Commentary

All India Institute of Medical Sciences (AIIMS), Delhi: Cyberattack Puts Digitalisation Under Scanner

IMIB Journal of Innovation and Management
2(2) 299–306, 2024
© The Author(s) 2024
DOI: 10.1177/ijim.241240911
jim.imibh.edu.in

Priyanka Gandhi[1] and Sonal Pahwa[2]

Abstract

'I Dream of a Digital India where cyber security becomes an integral part of National Security'—Narendra Modi
Fulling this dream one as to realise the fact
'Cyber Security is not easy. But it comes down to three basic principles—PROTECT, DETECT AND RESPOND as early as possible'—Advent from AIIMS Case
The All India Institute of Medical Sciences (AIIMS), a top public medical research facility and hospital with headquarters in New Delhi, India, announced a sophisticated cyber-incident on its servers on 23 November 2022. Several patient care services were rendered unavailable as a result of the incident, including registration, admission, billing and discharge. Several news sources claim that this cyber event, which affected the e-services of the AIIMS (New Delhi) starting at 7:00 a.m. on 23 November 2022, was of the ransomware variety. The testing runs of the e-hospital server were successful, and the majority of the lost data had been recovered during the previous few days, according to AIIMS authorities' confirmation on 6 December 2022. The case provides background on the healthcare industry and a brief analysis of the incident, along with the measures taken to prevent such attacks in the future.

Keywords

Digitalisation, healthcare, AIIMS, cyberattack

[1] Jagan Institute of Management of Studies, Rohini, New Delhi, India
[2] Bhagwan Parshuram Institute of Technology, Rohini, New Delhi, India

Corresponding author:
Priyanka Gandhi, Department of Management, Jagan Institute of Management Studies, Rohini, New Delhi 110085, India.
E-mail: priyankapunyani@jimsindia.org

Position in the Course

IT application and security in business, cybersecurity at undergraduate and postgraduate levels.

Teaching Objectives

1. To empathise the learner with the behaviour that must be adopted while using cyber technology.
2. To develop the learner capability to identify, analyse and remediate computer security breaches.
3. To get insight to the contingency plan for protecting the data online.
4. To emphasise the need to enhance the cybersecurity protection measures and the conduct of regular cyber audits.

Introduction

Industry Overview

The healthcare system in India is primarily provided by public-sector and private-sector facilities. The public healthcare system is managed by the government and aims to provide healthcare for all. This includes government-funded large super-specialty and multi-specialty hospitals located in Tier I and Tier II cities with all the medical facilities and infrastructure. In addition to this, district and tehsil-level hospitals provide medical services to the people in towns, and at the village level, primary healthcare centres provide services in remote areas. The private sector provides services on a chargeable basis and caters to the demands of people who either pay themselves or have some health insurance (Klecun, 2016).

According to NITI Aayog (2019), the healthcare industry is an emerging and ever-growing industry. With advancements in technology in the last couple of decades, substantial efforts have been made to support healthcare practices with information and communication technologies. Modern healthcare delivery models incorporate tech-savvy medical infrastructure along with patient-centric services for monitoring and sharing health-related data. For accurate and early diagnosis, there is a requirement to increase health data utilisation by implementing technologies like machine learning, data analytics and artificial intelligence (Gandhi, 2022).

There has been an exponential growth in healthcare infrastructure in the last couple of decades in India. Indian healthcare markets and assets have grown substantially with technological advancements. Revised government policies are boosting many medical institutes, and the government is encouraging medical colleges to be on par with international standards (Saxena et al., 2020, Saxena & Mayank, 2021).

As per industry trends, the entire focus of healthcare delivery is on creating a patient-centric, holistic environment rather than being just disease-centric. The change in approach is because most of the health issues being faced by people today are due to poor lifestyles and eating habits. Science has proven that health disorders are also connected with an individual's behaviour, preferences and topographical location. The health data required for the patient-centric approach is not easily available. Some critical information can be accessed only by compiling multiple datasets, which are maintained separately by different healthcare providers, and sometimes complete treatment records are missing, resulting in incorrect diagnoses and poor lines of treatment. The quality of such data is questionable for analysis purposes. As a result of modernisation and the use of technology in our daily lives, many lifestyle-related diseases such as diabetes, high blood pressure, cholesterol and liver problems caused by overconsumption of alcohol have replaced communicable diseases. Their management requires customised healthcare and treatment plans with a focus on self-care (Fullman et al., 2018).

According to best practices, health data should be kept confidential to prevent its misuse. Some of the popular techniques to ensure privacy are generalisation, anonymisation, role-based access control, perturbation and encryption.

Background of Organisation

AIIMS was established as an outcome of the health survey and development committee, chaired by Sir Joseph Bhore. In 1946, for India's development, Sir Bhore had already endorsed that a national-level medical centre should be established with the aim of fulfilling the requirement of qualified and competent medical manpower that would serve the nation's growing healthcare demands.

The foundation stone of AIIMS was laid in 1952, as a substantial grant was received under the Colombo Plan from New Zealand. In 1956, AIIMS was established as an autonomous institute via an Act of Parliament with the aim of functioning as the centre of excellence in healthcare delivery and education. It was a huge task to develop clinical and teaching faculties for undergraduate and postgraduate medical education in India and organise and manage the highest order of training facilities in all branches of medicine. As per the Act, AIIMS has comprehensive facilities for patient care, teaching, and research and imparts teaching programmes in medical and paramedical specialties at postgraduate and undergraduate levels (Sharma & Singh, 2018).

Many disadvantaged Indian citizens and people from neighbouring countries benefit from the world-class healthcare services rendered by AIIMS. Its premises are always crowded by patients, the majority of whom cannot afford good-quality treatment anywhere else. The high reputation of AIIMS brings hope to thousands of patients who come here on a daily basis after trying all the possible remedies. Currently, AIIMS is an empire of medical facilities with over 1,500 beds spread across the hospital, including the Cardiothoracic Centre, Dr Rajendra Prasad Centre for Ophthalmic Sciences, Neurosciences Centre, Institute Rotary Centre Hospital and De-addiction Centre. This entire set of facilities serves about 1.5 million OPD and 80,000 IPD patients per year. The number of surgeries performed at AIIMS is over 100,000 every year.

In today's technology-driven environment, data privacy and security are of paramount importance. With a significant amount of healthcare data available for analysis and prediction, maintaining the privacy of individual patients' health data requires lots of effort. At AIIMS, healthcare data security is a big challenge because of the huge numbers of outpatients and inpatients.

Cyber Threat Around the World

As per the combination of data from three major cybersecurity authorities, namely the National Cyber Security Index (NCSI), which is updated on a live basis, the Global Cybersecurity Index (GCI) and the Cybersecurity Exposure Index (CEI), the mean average of the NCSI, GCI and CEI's total scores is used to compute the cyber safety score.

From Table 1, the list of top 10 lowest risk countries for cyber threats is generated based on cyber threat criteria.

Table 1. Top 10 Lowest Risk Countries for Cyber Threats.

Country	National Cyber Security Index (NCSI)	Global Cybersecurity Index (GCI) 2020	Cybersecurity Exposure Index (CEI) 2020*	Cyber-Safety Score (Mean Average of NCSI and GCI)
Belgium	94.81	96.25	81.00	90.69
Finland	85.71	95.78	89.00	90.16
Spain	88.31	98.52	79.00	88.61
Denmark	84.42	92.60	88.30	88.44
Germany	90.91	97.41	75.90	88.07
Lithuania	93.51	97.93	70.30	87.25
France	84.42	97.60	77.20	86.41
Sweden	84.42	94.55	79.00	85.99
UK	77.92	99.54	79.30	85.59
Portugal	89.61	97.32	69.70	85.54

Source: https://seon.io/resources/global-cybercrime-report/

Table 2. Top 10 Highest Risk Countries for Cyber Threat.

Country	National Cyber Security Index (NCSI)	Global Cybersecurity Index (GCI) 2020	Cybersecurity Exposure Index (CEI) 2020*	Cyber-Safety Score (Mean Average of NCSI and GCI)
Afghanistan	11.69	5.20	0.00	5.63
Myanmar	10.39	36.41	9.00	18.60
Namibia	15.58	11.47	32.10	19.72
Libya	10.39	28.78	20.70	19.96
Honduras	22.08	2.20	39.70	21.33
Cambodia	15.58	19.12	29.70	21.47
Mongolia	18.18	26.20	26.20	23.53
Ethiopia	32.47	27.74	13.40	24.54
Venezuela	28.57	27.06	19.30	24.98
Nocaragua	29.87	9.00	40.00	26.29

Source: https://seon.io/resources/global-cybercrime-report/

From Table 2, the list of topTop 10 highest risk countries for cyber threat generated based on cyber threat indexes.

Based on the data available, it is very important to analyse and protect the cybersecurity in India

Cyberattack: AIIMS

'I Dream of a Digital India where cyber security becomes an integral part of National Security'—Narendra Modi

Fulling this dream one as to realise the fact

'Cyber Security is not easy. But it comes down to three basic principles – PROTECT, DETECT AND RESPOND as early as possible'—Advent from AIIMS Case.

Digitisation that is 'secure and sustainable' is essential for the Indian economy to take the lead on the world stage. The experience of India with regard to the fundamental changes in governance and socio-economic growth has led to the creation of the digital revolution. Digital India is growing sustainably thanks to the effective use of computing technology, extensive internet access and reliable networking in areas like digital literacy, financial inclusion, rural development and e-governance. However, the use of digital tools in conjunction with sustainable measures has significantly increased the dangers and attacks. The increase in cybercrime in recent years has had a significant impact on the long-term expansion of the digital economy (Gandhi & Tandon, 2019, 2021).

As the incident quoted in the Indian Express Newspaper dated 8 June 2022,

Chinese hackers launched a ransomware attack on the servers of the AIIMS, the premier medical institute in Delhi. The hack against AIIMS, Delhi, occurred on 23 November and the Delhi Police then filed a complaint of extortion and cyber terrorism on 25 November. It further stated that five of the 100 physical servers had been successfully breached by hackers. Hackers were able to breach 5 physical servers from a pool of 100, which included 40 physical and 60 virtual servers. Because of this ransomware attack that occurred last month, the confidential medical information of millions of patients at AIIMS Delhi was in danger. After this event, the case was handled by a special unit of the Delhi Police in December. According to the investigations, two emails' IP addresses that were discovered in the headers of files that the hackers had encrypted were from Hong Kong and the Henan province of China.

> The senders, according to sources, utilised the email service provider ProtonMail. The top cybersecurity organisation in the nation, the Indian Computer Emergency Response Team (CERT-In), discovered that the hackers used two ProtonMail web addresses, 'dog2398' and 'mouse63209'. According to the sources, CERT-In and Interpol were used to send the encoded web files to these two ProtonMail IDs during the investigation. After further analysis, they discovered that 'dog2398' and 'mouse63209' were created in Hong Kong during the initial first week of November. They also discovered that Henan Province in China sent another encrypted file. Additionally, sources claimed that three ransomware infections—Wammacry, Mimikatz and Trojan—had been found on the targeted servers.

CERT-In, Delhi Cybercrime Special Cell, Indian Cybercrime Coordination Centre, Intelligence Bureau, CBI and National Investigation Agency are all looking into the ransomware incident that may have exposed the records of nearly four crore patients (Liu et al., 2021). The event was examined by the CERT. According to an early investigation, servers were penetrated by unknown threat actors in the AIIMS information technology network as a result of faulty network segmentation, which led to operational interruptions owing to the non-functionality of essential applications, the author added. The complete data for online hospital services has been restored on new servers after being recovered from a backup server that was unaffected. After two weeks following the cyberattack, the majority of the capabilities of the online hospital application, including new patient registration, appointments, new admissions, discharge work, etc., have been restored.

Future Outlook

Counter plan: Created by the Computer Emergency Response Team (Rehman et al., 2022; Saini, 2021).

1. To combat cyberattacks and cyberterrorism, CERT-In had developed a Cyber Crisis Management Plan that was to be adopted by all of the ministries and departments of the union and state governments, as well as their organisations and critical sectors.
2. To inform health sector entities about the most recent cybersecurity risks, CERT-In has sent special advice to the Ministry of Health and Family Welfare on security practices to improve the resilience of health sector entities. Cybersecurity incidents must be tracked and monitored by CERT-In.
3. In August 2022, ‘India Ransomware Report H1-2022’ was released, detailing the most recent ransomware attacker strategies as well as incident response and mitigation techniques.
4. AIIMS, Delhi, took immediate action to improve security, including endpoint hardening, strict firewall policies and network segmentation to secure all of the institute’s data.

A committee was formed to propose a data privacy framework to be implemented for the health industry.

- The legislation must be adaptable and take into account newly developed technologies.
- Both public and private sector organisations must abide by the law.
- Any data processing should be accountable to the entities managing the data.
- Data processing and analysis must be kept to a minimum.
- A strong statutory authority should be in charge of enforcing the data protection framework.

More Recommendations

1. It is very essential to do proper identification of attributes affecting cybersecurity in India, and the framework and policy must be in accordance with these attributes.
2. The cybersecurity policy must be adaptive, evolving and tailored to meet new problems and requirements.
3. While adapting and framing any cybersecurity initiative, it is very essential to involve all stakeholders' participation, and the government could be the driving force behind the implementation.
4. An effective study of other nations' cyber protection initiatives can help our country in framing and implementing cyber initiatives in India.
5. Any nation's cyberspace cannot be safeguarded without a complete policy for all aspects of cybersecurity. If all governments agree on fundamental principles and implement a global cybersecurity strategy, cyberspace can become a safer place.
6. Extensive and immediate implementation of blockchain and other technologies has the capability to change the cybersecurity domain (Dua, 2023).

Acknowledgement

The authors are grateful to the anonymous referees of the journal for their extremely useful suggestions to improve the quality of the paper. Usual disclaimers apply.

ORCID iDs

Priyanka Gandhi https://orcid.org/0000-0002-0605-8081
Sonal Pahwa https://orcid.org/0009-0007-1560-2732

References

Dua, A. (2023). Review of adoption theories in the context of blockchain. *IMIB Journal of Innovation and Management*, *1*(1), 46–57.

Fullman, N., Yearwood, J., Abay, S. M., Abbafati, C., Abd-Allah, F., Abdela, J., Abdelalim, A., Abebe, Z., Abebo, T. A., Aboyans, V., Abraha, H. N., Abreu, D. M. X., Abu-Raddad, L. J., Adane, A. A., Adedoyin, R. A., Adetokunboh, O., Adhikari, T. B., Afarideh, M., Afshin, A., & Lozano, R. (2018). Measuring performance on the Healthcare Access and Quality Index for 195 countries and territories and selected subnational locations: A systematic analysis from the Global Burden of Disease Study 2016. *Lancet*, *391*(10136), 2236–2271.

Gandhi, P. (2022). A new era in healthcare marketing through digital transformation and CRM. *International Journal of Health Sciences*, *6*(S1), 13300–13310. https://doi.org/10.53730/ijhs.v6nS1.8608

Gandhi, P., & Tandon, N. (2019). *Application of web data mining techniques in CRM for its support to health industry* [Paper presented]. Proceedings of International Conference on Advancements in Computing & Management (ICACM). https://ssrn.com/abstract=3446619orhttp://doi.org/10.2139/ssrn.3446619

Gandhi, P., & Tandon, N. (2021). To assess the impact of CRM implementation in health industry. *Vidyabharati International Interdisciplinary Research Journal*, (Special Issue 10), 126–129. http://www.viirj.org/specialissues/SP10/Part%201.pdf

India Ransomware Report. (2022). https://www.certin.org.in/PDF/RANSOMWARE_Report.pdf

Klecun, E. (2016). Transforming healthcare: Policy discourses of IT and patient-centred care. *European Journal of Information Systems*, *25*(1), 64–76.

Liu, X., Deng, R. H., Choo, K.-K. R., & Yang, Y. (2021). Privacy-preserving reinforcement learning design for patient-centric dynamic treatment regimes. *IEEE Transactions on Emerging Topics in Computing*, *9*(1), 456–470.

NITI Aayog. (2019). *Healthcare system for new India: Building blocks—Potential pathway to reform*. Retrieved August 1, 2020, from https://niti.gov.in/sites/default/files/2019-11/NitiAayogBook_compressed.pdf

Rehman, T., Surendran, G., & Krishnamoorthy, Y. (2022). Developing counter strategy for information warfare in health sector–sifting ‘real’ from ‘fake’ news. *International Journal of Medicine and Public Health*, *12*(2), 46–49.

Saini, M. (2021). Preparing for cyberwar-A national perspective. https://www.vifindia.org/article/2012/july/26/preparing-for-cyberwar-a-national-perspective

Saxena, A. B., Aggarwal, D., & Sharma, D. (2020). Covid19 impressions: Health aspects of new educational model-stakeholders perspective. *Bioscience Biotechnology Research Communications*, *13*(10), 256–261.

Saxena, N., & Mayank, V. (2021). Scourge of cyber fraud during Covid-19: Challenges and resolutions. *The Indian Police Journal*, *1939*, 85–108.

Sharma, L., & Singh, V. (2018 October). *India towards digital revolution (security sustainability)* [Paper presented]. 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4) (pp. 297–302).