us the security adequacy expected to forestall refined digital assaults. Brought together administration and hazard perceivability finish up our security engineering. This can be accomplished by lessening our point item arrangements and merchants, and our general expenses.

To address worldwide cybersecurity challenges and work on digital trust, the World Economic Forum made the Center for Cyber security. This free worldwide stage expects to cultivate global discoursed and cooperation across private and public areas to build up the significance of cybersecurity. The organization has distinguished three critical needs as a feature of their work: building cyber resilience, reinforcing worldwide collaboration, and understanding future networks and innovation.

ACKNOWLEDGMENT

This work is supported by Widyatama University.

REFERENCES

Albahri1, A.S., Yaseen, M.G., Aljanabi1, M., Ali2, A.H., & Kaleel3, A. (2024). Securing Tomorrow: Navigating the Evolving Cybersecurity Landscape. Mesopotamian Journal of CyberSecurity.

Bryan, Kenza (2020) “Fraudsters impersonate airlines and Tesco in coronavirus scams, [Online] Available at: https://www.thetimes.co.uk/article/fraudsters-impersonate-airlines-and-tesco-in-coronavirus-scams-5wdwhxq7p (Accessed 11 Jan 2022).

Ceballos, G.A. (2021) “The World is not Prepared for a Cyber Pandemic.” Journal of The Americas, 1st ed 2021. [Online] Available at: https://www.airuniversity.af.edu/Portals/10/JOTA/Journals/Volume%203%20Issue%201/07-Afanador_eng.pdf

Check Point. (2020) ``A Perfect Storm: the Security Challenges of Coronavirus Threats And Mass Remote Working” [Online] Available at https://www.checkpoint.com/pages/cybersecurity-protect-from-cyber-pandemic/ (Accessed 11 Jan 2022).

Check Point. (2020) ``Cyber Security in the Age of Coronavirus," Check Point [Online] Available at https://www.checkpoint.com/pages/cybersecurity-protect-from-cyber-pandemic/ (Accessed 11 Jan 2022).

CISA (2020) “UK And US Security Agencies Issue Covid-19 Cyber Threat Update.” Cybersecurity and Infrastructure Security Agency [Online] Available at: https://www.cisa.gov/news/2020/04/08/uk-and-us-security-agencies-issue-covid-19-cyber-threat-update

E-ISSN : 2807-9035
Volume 4, **Number** 2, November 2024
https://doi.org/10.47709/brilliance.v4i2.4759

Davis, N. (2020) "What The COVID-19 Pandemic Teaches Us About Cybersecurity – And How to Prepare For The Inevitable Global Cyberattack." World Economic Forum. [Online] Available at: https://www.weforum.org/agenda/2020/06/covid-19-pandemic-teaches-us-about-cybersecurity-cyberattack-cyber-pandemic-risk-virus/

Gates, B. (2015) "The next epidemic? We are not ready." TED [Online] Available at: https://www.ted.com/talks/bill_gates_the_next_outbreak_we_re_not_ready?language=es

MalwareBytes. (2020) "Cybercriminals impersonate World Health Organization to distribute fake coronavirus e-book", [Online] Available at https://blog.malwarebytes.com/social-engineering/2020/03/cybercriminals-impersonate-world-health-organization-to-distribute-fake-coronavirus-e-book (Accessed 11 Jan 2022).

Paul, Kari (2020) "US Authorities Battle Surge in Coronavirus Scams, From Phishing to Fake Treatments," [Online] Available at: https://www.theguardian.com/world/2020/mar/19/coronavirus-scams-phishing-fake-treatments (Accessed 11 Jan 2022).

Phil (2016) "Cyber Resilience: Part Three What is Cyber Resilience?", Black Swan Security [Online] Available at:https://blog.blackswansecurity.com/2016/02/part-three-what-is-cyber-resilience/

Sadaghiani-Tabrizi, A. (2022). Revisiting Cybersecurity Awareness in the Midst of Disruptions. International Journal for Business Education.

Tressel T, Ding X (2021) Global Corporate Stress Tests—Impact of the COVID-19 Pandemic and Policy Responses. IMF Working Papers 2021 (212). https://doi.org/10.5089/9781513590820.001

Workman, M.D. (2021). An exploratory study of mode efficacy in cybersecurity training. Journal of Cybersecurity Education, Research and Practice.

YahiaMarzouk, Y., & Jin, J. (2022). Linking environmental scanning and organizational learning with organizational resilience of Egyptian SMEs: the moderating role of environmental uncertainty. International Journal of Organizational Analysis.