JOURNAL OF SOCIAL SCIENCE

Printed ISSN: 2720-9938
Electronic ISSN: 2721-5202

jsss.co.id

ANALYSIS OF ATTACKS AND CYBERSECURITY IN THE HEALTH SECTOR DURING A PANDEMIC COVID-19: SCOPING REVIEW

Awaludin*, Wahyu Sulistyadi, Alexandra Francesca Chandra
Faculty of Public Health, Universitas Indonesia, Indonesia
Email: awaludin.mmc@gmail.com*

ARTICLE INFO

Date received : December 7, 2022
Revision date : January 9, 2023
Date received : January 16, 2023

Keywords:
Cyber Attack, Cyber Security, Health, Pandemic, COVID 19

ABSTRACT

COVID-19 as a global pandemic in March 2020 medical personnel and all types of patients with various chronic conditions is undeniably the largest group of users of digital technology during the pandemic. Increased exposure and massive use of the internet is certainly a potential security threat in itself, especially in the threat of cyber-attacks. The purpose of this study is to analyze cyber-attacks and security in the health sector during the COVID 19 pandemic. The scoping review was conducted by searching two main scientific databases (PubMed and Scopus) using the search formula "COVID 19, Pandemic and cyber-attack, cyber security". Only articles in English published in the last decade are included (i.e., 2009-2020) to focus on current problems, challenges, and solutions. In total, 34 papers were included in review. We found information technology in the health sector that was used during the COVID 19 pandemic. The COVID-19 pandemic situation is a type of non-traditional security that has a broad impact on various aspects of human life, including the health sector. At a time when many countries have responded to the pandemic situation with various restrictive policies to the prohibition of mobilization, people are adapting by shifting to a new landscape of activity. The cyber world is then used by the community to continue to run productivity. This then has implications for the increase in internet users globally, including Indonesia. Further research is needed, especially exploring research on cyber-attacks during a pandemic from the point of view of implementation of cyber security.

INTRODUCTION

The declaration of COVID-19 as a global pandemic in March 2020 marked the beginning of the biggest global crisis this decade that had an impact on the human status quo. Since the first case was discovered in December 2019 until now, January 2021, the total confirmed cases have reached 99,363,967 cases with total deaths reaching 2,135,959 people (WHO, 2021). In particular, in Indonesia, the total number of cases that have been identified has almost touched

How to Cite: Awaludin, Sulistyadi, W. & Chandra, A. F. (2023). Analysis of Attacks and Cybersecurity in the Health Sector During a Pandemic COVID-19: Scoping Review. *Journal of Social Science*. *4*(1). https://doi.org/10.46799/jss.v4i1.512
E-Issn: 2721-5202
Published By: Ridwan Institute

1 million cases with a death rate of 2.8% or around 28 thousand people (WHO, 2021). The biggest health crisis of this decade has widely threatened various fundamental sectors of human life, including social, health, economic, political, to information and technology. In fact, after COVID-19 has infected the world for more than a year, a new type of variant of COVID-19 requires humans to once again evolve in order to adapt to the existing situation. As a virus that easily spreads through human-to-human contact, a number of countries have implemented adaptation policies by imposing restrictions on people's mobility.

As an implication of limiting people's activities outside the home, people are shifting various offline landscape activities to online. Various activities have been adapted, such as work from home work schemes, online class-based learning, to online buying and selling activities have also increased. The fact is that there was an increase in internet users in 2020 by 10% compared to 2019, until last July the world internet users were recorded at 3.96 billion (Datareportal, 2020b).

The presence of medical personnel and all types of patients with various chronic conditions is undeniably the largest group of users of digital technology during the pandemic. It includes radiologists, surgeons, and nurses active on the front lines to diagnose and treat patients. Radiologists hold an important position to classify computerized tomography of the chest as positive or negative for COVID-19 and describe the main computerized tomographic features and distribution of lesions (Strunk et al., 2020). At the same time, patients with different chronic diseases receive services and treatment from health professionals through the use of technology, especially for those who have been infected with the corona virus. Vulnerable populations such as patients with various chronic conditions or immunosuppression will face a difficult choice between the risk of exposure to iatrogenic COVID-19 during doctor visits and delaying the necessary treatment (Munawar, 2017). Whether choosing face-to-face visits, postponing visits, or using virtual healthcare, patients must face the inevitable use of technologies such as computerized tomography machines and video-based communication platforms to obtain instructions from healthcare professionals. For this reason, medical personnel and their patients are the largest group of technology users during COVID-19.

The increase in exposure and massive use of the internet is certainly a potential security threat, especially in the threat of cyber-attacks. Cybercrime incidents arising from the COVID-19 pandemic pose a serious threat to the safety and global economy of the world population, therefore understanding their mechanisms, as well as the spread and reach of these threats is very important (Kotenko & Chechulin, 2013; Tsakalidis & Vergidis, 2017). This study is to analyze cyber-attacks and security in the health sector during the COVID 19 pandemic.

METHOD

A. Protocol and Registration

The review was performed according to the PRISMA-ScR (Preferred Reporting Items for Systematic Reviews and Meta-Analyses Extension for Scoping Reviews). The aim of this review is to analysis health sector, cyber-attacks, cyber security, and solutions

B. Information Sources

A search of two major scientific databases (PubMed and Scopus) was performed to identify relevant articles. These include both original research articles and review articles. The search formula "COVID 19, Pandemic AND cyber-attack, cyber security" was used to search for articles. The articles identified should have either a COVID 19, Pandemic, cyber-attack, cyber security core or a healthcare core.

C. Eligibility Criteria

Only articles in English published in the last decade are included (i.e., 2009-2020). Reports, news articles or websites are also included only if they are directly related to previously published work, or are the only source of information currently available at the time of manuscript preparation. The inclusion criteria were as follows: (1) relevance to cyberattacks, health and (2) well-discussed scope of cybersecurity issues, challenges, and solutions.

D. Selection of Evidence Sources

The selection process is illustrated in Figure 1. The title and abstract of each paper were analyzed by 2 of the authors to assess eligibility. A total of 150 identified papers were screened and 50 duplicates were removed. An additional 30 papers were excluded for not focusing on the healthcare, cyber-attack, cybersecurity core or the COVID 19 pandemic core in the abstract. In total, 34 papers were included in the review.

RESULTS AND DISCUSSION

A. Health Sector Condition Changes Due to COVID-19

The findings pertaining to changes in conditions in the health sector as a result of COVID-19 The main changes to health services caused by the COVID-19 pandemic include decreased mobility, border closures, and the increasing reliance on remote work, often carried out with little previous experience and planning. These conditions have made the health sector more vulnerable to potential cyberattacks as health staff and patients are restricted in terms of movement due to the lockdown, the decrease in mobility and border closures make individuals and organizations turn to technology to provide essential health services such as appointments, diagnosis, and even operations. Examples are the use of e-consultation (electronic consultation) services for patients and electronic multidisciplinary teams. Although these technologies have their advantages, they leave users and receivers of these technologies open to a variety of attacks such as phishing campaigns and ransomware attacks (Weil & Murugesan, 2020).

Furthermore, health services staff often have limited previous experience with remote working and with planning for this change, which leaves the sector vulnerable to cyberattacks (Boddy et al., 2017; Jalali et al., 2020; Offner et al., 2020). As health services make use of a variety of medical devices, interconnectivity and interoperability create issues as they are now being accessed from outside health services' internal network perimeter. The medium and mode of access creates problems as access to the sensitive parts of health services can be reached via unsecured network connections or unpatched systems by staff working remotely (Hoffman, 2020; Jalali et al., 2020; Ronquillo et al., 2018). In addition, some medical devices use off-the-shelf software, such as commercial operating systems (eg, older versions of Windows). These systems are vulnerable to a large variety of threats such as malware, ransomware, etc. Overall, the health care industry significantly lags behind other industries in terms of cybersecurity and coupled with a lack of digital literacy among staff mostly working from home, makes it a prominent target. Additionally, the increase in demand for certain goods such as PPE and other protective merchandise such as masks, gloves, etc, are exposing health services and even governments to digital scams, especially in the form of phishing attacks. As health services need these essential items, they can be targeted by adversaries via luring emails with the intention of stealing sensitive information (Hoffman, 2020; Jalali et al., 2020; Kim et al., 2020; Ronquillo et al., 2018; Sardi et al., 2020; Schneck, 2020).

Table 1
Technology used in the health sector during the Covid-19 Pandemic

Type	Health sector
Hardware Technology in healthcare	Computerized tomography, Mobile Devices, Computers, Robots, Video devices, Sensors
Software Technology in healthcare	Zoom, Google Meet, WhatsApp, Facebook Messenger, Computer or mobile app, Google App, Online Survey, Electronic Health Records, Youtube, Twitter, Email, Facebook, X-ray
Hybrid Technology in healthcare	Artificial Intelligence Internet of Things Virtual Reality
Providers to Various User Groups in the health sector	Radiologists, Surgeons, Nurses, Psychologists, Urologists, Health Care Professionals Emergency Service Provider, X-Ray Technician, Hospital Managers, Caregivers, Physical Therapists, Medical Librarians, ENT Specialists, Ophthalmologists, Head and Neck Surgeons, Rheumatologists
Recipients in Various Groups in the field of health	Urology Patients, Infected Individuals, Emergency Room Patients, Cancer Patients, Orthopedic Patients, Total Joint Arthroplasty Patients, Elderly Patients, Musculoskeletal Patients, Mental Health Patients, Diabetes Patients, Critically Endangered Patients, Oral Disease Patients, Cirrhosis Patients, Geriatric Patients, Low Risk Patients
Technology Used in Various Activities in the health sector	Health Services, Communication, Patient Monitoring, Virus Diagnosis, Consultation, Imaging, Patient Assessment Virus Detection, Filter

B. Cyber Attacks in the Health Sector During the COVID 19 Pandemic

The COVID-19 pandemic has become the biggest security threat this decade because it has successfully threatened various aspects of human life, including social, health, economic, and political. Although this virus disrupts and threatens the existence of the country, the threat it poses cannot be categorized as a form of traditional security threat. This is because COVID-19 is not a threatening entity in a 'militaristic' context like traditional security threats. This is more accurately categorized as more of a security challenge that has an effect on public health that is capable of causing further harm to human security (Nurhasanah et al., 2020). Cyber-attacks during the pandemic are a significant double challenge for the people of Indonesia. There has been an increase in internet users in Indonesia by 17% or around 25 million users in 2020 (Datareportal, 2020a). Furthermore, social media users also experienced an increase of 12 million users or an increase of 8.1% (Datareportal, 2020a). This then makes the internet a substitute arena for carrying out human activities during the pandemic. This massive increase has then become an easy target for cyberattacks during the pandemic. UNODC strengthens the argument by stating that whenever a new crisis arises, criminals will see opportunities to exploit vulnerable victims because they are faced with situations of fear, uncertainty and doubt (UNODC, 2020).

Table 2
Cyber Attacks During the COVID 19 Pandemic

No	Type	Country	Researcher
1	Phishing, Malware	China	Henderson, et al 2020
2	Hacking	Czech	Rosso,2020
3	Phishing, Malware, Financial fraud	Philippines	Pilkey, 2020
4	Financial fraud, Malware, DDoS	USA	Kaspersky, 2020; Pranggono and Arabo,2020
5	Phising, Malware	Indonesia	Annef, 2021

No	Type	Country	Researcher
6	Phishing	Germany	Pranggono and Arabo,2020
7	DDoS	France	Pranggono and Arabo,2020
8	Malware	UK	Pranggono and Arabo,2020
9	Phishing	Taiwan	Pranggono and Arabo,2020
10	Malware	Canada	Pranggono and Arabo,2020

Cyber-attacks not only threaten personal and economic security, but also have potential threats to human collective security. Ransomware cases that occurred during the pandemic successfully paralyzed the activities of Universal Health Service (UHS) health facilities in the United States (Coverage 6, 2020). This then does not rule out the possibility of the threat of cyber and physical attacks in health facilities in Indonesia. Health facilities are critical entities during a pandemic. The inhibition or even the paralysis of the digital facilities of a health institution can result in security threats to public health. (Schaeffer et al., 2009) formulate the threat scale in cyber security, this threat scale is categorized based on the resulting impact. The threat scale is divided into 5 stages, namely; first, the low risk posed by hackers who manage to hack the system and create minor damage that has an impact on the business such as; second, the moderate risk posed by embedding malware on the network that could cause malfunctions and potentially create significant damage in financial losses; third, the risk is medium-high when hackers manage to obtain data and information in the form of personally identifiable information (PII); fourth, the high risk of being described as an 'insider' attack, this type of attack has the potential to result in the leakage of crucial organizational information; fifth, critical risk, is illustrated by hackers who manage to break into the system and can access PII as well as financial information and confidential information of the organization.

C. Mitigating and preventing cyber-attacks in the Health Sector During the COVID 19 Pandemic

Mitigating and preventing cyber-attacks are not a trivial task. According to (Furnell & Shah, 2020; Malecki, 2020; Pedley et al., 2020) there are practical approaches that can reduce the risk of cyber-attacks while WFH :

1) User Education: Security is only as strong as its weakest link. People are considered the weakest link in many security systems. Therefore, developing cybersecurity awareness among users by means of constant training is important to reduce the risks of cyber-attacks on an organization. A recent study shows that only 11% businesses have provided cybersecurity training to non-cybersecurity employees in the past year.
2) Virtual Private Network (VPN): VPN is an encrypted communication channel between two points on the Internet to protect the data that is sent and received. The use of a VPN to surf the Internet is the new normal. A VPN provides two aspects of security: confidentiality and integrity and allows organizations to extend security policies to remote workers.
3) Enable multi-factor authentication (MFA): MFA strengthens security by requiring a username and password plus a one-time code sent to mobile phone via SMS or an authentication app. MFA is an important factor to mitigate against password guessing and theft such as brute force cyber-attacks. An employee attempting to access her company's network from home will need to provide both her username and password and a one-time code sent to her mobile phone to verify her identity before being allowed to access the internal network.

4) Ensure all devices firmware is up-to-date: Ensure that all devices and equipment firmware/ OS are up-to-date with the latest security patches implemented to inoculate them against known vulnerabilities. Regular and up-to-date patches may reduce the risk of a zero-day attack.
5) Ensure that up-to-date anti-malware software is activated in all network connected devices: Cyber criminals targeting vulnerable people by spreading various types of malware. As millions of new malwares and its strain are generated every year, regular and up-to-date anti-malware may reduce the risk of cyber-attacks caused by malware.
6) Enable strong company online policy: Organizations have had little or no time to prepare for the WFH scenario. Robust and comprehensive WFH policy is necessary to protect data and prevent cyber-attacks. Strong WFH policies include avoiding holding sensitive work conversations in public, use only company-approved video and audio conference lines, etc. The policies should also include a robust and proven recovery plan and backup strategy. It is also essential to have these plans a regular test as a recent study highlighted that 46% businesses only test their recovery and backup plans once a year or less.
7) Segmentation and separation: Move away from an "all-in-one" single purpose device and network. Divide a network into different trusted zones: home office network (high trust level), guest and home entertainment network (low trust level) and Internet zone (untrusted). In smart homes, the IoT devices should be isolated in a separate Wi-Fi network. By isolating the IoT devices on a separate network segment, any compromise of an IoT device will not automatically grant access to a user's primary devices such as a corporate laptop.
8) Physical security of home office: It is important to physically protect home office devices. Practical approaches include ensuring that work devices are not left unattended, use a lock screen or lock the laptop, always log off devices after use, etc.

Table 3
Health sector security solutions From Cyber Attack

Solution	Method
Apply endpoint device management tools	- Apply perimeter-based defense (antivirus, firewalls) for protection against cyberattacks - Restrict the technologies and devices used by health staff to remain compliant with security regulations such as HIPAAa during pandemics - Adapt the NISTb approach to manage security IoTc medical devices
Secure the remote work environment	- Apply multifactor authentication - Apply a chaotic map–based authenticated security framework for remote point of care - Apply remote access monitoring such as the NHSd attack surface reduction rules - Apply perimeter security solution such as NHS Secure Boundary to enable secure access NHS Digital - The health care sector needs to ensure data protection mechanisms for securing system access and transmitting data
Raise security awareness	- Apply a holistic, integrated approach to improve staff awareness, competence, and mitigation of threats - Implement cybersecurity training programs and cybersecurity awareness campaigns Gordon et al - Apply the NCSC'se Board Toolkit to raise board-level security awareness NHS Digital - Provide comprehensive employee training and education to enable the identification and assessment of risks - Implement a positive organizational climate to influence people's behavior

Solution	Method
Ensure business continuity	- Apply a self-assessment tool such as the NHS Data Security and Protection Toolkit NHS Digital - Embrace cybersecurity and a develop strong culture of cyber vigilance - Ensure business continuity through data backups, intrusion detection, and prevention systems - Apply a systematic risk assessment of the impacts on health care business operations - Consider cybersecurity insurance in health care
Apply technical controls	- Apply network segmentation to isolate network traffic - Apply general technical controls including encryption, authentication, and authorization - Apply homomorphic encryption that ensures strong security and privacy guarantees while enabling analysis of encrypted data and sensitive medical information - Apply blockchain to facilitate health care interoperability - Apply cryptographic security to address data sharing and storage of patient information across network systems
Policies and legislations	- Laws and regulations can help to combat the issues of medical cyber-physical systems - Security instructions and control designs should be tailored - Regulatory changes or manufacturers should become more security-minded in the medical device design phase - Policymakers may need to alter policies to allow new technological innovations to be applied to health care - The US Congress passed the 21st Century Cures Act to promote patient control over their own health information while protecting privacy and cybersecurity
Incident reporting and cyber threat intelligence support	- NHS Digital issued two high-severity CareCERT alerts (BlueKeep and DejaBlue) and developed a high-severity alert process handbook to facilitate incident reporting and sharing Apply an evidence-based approach, such as the generic security template, for incident reporting and exchange - Establish an international workforce to facilitate cyber threat reporting and exchange to combat pandemic-themed cyber threats
Cybersecurity guidance specific to COVID-19	-The NHS has added guidance on working from home securely in the context of COVID-19 - The United Kingdom's Information Commissioner's Office created an information hub to assist individuals and organizations to manage data protection during the COVID-19 pandemic

During the pandemic, healthcare organizations dealing with COVID-19 have been the principal target of persistent cyber-attacks. It is imperative that healthcare organizations protect their valuable data and assets from cyber-attacks by improving their defense. Two important components as regards detecting malicious behavior that can compromise the security and trust of a network are intrusion detection system (IDS) and security incident and event management (SIEM). Typically, an IDS employs anomaly detection, stateful protocol analysis (aka deep packet inspection), signature matching or a combination of all three techniques (hybrid) to analyze incoming cyber-attacks. Due to its ability to detect zero-day attacks more accurately, AI-based anomaly detection IDS is growing in popularity to detect cyber-attacks. Furthermore, it is important for healthcare organizations to take a comprehensive approach to cybersecurity and not to view security from a technological perspective only, but in the framework of processes. Examples of a comprehensive approach to cybersecurity include the CERT Resilience Management Model (CERT-RMM), risk management, and incorporating cybersecurity into the strategic planning and budgeting process (Bhuyan et al., 2020; Malecki, 2020).

CONCLUSION

The COVID-19 pandemic situation is a type of non-traditional security that has a broad impact on various aspects of human life, including the health sector. At a time when many countries have responded to the pandemic situation with various restrictive policies to the prohibition of mobilization, people are adapting by shifting to a new landscape of activity. The cyber world is then used by the community to continue to run productivity. This then has implications for the increase in internet users globally, including Indonesia. Some of the cyberattacks include the practice of phishing emails targeting individual and corporate entities, ransomware targeting healthcare facilities and companies. Further research is needed, especially exploring research on cyber-attacks during a pandemic from the point of view of implementation of cyber security.

REFERENCES

Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., Kumar, S., Levy, M., Kedia, S., & Dasgupta, D. (2020). Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. *Journal of Medical Systems*, *44*(5), 1–9. Google Scholar

Boddy, A., Hurst, W., Mackay, M., & Rhalibi, A. El. (2017). A study into data analysis and visualisation to increase the cyber-resilience of healthcare infrastructures. *Proceedings of the 1st International Conference on Internet of Things and Machine Learning*, 1–7. Google Scholar

Datareportal. (2020a). *Digital 2020: Indonesia*. https://datareportal.com/reports/digital-2020-indonesia

Datareportal. (2020b). *Digital 2020: July Global Statshot*. https://datareportal.com/reports/digital-2020-july-global-statshot

Furnell, S., & Shah, J. N. (2020). Home working and cyber security–an outbreak of unpreparedness? *Computer Fraud & Security*, *2020*(8), 6–12. Elsevier

Hoffman, D. A. (2020). Increasing access to care: telehealth during COVID-19. *Journal of Law and the Biosciences*, *7*(1), lsaa043. Google Scholar

Jalali, M. S., Bruckes, M., Westmattelmann, D., & Schewe, G. (2020). Why employees (still) click on phishing links: investigation in hospitals. *Journal of Medical Internet Research*, *22*(1), e16775. Google Scholar

Kim, D., Choi, J., & Han, K. (2020). Risk management-based security evaluation model for telemedicine systems. *BMC Medical Informatics and Decision Making*, *20*(1), 1–14. Google Scholar

Kotenko, I., & Chechulin, A. (2013). A cyber attack modeling and impact assessment framework. *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, 1–24. Google Scholar

Malecki, F. (2020). Overcoming the security risks of remote working. *Computer Fraud & Security*, *2020*(7), 10–12. Google Scholar

Munawar, Z. (2017). Penggunaan Profil Media Sosial Untuk Memprediksi Kepribadian. *Tematik: Jurnal Teknologi Informasi Komunikasi (e-Journal)*, *4*(2), 18–37. Google Scholar

Nurhasanah, S., Napang, M., & Rohman, S. (2020). COVID-19 As A Non-Traditional Threat To Human Security. *Journal of Strategic and Global Studies*, *3*(1), 5. Google Scholar

Offner, K. L., Sitnikova, E., Joiner, K., & MacIntyre, C. R. (2020). Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation. *Intelligence and National Security*, *35*(4), 556–585. Google Scholar

Pedley, D., Borges, T., Bollen, A., Shah, J. N., Donaldson, S., Furnell, S., & Crozier, D. (2020). *Cyber security skills in the UK labour market 2020*. Department for Digital, Culture, Media & Sport. Google Scholar

Ronquillo, J. G., Erik Winterholler, J., Cwikla, K., Szymanski, R., & Levy, C. (2018). Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information. *JAMIA Open*, *1*(1), 15–19. Google Scholar

Sardi, A., Rizzi, A., Sorano, E., & Guerrieri, A. (2020). Cyber risk in health facilities: A systematic literature review. *Sustainability*, *12*(17), 7002. Google Scholar

Schaeffer, B. S., Chan, H., Chan, H., & Ogulnick, S. (2009). *Cyber Crime And Cyber Security: A White Paper For Franchisors, Licensors, and Others*. CCHpublications. Google Scholar

Schneck, P. A. (2020). Cybersecurity during COVID-19. *IEEE Security & Privacy*, *18*(06), 4–5. Google Scholar

Strunk, J. L., Temesgen, H., Andersen, H., & Packalen, P. (2020). Correlation of Chest CT and RT-PCR Testing in Coronavirus Disease. *Radiol. Soc. North Am*, *80*(2), 1–8. Google Scholar

Tsakalidis, G., & Vergidis, K. (2017). A systematic approach toward description and classification of cybercrime incidents. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *49*(4), 710–729. Google Scholar

UNODC. (2020). *COVID-19: Cyber Threat Analysis*.

Weil, T., & Murugesan, S. (2020). IT risk and resilience—Cybersecurity response to COVID-19. *IT Professional*, *22*(3), 4–10. Google Scholar

WHO. (2021). *WHO Corona Virus Disease (COVID-19) Dashboard*. Google Scholar