IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 30, 2021, accepted January 16, 2022, date of publication January 21, 2022, date of current version February 3, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3145372

Digital Healthcare - Cyberattacks in Asian Organizations: An Analysis of Vulnerabilities, Risks, NIST Perspectives, and Recommendations

KAMALANATHAN KANDASAMY[1], SETHURAMAN SRINIVAS[2,3], KRISHNASHREE ACHUTHAN[1], (Senior Member, IEEE), AND VENKAT P. RANGAN[4]

[1]Amrita Center for Cyber Security Systems and Networks, Amrita Vishwa Vidyapeetham, Amritapuri Campus, Kollam, Kerala 690525, India
[2]Information Security Program Executive, San Francisco, CA 94582, USA
[3]Amrita Vishwa Vidyapeetham, Amritapuri Campus, Kollam, Kerala 690525, India
[4]Amrita Vishwa Vidyapeetham, Ettimadai Campus, Coimbatore, Tamil Nadu 641105, India

Corresponding author: Kamalanathan Kandasamy (kamalanathan@am.amrita.edu)

ABSTRACT Cyberattacks on healthcare institutions are on an upsurge all over the world. Recently, Asian hospitals have become targets of numerous cyberattacks. While Western countries like the United States have implemented security-related laws, policies, standards, and other protective measures to deal with the healthcare cyberattacks, Asian countries are lagging. The Healthcare insurance portability and accountability act (HIPAA), enacted by the United States federal government, is a classic example of a law that has been in existence for a quarter-century now. Awareness about electronic health records (EHR) and their importance is increasing in Asia. Many hospitals and healthcare systems successfully implement solutions to protect healthcare data, including sensitive patient data. However, protecting healthcare data involves a sophisticated technology and compliance-driven approach due to the high value associated with the data. In this research, an earnest attempt is made to investigate the recent cyberattacks in Asian healthcare institutions. Based on the investigation, five types of cyberattacks are found to dominate Asian healthcare institutions. A detailed analysis of these attacks, their vulnerabilities, and associated risks are performed as a part of this study. In many countries with higher cybersecurity maturity, risk frameworks are successfully employed to manage the risks associated with healthcare data. In this study, the cyberattacks on Asian healthcare institutions are also analyzed through the lens of the National Institute of standards and technology (NIST) risk framework. Based on the literature review, a few unique recommendations are included in this research study to be used as risk mitigation measures by Asian healthcare organizations and researchers to manage and improve the growing situation of cyberattacks.

INDEX TERMS Cyberattacks, healthcare, vulnerability, risk, vulnerability management, risk management, ransomware, malware, data breach.

I. INTRODUCTION

The Healthcare industry has been rapidly migrating from paper-based systems to electronic health records (EHRs) systems to provide efficient and cost-effective services. EHR has brought a lot of improvement in patient care, diagnosis of diseases, accessibility of information, and even in medical practices [1]. Access to healthcare applications and data has become ubiquitous, increasing the cyber-attack surface area. The arrival of the Internet of Things (IoT) technology in healthcare is an example of technological sophistication impacting the attack surface of healthcare IT systems [2]. Security or privacy violations in healthcare information technology might severely affect patients' treatment and overall health conditions. Data security standards need to be improved to bring about better outcomes in the diagnostic and treatment process of individual patients [3].

The associate editor coordinating the review of this manuscript and approving it for publication was Jiafeng Xie.

A. WORLDWIDE HEALTHCHARE CYBERATTACKS

Several major healthcare data breaches have been reported in recent times. In 2018, the number of healthcare data breaches was 536, out of the total 2216 data breaches spanning 65 countries, with the impact on the healthcare industry

being the maximum [4]. In 2019, the number of worldwide healthcare data breaches was 505, resulting in the exposure of 41.2 million healthcare records [5]. The number of individuals affected by healthcare data breaches was 157.40 million in the last five years [6].

Healthcare data has become the target for hackers due to its demand. Administrative data, electronic health records, clinical data are the different types of healthcare data. Medical data has a higher value than credit card information in the black market [7]. A systematic literature review on cyber-risk in the healthcare sector presented in [8] concludes that the literature lacks research contributions to counter the healthcare sector's cyber risk management challenges and highlights the scientific community's insufficient attention to this topic. Cyberattacks are the most frequent causes of medical data breaches [9]. Healthcare systems collect and preserve patient data in their databases, electronic medical recording (EMR) systems, order communication systems (OCS), and picture archiving and communication systems (PACS) [10]. As data security is an inherent part of cybersecurity, these cybersecurity risks pose a grave danger to patient data, leading to patient information leakage, patient misdiagnosis, and mistreatment [11]–[13]. According to the Cybersecurity Survey by Healthcare Information and Management Systems Society (HIMSS), nearly 60 percent of hospital representatives and healthcare IT professionals in the US said that email was the most common point of information compromise [14]. Hackers commonly employ phishing scams and other forms of email fraud.

B. HEALTHCARE CYBERATTACKS IN ASIA

Based on the cyberattacks data on Asian healthcare organizations, gleaned from legitimate academic data sources and technology news articles, it is found that five significant categories of cyberattacks dominate these data sources, as given in Table 1 below. In this research, a sincere attempt is made to analyze the vulnerabilities and risks associated with these five types of cyberattacks. The popular National Institute of Standards and Technology (NIST) risk assessment framework and its principles are explored in the light of these attacks [15]. Given the relatively lower levels of maturity associated with information risk management in Asian health care organizations, analytical exploration of the risks inherently connected to these cyberattacks becomes an imminent need. Asia pacific region scored low in the Global Cybersecurity Index and Cyber Maturity index [16]. This research study has chosen the Asian healthcare systems as they are exposed to many cyberattacks due to the lack of security maturity [13]. In 2018, one of the most significant data breaches happened in Singapore, exposing 1.5 million health records of patients [17], [18]. The hackers have accessed the sensitive data by compromising a single SingHealth workstation with malware and were then able to obtain privileged account credentials to access the patient database. This incident revealed the lack of anti-malware protection.

The phishing attack is yet another frequently occurring attack in Asian healthcare organizations, wherein an attacker impersonates trusted organizations and individuals to steal sensitive data from victims. The number of phishing URLs detected by the Cyber Security Agency of Singapore (CSA) is 47,500 in 2019 alone [17]. The ransomware called WannaCry/ WannaCrypt/WanaCrypt0r 2.0, or Wanna Decryptor, hit nearly all the computers in two hospitals in Jakarta, Indonesia, resulting in the lock-up of IT systems that contained patient records and billing [17], [19].

The Global State of Information Security Survey (GSISS 2016) results show that 65% of Asian organizations' boards do not actively participate in their cyber risk review and the risk management process [20]. In addition, the Asia-specific healthcare cyberattack data extracted from legitimate data sources and academic sources point to a few Asian countries that recently experienced cyberattacks from 2018 to 2020. These countries include Singapore, India, Saudi Arabia, the Philippines, Thailand, Malaysia, and Indonesia [18], [21], [22].

C. ORGANIZATION OF THIS RESEARCH WORK AND CONTRIBUTIONS

This research work is organized into the following sections. Section 2 deals with the categories of cyberattacks in Asian healthcare organizations. Section 3 explains the above cyberattacks in detail, including the root causes and mitigation techniques. The vulnerabilities causing those attacks are described in Section 4. Ontology for vulnerability management is discussed in Section 5. Section 6 discusses the risk management practices for healthcare systems from the perspective of the NIST framework. Section 7 gives recommendations to Asian healthcare organizations in vulnerability and cybersecurity risk management. Section 8 concludes this research with future possibilities in this area.

Towards improving the cyber security posture in Asian healthcare systems, this work contributes to a few novel ideas TO 2020 as briefly listed here.

- Analysis of five significant cyberattacks in Asian healthcare systems and the connected vulnerabilities.
- An innovative means of computing EVPS (Enriched Vulnerability priority Score) to help in prioritizing the vulnerabilities.
- NIST best practices and approaches to handle healthcare risks and vulnerabilities.
- Two scientifically validated self-assessment survey instruments (questionnaires) for vulnerability management and risk management that can be employed in many Asian healthcare IT organizations as a quick self-assessment tool is a unique contribution of this research work.
- Five experts connected to the healthcare IT domain have validated the face and content validity of the above instruments.

II. ASIAN HEALTHCARE INSTITUTIONS – HIGH IMPACT CYBERATTACKS

Asia pacific healthcare cybersecurity market report has epitomized the impact of cyberattacks on the Asian healthcare industry [23]. As per this report, the intensification of the attacks will spur the growth of the healthcare cybersecurity market in Asia. Weak cyber security infrastructure is one of the major contributors to data breaches in healthcare systems in Asian countries. The Asian region has just started implementing cybersecurity best practices in the healthcare industry. Some of the focus areas are risk assessment, awareness and training, and compliance related to healthcare.

A. ASIA CYBERATTACK REPORTS – STATISTICS AND ANALYSIS

Cybersecurity maturity in healthcare traditionally lags other industries, despite increasing concerns around healthcare cyberattacks and breaches [24]. The WannaCry attack in 2017 is a widely recognized example of the potential consequences of cyberattacks on the healthcare sector. WannaCry was a ransomware attack that affected over 100 countries [25], [19]. Table 1 lists the countrywide Healthcare cyberattacks in recent years in Asia. Asia pacific data protection and cybersecurity regulation [26] discusses each country's several data protection laws. Digital Information Security in Healthcare (DISHA) act [27] mainly focuses on healthcare data security in India. The main reasons for the healthcare breaches in Asian countries are lack of proper anti-malware/anti-virus software, poor infrastructure, lack of cybersecurity awareness among the healthcare systems staff, and the absence of vulnerability and risk management processes and practices [23].

III. ASIAN HEALTHCARE INSTITUTIONS – ELABORATION OF FIVE TYPES OF CYBERATTACKS

Healthcare data may be corrupted, stolen, or modified by intrusive cyber agents, causing disruption to the medical treatment of patients and causing identity theft [33]. Even in a cyber-mature country like the USA, several breaches had occurred, including an employee responding to a phishing email with login credentials [34], successful hacking efforts by the Dark Overlord [35], and a multitude of various WannaCry ransomware encryptions [36]. Three thousand seven hundred five healthcare data breaches have been reported to the HHS' (Health and Human Service) Office for Civil Rights in the USA between 2009 and 2020. COVID-19 pandemic has only increased hackers' activity trying to steal the data related to the vaccine [37]. Asian healthcare organizations are no less vulnerable to cyberattacks. This section elaborates on the five major attacks in several healthcare systems in Asia, as highlighted by the literature review in Section 2. In addition, threat scenarios, associated vulnerabilities, possible mitigation techniques, and the ontology of vulnerability management and its relevance are discussed.

A. TROJAN ATTACK

Malware is malicious software installed on someone's device without their knowledge to gain personal information or damage the device, usually for financial gain. Different malware include viruses, spyware, ransomware, and Trojan horses [38]. For example, Trickbot banking trojan is used as a dropper to deploy Ryuk ransomware to cause ransomware attacks in hospitals. There has been a 71% increase in ransomware attacks on the healthcare sector in the USA during October 2020, and Ryuk ransomware was behind 75% of these incidents. A Trojan attack recently hit the Alaska Department of Health and Social Services, and two computers were found to have malicious software that masqueraded as legitimate applications [39]. It is a possibility that the Trojan horse had already created a backdoor through which patients' records were exposed. Trojans generally do not attempt to inject themselves into other files or propagate themselves [40].

Orangeworm is a cybercrime alliance that installs Trojans [41]. Amongst Asia's healthcare organizations, the most significant number of Orangeworm victims are found in India and Saudi Arabia, 7% each [42], [22] as stated in Table 1. Orangeworm group infiltrates the victim's network in an attack instance and deploys a backdoor Trojan called Kwampirs, giving the attackers remote access to the compromised computer. When executed, Kwampirs decrypts and extracts a copy of its primary payload. Before writing the payload to disk, it inserts a randomly generated string into the middle of the decrypted payload to evade hash-based detections. Kwampirs also collects basic information about the compromised computer, including basic network adapter information, system version information, and language settings. One of the largest communities of patients, 1.5 million members (including outpatients) of Singapore's well-known healthcare group (SingHealth) have had their sensitive personal data compromised due to this malware. The hackers accessed the exposed data by compromising a single SingHealth workstation with malware and obtaining privileged account credentials that helped access the entire patient database [18].

B. PHISHING ATTACKS

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. The recipient is tricked into clicking a malicious link, which can lead to the installation of malware or ransomware, leading to loss of sensitive information. [43] observes that, in the context of phishing emails, employee compliance intention and compliance behavior might not be strongly linked, and hence, hospitals must remain vigilant with vulnerabilities that cannot be easily managed. Anti-phishing tools are generally deployed to prevent phishing attacks [44]. Employees should be actively encouraged to question the authenticity of any email that deviates from its standard format. They should carefully consider the sender

TABLE 1. Countrywide healthcare cyberattacks (2018-2020).

Country /Region Affected	Cyber Attack Category	Cyber Attack Description	Year	Impact	Attack Count	Attack Source (academic and news reference)	National Cyber Governance framework
Singapore	Malware Credential Compromise & Phishing	Data breach – Malware attack stealing credentials Malicious phishing URLs	2018 2020	Loss of 1.5. M EHRs	2	**[18]** and News: TechCrunch & ChannelNews Asia [17]	SingCERT and CSA
Hongkong	Ransomware	Ransomware (due to lack of anti-virus and insecure websites)	2018	Data loss	1	**[21]** and The Straits Times, Asia [28] Straits	HkCERT
Indonesia	Ransomware	Ransomware WanaCrypt0r 2.0	2018	IT systems with patient records and billing were locked up	1	**[21]** and Gov insider Asia [29]	Indonesia CERT
Asia pacific	APT	Web defacement and data exfiltration APT attack	2019	Misconfigured IT systems	1	**[30]** and ZDNet [31]	Asia pacific CERT
Saudi Arabia	Trojan	Trojan - kwampirs on medical devices	2018	Device failure	1	**[22]** and Computer weekly [32]	Saudi CERT
India	Trojan	1. Data breach 2. Trojan - kwampirs	2019 2019	68 lakh EHR impacted	2	**[22]** and Gulf news, Computer weekly [32]	DISHA & India CERT

and context and report the email to the organization's security team. All staff should be educated regarding the potential dangers of malicious email attachments. Specifically, staff should never 'verify' any details from an email, click on hyperlinks, or open attachments that may be malicious [45].

There were 9,430 cybercrime cases reported in 2019 in Singapore alone, and the phishing attacks dominate the critical findings released from the Singapore Cyber Landscape 2019 report [35]. The healthcare sector has been the worst hit in Singapore, with the number of phishing attacks multiplying by almost 200 times from January to April 2020 [46] as given in Table 1. According to the Australian Cyber Security Center (ACSS), in 2020, cybercriminals compromised email servers of health sector entities in Australia. This was done to distribute COVID-19 related phishing emails to deploy malicious software, including ransomware [47]. According to the Symantec Internet Security Threat Report (ISTR) 2018 study, Malaysia ranks third for phishing attacks in Asia.

C. RANSOMWARE

Ransomware is a unique subset of malware that limits or blocks users' access by locking the system and data unless a ransom is paid [48]. Outdated operating system (OS) poses severe threats to healthcare devices as new-found bugs are not addressed in the older versions of the OS by the vendor. Attackers could inject malicious code snippets or software and exploit the existing OS bugs [49].

WannaCry ransomware attacks are launched against unpatched healthcare devices, where OS updates were not applied on time. If medical equipment like X-ray machines and anesthetic machines are running on an old and insecure version of Operating systems (e.g., Windows Vista, Windows XP, etc.), ransomware attacks are highly possible [17]. Such unpatched Operating systems run unprotected, insecure, and vulnerable applications with no firewall or protection against malware. It is worth discussing a couple of vulnerabilities that led to Wannacry attacks in this context. CVE-2017-0143 vulnerability allows remote attackers to execute arbitrary code via crafted packets, "Windows SMB Remote Code Execution Vulnerability." WannaCry exploits CVE-2017-0144, a well-known vulnerability in Microsoft Server Message Block 1.0 (SMBv1), to infect endpoints. The security flaw is exploited using an exploit leaked by the Shadow Brokers group, the "EternalBlue" exploit [50].

In May 2017, WannaCry hit hospitals in 150 countries, including Japan, China, Indonesia, and Taiwan [21], as stated in table 1. It brought some major hospitals briefly to a virtual stop, with some turning away patients [17]. WannaCry/ WannaCrypt/WanaCrypt0r 2.0, or Wanna Decryptor hit nearly all the computers in two hospitals in Jakarta, Indonesia, and the IT systems with patient records and billing were locked up [51]. According to Trend Micro, Malaysia ranked third for ransomware attacks [52].

The deployment of any ransomware decryptor and anti-threat toolkit helps to prevent this ransomware attack.

TABLE 2. Asian healthcare organizations - vulnerability heat map.

ATTACK	MEDIUM	HIGH	CRITICAL
Phishing	108	12	2
Ransomware	4	8	1
APT	162	234	98
Trojan	11	87	1
Malware	51	70	7

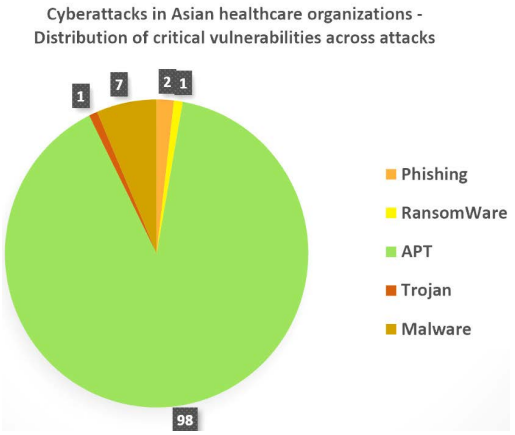

FIGURE 1. Pie chart for critical vulnerabilities for the five types of cyberattacks (taken from "Critical" column from the heatmap shown in Table-2).

The contribution of [53] is an automatic, intelligent, and real-time system to detect, classify, and mitigate ransomware in Integrated clinical environments (ICE). Recommendations [54] for the above-mentioned Wannacry vulnerability CVE-2017-0143 are to a) apply appropriate patches provided by Microsoft to vulnerable systems immediately after performing vulnerability scanning. b) disable version1 of Server Message Block (SMBv1) on all systems and utilize SMBv2 or SMBv3 after appropriate testing. c) run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

D. ADVANCED PERSISTENT THREAT (APT)

An advanced persistent threat (APT) attack is a high-scale attack deployed over a longer duration. It is a selective attack that obtains unauthorized access to information and communication systems to exfiltrate confidential data [30]. The objective of an APT attack is to steal data and sabotage organizational infrastructures or surveillance systems for a long time. The eight-stage process of an APT attack [55] are: (i) Initial Recon, (ii) Initial Compromise, (iii) Establish Foothold, (iv) Escalate Privileges, (v) Internal Recon, (vi) Move Laterally, (vii) Maintain Presence, and (viii) Complete Mission.

The geopolitical landscape and the Covid-19 pandemic were exploited by advanced persistent threat (APT) groups to advance their motives in Southeast Asia in 2020 [56]. In August 2019, an Indian healthcare website was attacked by a Chinese APT group (APT22), and 68 lakh records were stolen [32] as stated in table 1. APT22 has a nexus to China and has been operational since early 2014, carrying out intrusions and attack activity against public and private sector entities [57]. The pie chart in Figure 1 shows that the APT critical vulnerabilities have the most significant share of the pie, indicating that mitigation of APT vulnerabilities is a very high priority for the Asian healthcare sector. [58] aims to facilitate the detection and analysis of Advanced Persistent Threats (APTs) and anomalous activities on healthcare organizations and expand the sector awareness on cyber threats and risks.

E. MALWARE - CREDENTIAL COMPROMISE

Malware (Malicious Software) is a common form of cyberattack which executes unauthorized actions on the victim's system. This includes spyware, ransomware, trojan etc. A classic example of a typical malware attack (credential compromise) is briefed in this section. Credential compromise is the first step during any major cyber-attack. [59] discusses the leaked 100 email accounts via paste sites, underground forums, and virtual machines infected with malware. [60] presents the study of how miscreants obtain stolen credentials and bypass risk-based authentication schemes to hijack a victim's account. In 2018, 1.5 million members of Singapore's largest healthcare group have had their personal data compromised [17]. The hackers have accessed the sensitive data by compromising a single SingHealth workstation with malware and were then able to obtain privileged account credentials with which they accessed the patient database.

IV. ONTOLOGY FOR VULNERABILITY MANAGEMENT AND ITS RELEVANCE

An anatomy of any cyber-attack will always point to three components; vulnerability, threat and the exploit. Of the three components involved in the attack, vulnerability plays a key role either in facilitating or blocking an attack depending on whether the vulnerability was successfully exploited or not. It is important to understand the ontological aspects of vulnerability before scrutinizing the vulnerabilities that are connected with the cyber-attacks explained above.

A. ONTOLOGY FOR VULNERABILITY MANAGEMENT

Ontology is knowledge represented in a formal and structured form. [61] introduced the concept of ontology for vulnerability management (OVM) in their acclaimed work. The standardized language and vocabulary connected with vulnerability management are well integrated in the definition of OVM. For example, Common vulnerability enumerator (CVE) invented by researchers at MITRE are part of

OVM design. OVM supports researchers who attempt to analyze and recommend innovative solutions to vulnerabilities. Ontology for Vulnerability Management (OVM) helps to capture the relationships between IT products, vulnerabilities, attackers, security metrics, and countermeasures. This system introduces the design and reasoning within the ontology with examples in vulnerability analysis and assessment. OVM integrates common standards such as CVE (Common Vulnerabilities and Exposures), Common Vulnerability Scoring System (CVSS), CWE (Common Weakness Enumeration), CPE (Common Platform Enumeration), and CAPEC (Common Attack Pattern Enumeration and Classification) into its model.

B. RELEVANCE OF OVM

OVM lays a solid foundation for this research to further the cause of vulnerability management. OVM defines the key concepts in vulnerability management and captures their inherent nature and relationship with each other. CVSS and its relevance are mentioned in OVM for Information Security Automation Program (ISAP). This research has used many foundational aspects of OVM, the most important being the National vulnerability database (NVD). CVSS scores and NVD are extensively used in this research, both for analysis and recommendations. Failure Mode and Effect Analysis (FMEA) is another theoretical construct applicable for the vulnerability management. Healthcare FMEA includes testing to ensure that the system functions effectively and new vulnerabilities have not been introduced in any aspect of the healthcare information systems [62]. Crown jewel analysis (CJA) refers to identifying those cyber assets that are most critical to an organization's business goals [63], which helps healthcare organizations prioritize cyber assets and apply limited resources effectively for cyber resiliency. OVM, FEMA, and CJA form a solid ontological and theoretical research foundation for vulnerability analysis and research.

V. ASIAN HEALTHCARE SYSTEMS – MAIN VULNERABILITIES

This section describes the different types of vulnerabilities that lead to cyberattacks on the Asian healthcare systems, identified in the earlier sections. In addition, a minor analysis of the cloud-related healthcare vulnerabilities is also included.

A. VULNERABILITIES CAUSING FIVE TYPES OF CYBERATTACKS

A vulnerability that has the potential to be exploited by a threat triggers a risk. Measurement of organizations' preparedness to deal with vulnerabilities depends on the strength of its security program and the policies that govern vulnerability management [64]. National Vulnerability Database (NVD) data enables automation of vulnerability management, security measurement, and compliance [65]. Each vulnerability is categorized into the following types: critical, high, medium, and low. Common Vulnerabilities and Exposures (CVE) is a list of publicly disclosed computer security flaws. Some critical vulnerabilities that were exploited in the cyberattacks in the Asian healthcare systems were extracted from the NVD database. The Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to the threat. In addition, scores are calculated based on the ease of the exploit and the impact of the exploit.

Vulnerability management is the process of identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them. A vulnerability scanner enables organizations to monitor their networks, systems, and applications for security vulnerabilities [66]. Most security teams utilize vulnerability scanners to bring to light security vulnerabilities in their computer systems, networks, applications, and procedures. There are cloud-based, host-based, network-based, and database-based vulnerability scanners. Web Application Attack Audit Framework (W3AF), Open Security Content Automation Protocol (OpenSCAP), Open Vulnerability Assessment Scanner (OpenVAS), and Network mapper (Nmap) are some of the open-source vulnerability scanners.

It is essential to understand the vulnerabilities and severity for each of the five attacks discussed in Sections 1 and 2. A vulnerability heat map is included in Table 2 to summarize the distribution of vulnerability counts across severities and pertains to three years (Jan'2018 – Jan' 2021). These vulnerability counts were extracted from the National vulnerability database (NVD) [65] and are presented here to underscore the importance of mitigating these vulnerabilities by the Asian healthcare organizations.

As mentioned earlier, Table 2 lists some of the vulnerabilities with critical and high severity for the cyber-attacks in Asian healthcare systems. CVSS Scores range from 0 to 10, with ten being the most severe. Some of the high and critical vulnerabilities that have the potential to trigger one of the five attacks, along with their CVE scores, are included in Table 2. These vulnerabilities are extracted from the National vulnerability database (NVD) database. Table 2 is intended for all cybersecurity practitioners and researchers connected to Asian healthcare IT systems.

The Pie chart in Figure 1 is a drill-down of the vulnerability counts from the heat map (Table 2) extracted from NVD as mentioned earlier. It depicts only the Critical vulnerabilities across all five types of cyberattacks. The APT attack has the maximum number of critical vulnerabilities, thereby accentuating the need to prioritize its mitigation. Pie chart is chosen because of the need to underscore the proportion of these attacks in terms of critical vulnerabilities in Asian healthcare systems.

With the above discussion on vulnerabilities, it is amply clear that there is a need for an immediate focus on the vulnerability and risk management practice in Asian healthcare

systems to detect, prioritize, and mitigate the risks created by the vulnerabilities across the five categories of attacks.

B. HEALTHCARE CLOUD-RELATED ATTACKS AND VULNERABILITIES

Advanced Asian countries such as Japan, South Korea, and Singapore provide successful examples of how cloud computing can be used to develop a) nationwide databases of electronic health records, b) real-time health monitoring for the elderly population, c) genetic databases to support advanced research, cancer treatment, and telemedicine [18]. However, despite cloud adoption, almost 39% of healthcare organizations suffered from ransomware attacks in the cloud in 2020 [67]. The other dominant types of security incidents are phishing attacks and data breaches [68]. In general, there are many security risks associated with employing the cloud in healthcare, including failure to separate virtual users, identity theft, privilege abuse, and poor encryption [69]. Cloud-based E-health security and privacy issues and their possible solutions are elaborated in [70]. Among the different Cyber Security Risk Frameworks (CSRF), including NIST, OCTAVE, TARA, and ISO, healthcare industries widely use NIST [71]. NIST also covers the CIA triad (Confidentiality, Integrity, and Availability) and IoT standards. The following section introduces the NIST risk management framework, its suitability, and applicability to Asian healthcare systems.

VI. NIST AND RISK MANAGEMENT FOR ASIAN HEALTHCARE SYSTEMS

This section introduces NIST cyber security framework and analyses its suitability to Asian healthcare systems. NIST's vulnerability management, risk management, and security controls are also analyzed, keeping in view the Asian cyberattacks. This analysis helps to understand the suitability of NIST in Asian healthcare systems.

A. NIST – AN INTRODUCTION

The NIST-CSF (National Institute of Standards and Technology - Cyber Security Framework) is organized into five core functions: identity, protect, detect, respond, and recover to address risk management decisions, threats, and vulnerabilities. The NIST CSF provides a standard structure that is flexible and adaptable for managing cybersecurity risk. NIST risk management framework is currently adopted by many healthcare organizations worldwide as a baseline [72]. Gaps between NIST CSF and other risk frameworks are analyzed. An Information Security Maturity Model (ISMM) is proposed to fill in the gaps and measure NIST CSF implementation progress [73].

Based on the five main functions of NIST, healthcare organizations typically identify physical and software assets, their interconnections, and defined roles and responsibilities along with the identification of current risks and exposure. NIST framework aids in controlling access to digital and physical assets, provides awareness and training to personnel, and includes a recovery plan. NIST Framework can shift the cybersecurity landscape internationally, especially in places that largely favor a voluntary approach to enhancing cybersecurity, including the United Kingdom, Asian countries, and the European Union [74].

B. SUITABILITY OF NIST TO ASIAN HEALTHCARE INSTITUTIONS

NIST framework ensures effective information security risk management using its core elements, implementation tiers, and a profile that aligns with business requirements, financial capabilities, and risk tolerance. The flexibility and adaptability of the NIST Framework [15] allow healthcare organizations to choose NIST for regulation and compliance requirements. NIST Framework is outcome-driven and does not mandate how an organization must achieve those outcomes, and it enables scalability.

NIST SP 800-66R1 explains the information security terms used in the HIPAA Security Rule and the techniques to improve the security standards set out in the Security Rule [75]. NIST is actively developing medical device communication test methodologies and tools to enable consistent and correct communication between medical devices and device gateways across healthcare enterprises [76]. The Information Technology Laboratory of NIST is involved in several healthcare automation activities focused on developing associated test methods, protocols, and specifications for Interoperability. Many stakeholders in critical infrastructure sectors, including the healthcare and public health (HPH) sector, have adopted the NIST Cybersecurity Framework [77]. NISTIR 7804 deals with the technical evaluation, testing, and validation of the usability of Electronic Health Records and helps to ensure that the application user interface is free from critical usability issues and supports error-free user interaction with EHR [78]. It is pertinent to explore NIST's vulnerability principles in the light of the five cyberattacks that form the core part of this research for Asian healthcare organizations.

C. VULNERABILITY MANAGEMENT IN NIST

Vulnerability management is a process of identifying vulnerabilities and mitigating them. The vulnerability scanning process, which is the first step, includes detecting and classifying system weaknesses in networks, communications equipment, and computers [79]. In addition to identifying security holes, the vulnerability scans also provide countermeasures for any threat or attack [80]. Penetration testing (Pentest) is a key part of the vulnerability assessment process used to assess an IT system's ability to withstand intentional attempts to circumvent system security. It is an authorized simulated cyberattack on a computer system performed to evaluate the security of the system [81]. Its objective is to test the IT system from a threat-source viewpoint and identify potential failures in the IT system protection schemes. IT system component areas can include applications, ports, websites, services, networks,

and systems external customers or users access. [82] elaborates the testing and assessment of healthcare data security using the Nmap (Network mapper) tool in Asian hospitals.

NIST framework categorizes vulnerabilities using a tier-based approach. The organization level (tier 1), business process level (tier 2), and information system level (tier 3) are the three tiers. Vulnerabilities related to organizational governance and external dependencies like electrical power, supply chain, and telecommunications are identified at Tier 1. However, most vulnerability identification occurs at Tiers 2 and 3. At Tier 2, process and architecture-related vulnerabilities, including Malware and APTs, are more likely to be identified. At Tier 3, information system vulnerabilities are the primary focus. These vulnerabilities are commonly found in the hardware, software, and firmware components of information systems or in the environments in which the systems operate as per NIST SP800-39 [83]. Phishing, Ransomware, APT, Trojans, and Malware – Credential-Compromise attacks dealt with within this research work will fall under tiers 2 and 3. NVD provides vulnerability scores based on CVSS; this score gives only the severity of the vulnerabilities. Severity describes the impact of the vulnerability but does not directly help in prioritizing it. Given the lesser maturity of the cybersecurity domain in Asian healthcare organizations, a faster and innovative approach to prioritize vulnerabilities will be a welcome approach. This unique proposed approach is described in the next section.

D. ENRICHED VULNERABILITY PRIORITY SCORE (EVPS)

A vulnerability priority score is commonly a rolled-up representation of the priority of a vulnerability. This score helps the cybersecurity team to prioritize the fix for a vulnerability. To prioritize vulnerabilities, one would consider a few more not so common aspects related to the vulnerabilities as follows: (i) if a vulnerability has caused any suspicious security event earlier within the organization, (ii) if the hospital or healthcare system has already encountered the same vulnerability, (iii) if any healthcare system in the country has encountered this vulnerability. The popular CVSS scores are enriched based on the answers (weightage) to questions Q1 through Q5, leading to Enriched Vulnerability priority Score (EVPS). Some vulnerability examples connected to the Asian healthcare cyberattack types discussed earlier in this paper are provided in Table 3. The questions given below help the cybersecurity technical staff to understand these features and build a near-accurate score.

- Q1: Has there been a suspicious security event to exploit this vulnerability at your hospital or healthcare organization?
- Q2: Has this vulnerability been exploited already in your country, in the healthcare domain?
- Q3: Do you have enough technology and resources to implement a solution to this vulnerability?
- Q4: Is there any end-of-life entity (example: operating system) that has gone past the end of life in your organization for this vulnerability? (example: Windows OS expiry)
- Q5: What is the age of this vulnerability in this hospital or healthcare organization? (score would be 0.25 if this vulnerability exists for less than a year, and 0.5 if this vulnerability exists for more than a year)

For questions Q1-Q4, the score is 0.25 if the response is *yes* and 0 if the response is *no*. For example, For the vulnerability ''Windows SMB remote code execution'', Q1 and Q4 answers are *no,* and hence they both get a score of 0. For questions Q2 and Q3, the score is 0.25 each since the response is *yes* for both. Since the age of the vulnerability is more than a year, Q5 gets a score of 0.5. Hence the total score = Base score of $8.1 + 1.0 = 9.1$.

Given the depiction of the cyberattack situation in Asian healthcare organizations in the earlier sections, every organization must have a quick self-assessment process to understand its vulnerabilities. Therefore, the authors have developed a scientifically validated self-assessment questionnaire (SAQ) that vulnerability management practitioners can employ towards this goal.

E. ASIAN HEALTHCARE CYBERATTACKS – VULNERABILITY AND THREAT PAIR

The threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the current controls to determine the likelihood of a future adverse event. The vulnerability and threat pair concept is introduced in the vulnerability identification section of NIST SP800-30 [84]. Vulnerability identification is the first step from the vulnerability sources. Open Web Application Security Project (OWASP) lists the top ten vulnerabilities from an application perspective [85]. Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerability is exploited, such an attack can facilitate severe data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts. OWASP's secure medical device deployment standard serves as a comprehensive guide to the secure deployment of medical devices within a healthcare facility [86]. NIST refers to the NVD database [65] to list the possible vulnerabilities along with their severities. The next section provides the classification of the top five Asian healthcare cyberattacks into NIST tiers, as per the NIST framework.

Table-4 gives the vulnerability/threat action relationship for the top five Asian healthcare cyberattacks, as defined by the NIST tiers. This table is presented to help the reader understand the importance of applying NIST vulnerability management principles in the Asian healthcare IT industry. Bowtie analysis is a very prominent method to identify and analyze the likelihood of Risk [87]. It presents a combination between Fault Tree Analysis (FTA) and Event Tree Analysis (ETA). FTA explores the causes of system-level failures. ETA

TABLE 3. Enriched vulnerability priority scoring (EVPS).

Vulnerability	Base Score	Q1	Q2	Q3	Q4	Q5	Total
Windows SMB remote code execution	8.1	0	0.25	0.25	0	0.5	9.1
Anti-Ransomware Tool was vulnerable to a DLL hijacking	7.2	0	0.25	0.25	0	0.5	8.2
Buffer overflow in PTP (Picture Transfer Protocol) of EOS series digital cameras	8.8	0.25	0.25	0.25	0	0.25	9.8
Browser Proxy allows you to manipulate HTTP requests and responses, capture HTTP content	10	0	0.25	0.25	0	0	10+

TABLE 4. Vulnerability/threat pair for the asian healthcare.

Top Five Cyberattacks in Asia	Vulnerability	Threat action	NIST tier impacted by the vulnerability
Phishing	Email/URL scanner is not employed	Sends phishing URL via email	Tier-3 (software)
Ransomware	Unencrypted data	Encrypts data and demands payment	Tier-2 (Architecture)
APT	Spear-Phishing	Exfiltration of data	Tier-3 (software)
	Ransomware possibilities	Data gets encrypted	
Trojan	Unscanned email attachments	Installs backdoor and accesses the system	Tier-3 (software)
Malware	System and/or email server is not protected	Spying system or data access	Tier-3 (software/Firmware)

is an inductive failure analysis performed to determine the consequences of a single failure for the overall system risk or reliability. ETA and FTA describe the relationships between the undesirable event, its causes, and implications for a systematic hazard representation. A threat-vulnerability pair is a matrix that matches all the threats in a threat listing with the current or hypothetical vulnerabilities that could be exploited by the threats [88]. Figure 2 provides the Bowtie diagram for the threat-vulnerability pair for the five types of cyberattacks experienced by the Asian IT healthcare organizations.

F. NIST ORIENTATION – SECURITY CONTROLS AND RISK MANAGEMENT

In an information security scenario, a risk may be defined as the potential for loss or damage when a threat exploits a vulnerability. From a quantitative perspective, the likelihood and impact are the main components of a risk equation [83]. Risk mitigation in healthcare systems involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended by the cybersecurity risk management journal [89]. Different risk mitigation options are risk acceptance, risk avoidance, risk reduction, and risk transference. Risk mitigation strategy [84] helps organizations choose appropriate mitigation options and implement the proper security controls to mitigate the risks. Healthcare data, considered valuable in the Hacker's market, will attract serious violations leading to security incidents, including data breaches. Therefore, it is worth assessing the security risks associated with the five cyberattacks for Asian healthcare organizations.

NISTIR-8228, which provides considerations for managing IoT cybersecurity and privacy risks, also helps assess the cyber risks of medical devices connected to the internet, i.e., the internet of medical things (IoMT) for healthcare

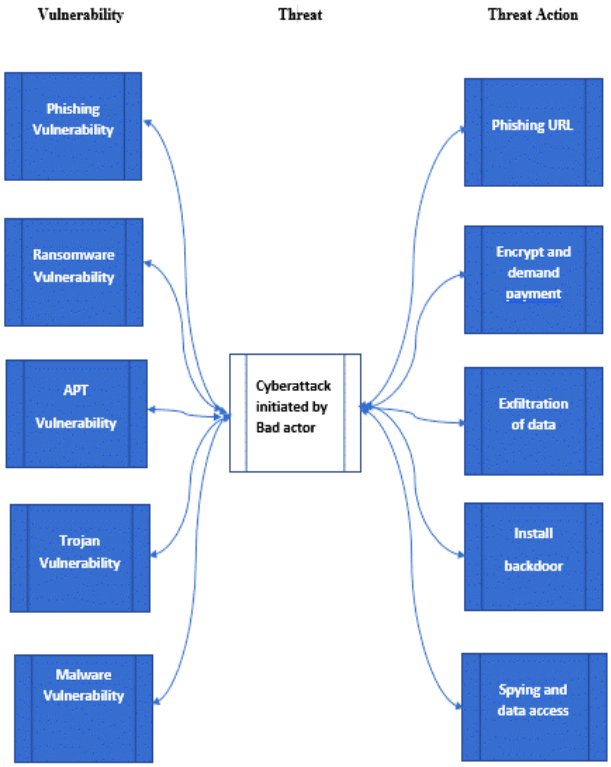

FIGURE 2. Bowtie diagram showing vulnerability/threat pair – asian healthcare cyber attacks.

systems [90]. NIST has technical, management, and operations security controls [84] to avoid, detect, counteract, or minimize security risks. Security countermeasures are specific controls that protect the healthcare business from attacks and are very suitable to the research subject area of this paper. NIST [84], [91] and ISO [92] generally define risk assessment as a holistic process of identifying risks, analyzing and evaluating them through a combination of various inputs from different security assessment sub-processes, such as threat, vulnerability, and impact assessment. [71] explains the holistic analysis of cyber-Risk and its risk vector calculations for IoT devices and then maps the risk vector calculations for Internet of Medical Things (IoMT) devices. Risk management is the process of identifying Risk, assessing Risk, and taking steps on risk mitigation [93]. For the different types of the Asian healthcare cyber-attacks discussed in Section 1, the following subsection investigates the corresponding risk mitigation techniques from the NIST risk management advisories provided in SP800-30 [84] and SP800-39 [83].

G. ASIAN HEALTHCARE CYBERATTACKS – ANALYSIS THROUGH THE NIST LENS

The Asian cyberattacks mentioned earlier are analyzed through the vulnerability and risk management sections of NIST SP800-30 [84] and NIST SP800-39 [83]. For each cyberattack, the recommendations from NIST have been briefly explored and presented here to the research community and the practitioners.

1) PHISHING ATTACK

In general, awareness training given to the IT staff and employees on Phishing attacks orients them on the possibilities of phishing attacks through social media. [94] describes the effect of a mandatory training program for employees that repeatedly clicked on simulated phishing emails. Preventive management security control of NIST SP800-30 explains the importance of conducting security awareness and technical training to ensure that the end-users know their responsibilities in protecting the information systems [84]. Given the Phishing attack data on Asian healthcare institutions provided in Section 3.2, it is of paramount importance that the impacted healthcare IT systems in Asian countries plan on implementing Phishing awareness training with the help of many modern training platforms.

2) RANSOMWARE

As per the HIMSS Healthcare survey conducted in 2018, ransomware contributed 11% of the total healthcare cyberattacks [14]. As discussed in the earlier section, ransomware attacks cause the data to be encrypted by the attackers leading to high ransom demands. Table 1 provides the details on two instances of a Ransomware attack in Asia. Cryptographic keys must be securely managed, and the data needs to be protected using encryption to prevent this attack. Cryptographic key management includes key generation, distribution, storage, and maintenance. Hence, the Cryptographic Key Management concepts from the supporting technical control of NIST risk mitigation [84] are very relevant and applicable to the Asian healthcare IT organizations.

3) MALWARE – CREDENTIAL COMPROMISE

SingHealth attack described in the earlier section was a malware-driven attack [17], [18]. NIST special publication SP800-39 [83] gives the evaluation procedures for responding to such an attack. It also provides details about detecting such an attack and protecting the data. For example, to detect a potential insertion of malware into the hardware, firmware, or software, the following three methods are suggested. (i) providing users with clean laptops; (ii) removing hard drives from laptops and letting them operate from CDs or DVDs; or (iii) having laptops or endpoints go through a detailed assessment before being allowed to connect to organizational networks. A combination of detecting and protective measures can be selected based on the budgetary constraints, consistency with investment management strategies, and privacy protection.

4) ADVANCED PERSISTENT THREAT (APT)

The APT attack is found to have the maximum number of critical vulnerabilities, as explained in the Vulnerability heat map for Asian healthcare organizations (Table 2). The web defacement attack described in Table 1 was a well-orchestrated APT attack. Implementing NIST controls assumes a lot of significance in the context of the Asia cyberattack scenario.

Preventive technical control of NIST SP800-39 [83] methods, including authentication, authorization, access control mechanism, protected communication using encrypted methods, helps to prevent APT attacks. [95] describes a study on cyber threat prediction based on intrusion detection events for APT attack detection. NIST SP 800-66R1 explains the information security terms used in the HIPAA Security Rule [75], which are quite helpful to understand attacks like APT. As a part of risk response to APT attacks, organizational information systems provide a failover mode that helps to ensure that failed components trigger appropriate backup components with similar capability.

5) TROJANS

NIST Computer Security incident handling guide SP800-61R2 gives details on the ports to be checked for trojan horse [96]. It also includes trojan analysis, evidence gathering procedures, and mitigation techniques. The incident response life cycle with four steps: preparation, detection & analysis, Containment eradication & recovery, and the post-incident recovery procedures are elucidated in detail to handle the trojan and similar malware attacks. The preparation step provides introductory advice on preparing to manage incidents and on preventing incidents. The detection and analysis step details the trojan detection mechanisms and incident prioritization. Containment provides time for developing a tailored remediation strategy. Eradication and recovery step is necessary to eliminate components of the incident, such as deleting trojan and disabling breached user accounts, and identifying and mitigating all vulnerabilities that were exploited. Finally, the post-incident activity includes learning and improving that evolves to reflect new threats, improved technology, and lessons learned.

VII. RECOMMENDATIONS FOR HEALTHCARE INFORMATION SECURITY PRACTICE

A good amount of analysis was presented in Sections 3 and 4 on the vulnerabilities and risks associated with Asia's five types of healthcare cyberattacks introduced in Section 2. The analysis was done to bring more awareness and cybersecurity discipline to the cybersecurity practitioners and researchers in the Asian healthcare IT domain. However, it will be a tough climb for organizations to go through the cybersecurity maturity ladder. One of the most daunting challenges will be in procuring the budget that drives all the needed changes that bring up maturity. In 2021, 59% of businesses state that their cybersecurity budget is below its needs [3], [17]. A useful set of self-assessment questionnaires (SAQ), both from a vulnerability and risk management perspective, gleaned from the principles discussed in earlier sections is presented here. These questionnaires can be employed in many of the Asian healthcare IT organizations as a quick self-assessment tool to understand cybersecurity maturity from a vulnerability and risk perspective. This section introduces two self-assessment questionnaires that were field-tested with five experts in the Healthcare IT domain.: the vulnerability Self-Assessment Questionnaire (VSAQ) and the risk Self-Assessment Questionnaire (RSAQ).

A. FIELD TESTING OF QUESTIONNAIRES – CONTENT AND FACE VALIDITY

Field testing involves administering an early version of a survey to a sample of the target audience. A field test typically consists of two components: face validity and content validity [97]. Face validity refers to researchers' subjective assessments of the presentation and relevance of the measuring instrument as to whether the items in the instrument (questionnaire) appear to be relevant, reasonable, unambiguous. The face validity for these two questionnaires was established by validating for comprehensiveness and completeness of the content. All the five field test participants also ensured that the questionnaires (instrument) can be easily filled by them [98]. Content validity is defined as ''the degree to which items in an instrument reflect the content universe to which the instrument will be generalized'' [99]. The CVR (content validity ratio) is a linear transformation of a proportional level of agreement on how many ''experts'' within a panel rate an item (question) ''essential''. The following steps were followed to establish content validity.

1. An exhaustive literature review was done to extract the questions for VSAQ and RSAQ questionnaires.
2. Five experts from the IT healthcare domain assessed each question using a three-point scale with three options; not necessary, useful but not essential, and essential [100].
3. The roles of the five expert members are Hospital Information System Architect, Hospital Information System Manager, Research Professor in Healthcare Information Technology, Healthcare Database Architect, and Information Technology Executive in Healthcare systems.
4. The content validity ratio (CVR) was then calculated for each item by employing Lawshe (1975) 's method [100], as given below.

$$CVR = [ne - (N/2)]/(N/2) \tag{1}$$

''*ne*'' is the total number of panel members who voted ''essential'' for any given question in the questionnaire, and N is the total number of panel members. The final evaluation to retain the question based on the CVR depends on the number of panel members.

5. Items that are not significant at the critical level were eliminated i.e., even if one member of a panel has voted a question as 'not essential', the question is eliminated based on the CVR calculations.

The CVR ratio for each item (question) has been calculated and approved only when CVR = 1 (i.e., when all panel members indicate the item as ''essential'') and rejected the item when the CVR < 1. Few questions were considered as 'not essential' at least by one of the panel members. CVR value for such questions was computed as 0.6, and hence these questions were removed from the group.

TABLE 5. Vulnerability self-assessment questionnaire (VSAQ).

Type	Questions	Asia attack-based weightage (W)	Base score (B) (Yes=10, No=0)	Total Score (W*B)
Vulnerability Management Culture	Q1: Does the information security team proactively identify medical devices related vulnerabilities based on a pre-scheduled vulnerability scanning routine?	**15**	**0**	**0**
	Q2: Is there an established process to review the vulnerabilities from past security incidents for the medical devices and infrastructure components that store patient-sensitive data?	**10**	**10**	**100**
	Q3: Is there a process to receive newly published vulnerabilities for all the IoMT devices and IT systems in your hospital?	**20**	**10**	**200**
	Q4: Does the hospital register risks based on high and critical vulnerabilities that are detected?	**10**	**0**	**0**
	Q5: Is there a process to prioritize vulnerabilities based on your hospital's unique IT landscape?	**20**	**10**	**200**
	Q6: Do past security incidents include incidents outside the organization as well or just within the organization?	**10**	**10**	**100**
	Q7: Does the hospital have a process to address the risks registered and detected?	**20**	**10**	**200**
Vulnerability Process and Technology	Q8: Are the patient data and physician's desktops/laptops frequently scanned for known vulnerabilities?	**20**	**10**	**200**
	Q9: Are all the infrastructure components supporting critical patient care systems kept up to date in terms of systems and OS patches?	**15**	**0**	**0**
	Q10: Is there a network vulnerability scanning tool implemented to scan IT systems in your hospital?	**10**	**0**	**0**
	Q11: Are the vendor-specific security updates checked and installed for the medical devices at the right time to avoid exploitation of vulnerabilities?	**10**	**10**	**100**
	Q12: Is vulnerability scanning done on clinical information systems that contain patient care data and clinical data?	**20**	**10**	**200**

TABLE 5. *(Continued.)* **Vulnerability self-assessment questionnaire (VSAQ).**

	Q13: Is the clinical support system (labs, pharmacy, blood bank, Operation theatres) often monitored for any known vulnerabilities in the CVE database?	**15**	**10**	**150**
	Q14: Is the patient monitoring system (registration, appointments, charging, and billing) kept up to date without any security vulnerabilities (by patching)?	**15**	**0**	**0**
	Q15: Are the common vulnerabilities associated with medical imaging identified and addressed?	**10**	**0**	**0**
	Q16: Is there any open-source application security vulnerability scanning tool (example: SAST) implemented to identify healthcare-related application vulnerabilities in your organization?	**15**	**0**	**0**
	Q17: Is there a particular focus on remediation of critical vulnerabilities (APT, Malware, Ransomware) commonly exploited in healthcare organizations?	**20**	**10**	**100**
	Q18: Was there any successful vulnerability exploit within the IT/medical device/telemedicine domain?	**15**	**0**	**0**
	Q19: Is there a well-defined process (Vulnerability Management Process and Documentation) within the organization that helps in dealing with security incidents?	**15**	**10**	**150**

B. VULNERABILITY SELF-ASSESSMENT QUESTIONNAIRE (VSAQ)

While many reputed organizations can help assess the cybersecurity maturity of Asian healthcare IT organizations, organizational and budgetary constraints will slow down and delay assessments. Ideally, researchers in the cybersecurity domain must collaborate with healthcare IT organizations to improve maturity. Table 5 depicts the vulnerability self-assessment questionnaire that may be utilized by any Asian healthcare IT organization for the purpose of self-assessing their vulnerability management practice. The columns in this table are explained here; ''Type'' can be one of the two values, vulnerability culture or vulnerability process, and technology. Culture refers to the level of awareness about vulnerability management and its practices. Process and technology refer to the maturity of operations and technology in the vulnerability space within the organization. A value of 0 or 10 is given based to ''Base Score'' depending on whether the answer to the question is a No or a Yes respectively. ''Asia attack-based weightage'' is defined based on the relevance of the question to one of the five types of cyberattacks that are at the core of this research study. The weights given to the questions belong to three categories: Medium (10), High (15), Critical (20). The base score column in the above table has assumed a Yes or a No, for all the questions. For example, the answer is assumed to be a ''No'' for Q1 and Q4 under vulnerability management culture, and hence get the value of 0 for the base-score (B). The questions are closed-ended questions with a Boolean approach (yes or no answers). This is a quantitative approach to building questionnaires [101].

1) MATURITY SCORE COMPUTATION FOR VULNERABILITY MANAGEMENT CULTURE (VMC)

Based on the weightage and base scores, the Vulnerability management Culture (VMC) total score is calculated. An example is provided below.

Vulnerability management Culture (VMC) Total score = Sum of (Asian attack-based weightage (W) ∗ Base-score (B)).

TABLE 6. Risk self-assessment questionnaire (RSAQ).

Type	Questions	Likelihood Weightage based on attack information and vulnerability analysis (W)	Base Impact score (B) (Yes=10, No=0)	Risk score = W*B
Risk Management Culture	Q1: Is the information security program in the hospital closely tied with the IT and business risk management programs?	**10**	**0**	**0**
	Q2: Is the Risk assessed quarterly for all the medical business systems and processes? (example: Payment card industry-PCI risk)	**10**	**10**	**100**
	Q3: Is the risk assessment performed whenever a new medical device technology is introduced to cover the expanded attack surface?	**10**	**10**	**100**
	Q4: Is there an internal or external risk audit done annually?	**10**	**0**	**0**
	Q5: Is there a policy to detect, prevent and mitigate financial and medical identity theft (Preventative Control)?	**15**	**0**	**0**
	Q6: Is the information security program in the hospital closely tied with the corporate risk management programs?	**10**	**0**	**0**
	Q7: Are there regular security awareness campaigns conducted to reduce the cybersecurity risks in your organization?	**20**	**10**	**200**
	Q8: Does your organization allocate a budget for cyber risk-related policies and activities?	**20**	**0**	**100**
Risk Process and	Q9: Is the Risk assessed quarterly for all the medical business systems and processes? E.g., Payment card industry-PCI Risk	**10**	**10**	**100**
	Q10: Is HIPAA or HITRUST framework or their equivalent used in the cyber risk management process in your hospital?	**20**	**10**	**200**
	Q11: Is there an established encryption standard followed in your hospital to encrypt sensitive personal data of patients?	**15**	**10**	**150**
	Q12: Is there a continuous risk assessment performed in your hospital to address risks arising from the new medical devices and technologies?	**15**	**0**	**0**

TABLE 6. *(Continued.)* **Risk self-assessment questionnaire (RSAQ).**

Technology	Q13: Is privacy assessment performed for patient information systems that store and manipulate patient data?	**15**	**10**	**150**
	Q14: Are the anti-malware and intrusion prevention tools upgraded regularly (to include the recent healthcare attack signatures) to address malware-related risks?	**20**	**10**	**200**
	Q15: Is a regular crown jewel analysis (CJA) performed on patient data in your hospital to address healthcare data risks?	**20**	**10**	**200**
	Q16: Is there regular security auditing performed to determine the effectiveness of security controls in protecting the medical records (EHR) in your hospital?	**15**	**0**	**0**
	Q17: Does the hospital use the Secured Socket layer (SSL) technology to avoid the Risk of integrity and authenticity to patient data?	**15**	**10**	**150**
	Q18: Do the medical devices in your hospital use DoS blockers to ensure a DoS attack-free environment?	**15**	**0**	**0**
	Q19: Is there a risk registry tool (where risk score, impact, and risk-likelihood are stored) already in use in your hospital?	**10**	**0**	**0**
	Q20: Is your organization assessing risks of being not compliant with national information technology-related laws (E.g., IT ACT 2000 – India, Republic Act 10844 of Philippines)	**10**	**0**	**0**
	Q21: Is the risk assessment done for the hospital information system integrated with external systems, e.g., insurance systems?	**10**	**10**	**100**
	Q22: Do you assess risks related to mobile devices for payment transactions?	**15**	**0**	**0**
	Q23: Do you assess risks associated with SSO and active directory credential validation in your organization?	**20**	**10**	**200**
	Q24: Is your hospital certified with any one of the following? a) ISO 27001 b) NABH (National Accreditation Board for Hospitals and Healthcare providers) c) JCI (Joint Commission International)	**20**	**10**	**200**

Based on the Total score column values, for Q1 through Q7, in Table 5, VMC's total maturity score is 800. The maximum possible score is 1050 (assuming an answer of Yes for all the questions in the VMC section.

The three maturity levels for vulnerability management culture (VMC) and the scores are defined below.

0 - 450 = Low maturity level; 500- 950 = Medium maturity level; 1000-1400 = High maturity level

Based on the example values in Table 5, the VMC maturity is medium (score of 800).

2) MATURITY SCORE COMPUTATION FOR VULNERABILITY PROCESS AND TECHNOLOGY (VPT)

Based on the weightage and base scores, the Vulnerability process and Technology total score is calculated. An example is provided below.

Vulnerability process and Technology (VPT) Total score = Sum of (Asian attack-based weightage (W) ∗ Base score (B)).

Based on the Total score column values in Table 5, for Q8 through Q19, VPT's Total maturity score is 900. The maximum possible score is 1600 (assuming an answer of Yes for all the questions in the VPT section. The three maturity levels for vulnerability process and technology (VPT), along with the scores, are defined below.

0-800 = Low maturity level; 850- 1600 = Medium maturity level; 1650-2400 = High maturity level.

Based on the example values in Table 5, the VPT maturity is medium.

C. RISK SELF-ASSESSMENT QUESTIONNAIRE (RSAQ)

Table 6 shows the Risk self-assessment questionnaire that the Asian healthcare systems could use to conduct a self-assessment about their risk management practice. The columns in this table are explained here; type can be one of the two values, risk culture or risk process, and technology. Culture refers to the level of awareness about risk management and its practice. Process and technology refer to the maturity of processes and technology within the risk space in the organization. A Base score of 0 or 10 is given based on whether the answer to the question is a "No" or a "Yes". Likelihood weightage is defined based on the close relationship of the question to the earlier analysis done on cyberattacks and their vulnerabilities. The weights given to the questions belong to three categories: Medium (10), High (15), Critical (20). The base score column in the above table has assumed either a Yes or a No, for all the questions. For example, for Q1 and Q4, the answer is assumed to be a No and hence get the value of 0 for the base-score (B).

1) MATURITY SCORE COMPUTATION FOR RISK MANAGEMENT CULTURE (RMC)

Based on the weightage and base scores, Risk Management Culture (RMC) total score is calculated. An example is provided below.

Risk management Culture Total score = Sum of (Asian attack-based weightage (W) ∗ Base-score (B)).

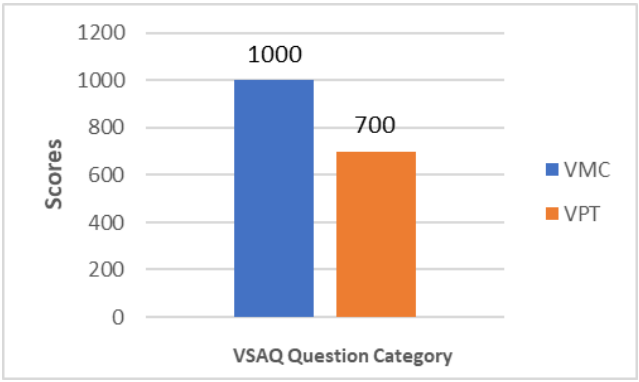

FIGURE 3. VSAQ scores.

Based on the Total score column values, for Q1 through Q8, in Table 6, RMC's total score is 500. The maximum possible score is 950 (assuming an answer of Yes for all the questions in the RMC section. The three maturity levels for Risk Management Culture (RMC) and the scores are defined below.

0 - 350 = Low maturity level; 400- 600 = Medium maturity level; 650-950 = High maturity level.

Based on the example values in Table 6, the RMC maturity is medium.

2) MATURITY SCORE COMPUTATION FOR RISK PROCESS AND TECHNOLOGY (RPT)

Based on the weightage and base scores, the total score of Risk Process and Technology (RPT) is calculated. An example is provided below.

Risk Process and Technology Total score = Sum of (Asian attack-based weightage (W) ∗ Base score (B)).

Based on the values in the Total score column in Table 6, RPT's Total score is 1650. The maximum possible score is 2450 (assuming an answer of Yes for all the questions in the RPT section. The three maturity levels for Risk Process and Technology (RPT) and the scores are defined below.

0-950 = Low maturity level; 1000-1700 = Medium maturity level; 1750-2450 = High maturity level.

Based on the example values in Table 6, the RPT maturity is medium.

The bar charts below (Figures 3 and 4) show the score results for both VSAQ and RSAQ, respectively.

From the above bar chart examples, one could infer that, in the area of vulnerability self-assessments, VMC score is more than that of VPT (Figure 3). This likely means that the awareness about the vulnerability culture is high in the organization, but implementation of process and technology needs improvement. To bring about this improvement, a strong focus in the area of security tool investment and connected processes will be a good initial step. Similarly, in the area of risk self-assessment example (Figure 4), RPT score is more than RMC. This reveals that management support and

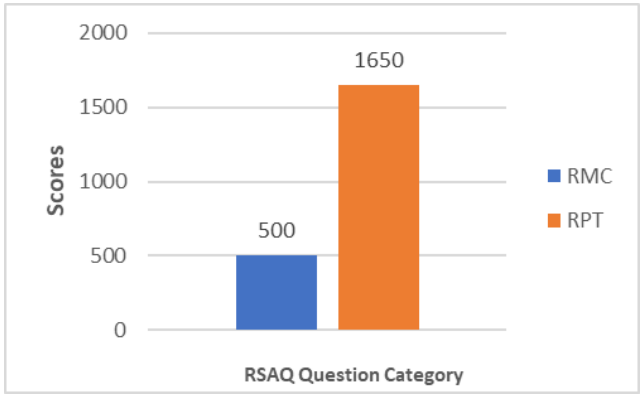

FIGURE 4. RSAQ scores.

technology budget for risk processes and tools is most likely in a mature state, but the risk culture is lacking.

D. OTHER VULNERABILITY MANAGEMENT METHODS

This research team strongly recommends using cyber risk management frameworks like ISO, NIST, and HIPAA depending upon the nature and maturity of the organization [71]. [47] has proposed the Vulnerability-Driven National Cyber Security Maturity Model for measuring the readiness levels of national critical infrastructure protection efforts. Healthcare organizations in Asia can adopt a similar approach. Healthcare organizations with lower maturity can adapt the ISO model, and medium maturity organizations can adapt the NIST framework. ISO 27799:2016 gives guidelines for healthcare organizational information security standards and information security management practices, including selecting, implementing, and managing controls. This approach takes into consideration the healthcare organization's information security risk landscape. [102] created a software platform called Cyber Risk Vulnerability Management (CYRVM) that can be used for cyber risk management using the standard NIST 800-30. This platform uses the combination of vulnerability assessment based on open-source vulnerability scanning method and risk analysis based on custom programming.

VIII. CONCLUSION AND FUTURE WORK

Five major types of recent cyberattacks in Asian healthcare institutions were identified and presented in this research work. Depiction of a vulnerability heat map and a pie chart captured the vulnerability landscape in Asian healthcare organizations. This work also presented a detailed analysis of these healthcare cyberattacks, their anatomy, associated vulnerabilities, threats, and risks. The National Institute of standards and technology (NIST) risk framework is leveraged in this research work to analyze the five cyberattacks on Asian healthcare institutions. NIST mitigation recommendations to these attacks are elucidated. A unique and enriched vulnerability priority score system (EVPS) was recommended to prioritize the vulnerabilities. This work also presented a few special recommendations, including the vulnerability and risk self-assessment questionnaires (scientifically validated with the help of healthcare IT experts) that Asian healthcare organizations can adopt to improve cybersecurity maturity leading to a better cyber posture against the five types of cyber-attacks.

The analytical outcomes of VSAQ and RSAQ scores point to the usefulness of the survey questionnaires and the computational approach. Healthcare institutions in Asia can use the recommended assessment approach to perform self-assessments and set maturity goals.

In the future, possible extensions to this work will involve studying the cybersecurity healthcare risk practices in specific Asian countries using quantitative processes. Identifying success factors that impact the cybersecurity maturity in Asian healthcare organizations and understanding correlations amongst them will help to improve the cybersecurity posture in these organizations. Studying cybersecurity best practices in Asian healthcare IT organizations in different Asian countries will increase awareness and maturity.

ACKNOWLEDGMENT

The authors would like to express their immense gratitude and respect to their beloved Chancellor Sri. Mata Amritanandamayi Devi (AMMA) for providing them with motivation and inspiration for this manuscript.

REFERENCES

[1] K. M. Cresswell and A. Sheikh, "Health information technology in hospitals: Current issues and future trends," *Future Hospital J.*, vol. 2, no. 1, pp. 50–56, Feb. 2015.

[2] R. K. Pathinarupothi, P. Durga, and E. S. Rangan, "IoT-based smart edge for global health: Remote monitoring with severity detection and alerts transmission," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2449–2462, Apr. 2019, doi: 10.1109/JIOT.2018.2870068.

[3] P. Kubban, M. Dumontier, and A. Dekker, *Fundamentals of Clinical Data Science*. Springer, 2019.

[4] (2018). *Data Breach Investigations Report*. Accessed: Jan. 14, 2020. [Online]. Available: https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf

[5] (2019). *Healthcare Data Breach Report*. [Online]. Available: https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/

[6] *Data Breaches Report*. Accessed: Feb. 15, 2020. [Online]. Available: https://privacyrights.org/data-breaches

[7] A. H. Seh, M. Zarour, M. Alenezi, A. K. Sarkar, A. Agrawal, R. Kumar, and R. A. Khan, "Healthcare data breaches: Insights and implications," *Healthcare*, vol. 8, no. 2, p. 133, May 2020, doi: 10.3390/healthcare8020133.

[8] A. Sardi, A. Rizzi, E. Sorano, and A. Guerrieri, "Cyber risk in health facilities: A systematic literature review," *Sustainability*, vol. 12, no. 17, p. 7002, Aug. 2020.

[9] P. Ambrose and C. Basu, "Interpreting the impact of perceived privacy and security concerns in patients' use of online health information systems," *J.Inf. Privacy Secur.*, vol. 8, no. 1, pp. 38–50, Feb. 2015.

[10] R. K. Pathinarupothi, "Clinically aware data summarization at the edge for Internet of Medical Things," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2019, pp. 437–438.

[11] D. Birnbaum, E. Borycki, B. T. Karras, E. Denham, and P. Lacroix, "Addressing public health informatics patient privacy concerns," *Clin. Governance Int. J.*, vol. 20, no. 2, pp. 91–100, 2015.

[12] Q. W. Cao, "Description of SA weak password's harm and solution in the SQL server system," *J. Xingtai Polytech. College*, vol. 29, no. 1, Feb. 2012.

[13] A. S. Salsabila, D. M. Fikri, S. M. Andika, and A. N. Harahap, "Potential and threat analysis towards cybersecurity in South East Asia," *J. ASEAN Dyn. Beyond*, vol. 1, pp. 1–13, 2020.
[14] (2018). *HIMSS Cybersecurity Survey*. [Online]. Available: https://www.himss.org/sites/hde/files/d7/u132196/2018_IMSS_Cybersecurity_Survey_Final_Report.pdf
[15] *NIST Cyber Framework*. Accessed: Jan. 25, 2022. [Online]. Available: https://www.nist.gov/cyberframework
[16] W. Burke, T. Oseni, A. Jolfaei, and I. Gondal, "Cybersecurity indexes for eHealth," in *Proc. Australas. Comput. Sci. Week Multiconf.*, Jan. 2019, pp. 1–8.
[17] (2018). *Healthcare Data Breach Report*. [Online]. Available: https://techcrunch.com/2018/07/20/singapore-hack-health/?guccounter=1
[18] A. Raghavan, M. A. Demircioglu, and A. Taeihagh, "Public health innovation through cloud adoption: A comparative analysis of drivers and barriers in Japan, South Korea, and Singapore," *Int. J. Environ. Res. Public Health*, vol. 18, no. 1, p. 334, Jan. 2021, doi: 10.3390/ijerph18010334.
[19] T. A. Mattei, "Privacy, confidentiality, and security of health care information: Lessons from the recent wannacry cyberattack," *World Neurosurgery*, vol. 104, pp. 972–974, Aug. 2017.
[20] (2016). *Global State of Information Security Survey*. [Online]. Available: https://www.pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf
[21] A. Boin, *Wannacry as a Creeping Crisis—From the Book: Understanding the Creeping Crisis*. London, U.K.: Palgrave Macmillan, May 2021.
[22] Y. He, A. Aliyu, M. Evans, and C. Luo, "Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review," *J. Med. Internet Res.*, vol. 23, no. 4, Apr. 2021, Art. no. e21747.
[23] (2020). *Asia Pacific Healthcare Cybersecurity Market*. [Online]. Available: https://www.marketdataforecast.com/market-reports/asia-pacific-healthcare-cybersecurity-market
[24] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, pp. 48–52, Jul. 2018.
[25] (2019). *Government Insider Asia Report*. [Online]. Available: https://govinsider.asia/innovation/ransomware-attack-asia-wannacry/
[26] (2018). *Asia Pacific Data Security Report*. [Online]. Available: https://www.hldataprotection.com/files/2018/06/Hogan_Lovells_Asia_Data_Protection_and_Cyber_Security_Guide_2018.pdf
[27] (2017). *Digital Information Security in Healthcare Act (DISHA) of India*. [Online]. Available: https://www.nhp.gov.in/NHPfiles/R_4179_1521627488625_0.pdf
[28] *Straitstimes News Article*. Accessed: Jan. 25, 2022. [Online]. Available: https://www.straitstimes.com/asia/east-asia/hong-kongs-health-department-computers-hit-by-ransomware-planted-by-hackers
[29] *GovInsider News Article*. Accessed: Jan. 25, 2022. [Online]. Available: https://govinsider.asia/innovation/ransomware-attack-asia-wannacry/
[30] *Cyber Threats 2020: A Year in Retrospect*. Accessed: Jan. 25, 2022. [Online]. Available: https://www.pwc.co.U.K./cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
[31] *Zdnet News Article*. Accessed: Jan. 25, 2022. [Online]. Available: https://www.zdnet.com/article/cyberattacks-can-cost-apac-healthcare-firms-23-3m/
[32] 2020 Gulf News. *Hackers Attack Indian Healthcare*. Accessed: Jan. 25, 2022. [Online]. Available: https://gulfnews.com/world/asia/india/hackers-attack-indian-healthcare-website-steal-68-lakh-records-1.1566457355100
[33] R. D. Stachel and M. DeLaHaye, "Security breaches in healthcare data: An application of the actor-network theory," *Issues Inf. Syst.*, vol. 16, no. 2, pp. 1–10, 2015, doi: 10.48009/2_iis_2015_185-194.
[34] J. Davis, "Phishing attack on UC Davis health breaches data on 15,000 patients," Healthcare IT News Provider, Healthcare IT News, USA, Tech. Rep., 2017.
[35] *2020 News Asia Report*. Accessed: Jan. 25, 2022. [Online]. Available: https://www.channelnewsasia.com/news/singapore/cybercrime-jumps-more-than-50-2019-new-threats-covid-19-csa-12872818
[36] *2017 Healthcare IT News*. Accessed: Jan. 25, 2022. [Online]. Available: https://www.healthcareitnews.com/news/nsa-uncovers-ties-between-north-korea-and-wannacry-attacks
[37] M. Muthuppalaniappan and K. Stevenson, "Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health," *Int. J. Quality Health Care*, vol. 33, no. 1, p. mzaa117, Sep. 2020.
[38] S. M. Tabish, M. Z. Shafiq, and M. Farooq, "Malware detection using statistical analysis of byte-level file content," in *Proc. ACM SIGKDD Workshop CyberSecurity Intell. Inform.*, 2009, pp. 23–31.
[39] (2017). *2017 Healthcare IT News*. [Online]. Available: http://www.healthcareitnews.com/news/alaska-dhss-facing-potential-breachafter-two-trojan-malware-attacks
[40] S. A. E. Hoffman, "Cybersecurity threats in healthcare organizations: Exposing vulnerabilities in the healthcare information infrastructure," *Inf. Secur., Emerg. Voices*, vol. 24, no. 1, Jul. 2020.
[41] *Orangeworm: Need-to-Know Information for Healthcare IT*. [Online]. Available: https://www.atlantic.net/life-sciences-pharma-biotech/orangeworm-need-to-know-information-for-healthcare-it/
[42] *Computer Weekly Report*. [Online]. Available: https://www.computerweekly.com/news/252439782/Orangeworm-cyber-attack-group-targeting-health-sector
[43] M. S. Jalali, M. Bruckes, D. Westmattelmann, and G. Schewe, "Why employees (still) click on phishing links: Investigation in hospitals," *J. Med. Internet Res.*, vol. 22, no. 1, p. e16775, 2020.
[44] E. Kirda and C. Kruegel, "Protecting users against phishing attacks with AntiPhish," *Comput. J.*, vol. 49, no. 5, pp. 554–561, 2006.
[45] W. Priestman, T. Anstis, I. G. Sebire, S. Sridharan, and N. J. Sebire, "Phishing in healthcare organisations: Threats, mitigation and approaches," *BMJ Health Care Informat.*, vol. 26, no. 1, Sep. 2019, Art. no. e100031.
[46] *2020 ICLG News on Cyberattacks*. Accessed: Jan. 25, 2022. [Online]. Available: https://iclg.com/briefing/13713-singapore-rise-in-cyber-attacks-particularly-in-health-sector
[47] B. Karabacak, S. O. Yildirim, and N. Baykal, "A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness," *Int. J. Crit. Infrastruct. Protection*, vol. 15, pp. 47–59, Dec. 2016.
[48] S. Maniath, P. Poornachandran, and V. G. Sujadevi, "Survey on prevention, mitigation and containment of ransomware attacks," in *Security in Computing and Communications*, vol. 969. Singapore: Springer, 2019, pp. 39–52.
[49] A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, "A survey on security and privacy issues in modern healthcare systems: Attacks and defenses," *ACM Trans. Comput. Healthcare*, vol. 2, no. 3, pp. 1–44, Jul. 2020.
[50] *2021 TrendMicro Report*. [Online]. Available: https://success.trendmicro.com/solution/1117391-preventing-wannacry-wcry-ransomware-attacks-using-trend-micro-products
[51] M. Anandarajan and S. Malik, "Protecting the Internet Of Medical Things: A situational crime-prevention approach," *Cogent Med.*, vol. 5, no. 1, Jan. 2018, Art. no. 1513349.
[52] *2019 Parima Report*. [Online]. Available: https://www.parima.org/asian-attacks-lead-to-rise-in-cyber-policies/
[53] L. F. Maimó, A. H. Celdrán, Á. P. Gómez, F. G. Clemente, J. Weimer, and I. Lee, "Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments," *Sensors*, vol. 19, no. 5, p. 1114, Mar. 2019, doi: 10.3390/s19051114.
[54] *2017 Center for Internet Security Advisory*. Accessed: Jan. 25, 2022. [Online]. Available: https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-microsoft-windows-smb-server-could-allow-for-remote-code-execution/
[55] S. Quintero-Bonilla and A. M. del Rey, "A new proposal on the advanced persistent threat: A survey," *Appl. Sci.*, vol. 10, no. 11, p. 3874, Jun. 2020, doi: 10.3390/app10113874.
[56] *2020 Computer Weekly News Report*. Accessed: Jan. 25, 2022. [Online]. Available: https://www.cyfirma.com/news/southeast-asia-remains-hotspot-for-cyber-attacks/.
[57] *Fireeye Report on APT*. Accessed: Jan. 25, 2022. [Online]. Available: https://www.fireeye.com/current-threats/apt-groups.html
[58] S. Papastergiou, H. Mouratidis, and E.-M. Kalogeraki, "Handling of advanced persistent threats and complex incidents in healthcare, transportation and energy ICT infrastructures," *Evolving Syst.*, vol. 12, no. 1, pp. 91–108, Mar. 2021.
[59] J. Onaolapo, E. Mariconti, and G. Stringhini, "What happens after you are pwnd: Understanding the use of leaked webmail credentials in the wild," in *Proc. Internet Meas. Conf.*, Nov. 2016, pp. 65–79.
[60] K. Thomas, F. Li, A. Zand, J. Barrett, J. Ranieri, L. Invernizzi, Y. Markov, O. Comanescu, V. Eranti, A. Moscicki, D. Margolis, V. Paxson, and E. Bursztein, "Data breaches, phishing, or malware?: Understanding the risks of stolen credentials," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2017, pp. 1421–1434.
[61] J. A. Wang and M. Guo, "OVM: An ontology for vulnerability management," in *Proc. 5th Annu. Workshop Cyber Secur. Inf. Intell. Res. Cyber Secur. Inf. Intell. Challenges Strategies (CSIIRW)*, 2009, pp. 1–4.

[62] J. DeRosier, E. Stalhandske, J. P. Bagian, and T. Nudell, "Using health care failure mode and effect analysis: The VA national center for patient safety's prospective risk analysis system," *Joint Commission J. Quality Improvement*, vol. 27, no. 5, pp. 248–267, 2002.
[63] W. Heinbockel, S. Noel, and J. Curbo, "Mission dependency modeling for cyber situational awareness," in *Proc. NATO IST Symp. Cyber Defence Situation Awareness*, 2016, pp. 1–14.
[64] M. Nyanchama, "Enterprise vulnerability management and its role in information security management," *Inf. Syst. Secur.*, vol. 14, no. 3, pp. 29–56, Jul. 2005.
[65] *National Vulnerability Database*. Accessed: Jan. 25, 2022. [Online]. Available: https://nvd.nist.gov/vuln
[66] S. acharya, M. Terry, and O. D. Oigiagbe, "A comprehensive security assessment toolkit for healthcare systems," *Colonial Academic Alliance Undergraduate Res. J.*, vol. 4, no. 1, p. 6, 2015.
[67] *2021 Netwrix Cloud Data Security Report*. Accessed: Jan. 25, 2022. [Online]. Available: https://www.netwrix.com/download/collaterals/2021%20Netwrix%20Cloud%20Data%20Security%20Report.pdf
[68] *Netwrix Cloud Security Report*. Accessed: Jan. 25, 2022. [Online]. Available: https://www.netwrix.com/download/collaterals/2021%20Netwrix%20Cloud%2 0Data%20Security%20Report.pdf
[69] A. M.-H. Kuo, "Opportunities and challenges of cloud computing to improve health care services," *J. Med. Internet Res.*, vol. 13, no. 3, p. e67, Sep. 2011.
[70] R. Sivan and Z. A. Zukarnain, "Security and privacy in cloud-based E-health system," *Symmetry*, vol. 13, no. 5, p. 742, Apr. 2021, doi: 10.3390/sym13050742.
[71] K. Kandasamy, S. Srinivas, K. Achuthan, and V. P. Rangan, "IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process," *EURASIP J. Inf. Secur.*, vol. 2020, no. 1, pp. 1–18, Dec. 2020.
[72] *Adopting the NIST Cybersecurity Framework in Healthcare*. Symantec Whitepaper. Accessed: Jan. 25, 2022. [Online]. Available: https://docs.broadcom.com/doc/adoping-the-nist-cybersecurity-framework-in-healthcare-en
[73] S. Almuhammadi and M. Alsaleh, "Information security maturity model for NIST cyber security framework," *Comput. Sci. Inf. Technol. CS IT*, vol. 7, pp. 51–62, Feb. 2017.
[74] S. Shackleford, A. Andrew Proia, B. Martell, and A. Craig, "Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices," *Texas Int. Law J.*, 2015.
[75] M. Scholl, K. Stine, and J. Hash, "An introductory resource guide for implementing the HIPAA security rules," NIST Special Publication 800-66 Revision, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST 800-66R, 2008.
[76] M. Barrett, J. Marron, V. Y. Pillitteri, J. Boyens, G. Witte, and L. Feldman, "The cybersecurity framework: Implementation guidance for federal agencies," Draft NIST IR, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST IR 8170, 2017.
[77] *2017 HIMSS (Healthcare Information and Management Systems Society) Cybersecurity Survey Report*. Accessed: Jan. 25, 2022. [Online]. Available: https://content.govdelivery.com/attachments/USDHSCIKR/2017/08/23/file_attachments/868026/2017-HIMSS-Cybersecurity-Survey-Final-Report.pdf
[78] S. Lowry, "Technical evaluation, testing, and validation of the usability of electronic health records," NIST IT, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST IT 7804, 2015.
[79] J. Fonseca, M. Vieira, and H. Madeira, "Testing and comparing web vulnerability scanning tools for SQL injection and XSS attacks," in *Proc. 13th Pacific Rim Int. Symp. Dependable Comput. (PRDC)*, Dec. 2007, pp. 365–372, doi: 10.1109/PRDC.2007.55.
[80] H. Hasanova, U.-J. Baek, M.-G. Shin, K. Cho, and M.-S. Kim, "A survey on blockchain cybersecurity vulnerabilities and possible countermeasures," *Int. J. Netw. Manage.*, vol. 29, no. 2, p. e2060, Mar. 2019.
[81] G. Mcgraw, "Software penetration testing," *IEEE Secur. Privacy*, vol. 3, no. 1, pp. 1540–7993, Feb. 2005.
[82] T. Tang, M.-C. Zhou, Y. Quan, J.-L. Guo, V. S. Balaji, V. Gomathi, and V. Elamaran, "Penetration testing and security assessment of healthcare records on hospital websites," *J. Med. Imag. Health Informat.*, vol. 10, no. 9, pp. 2242–2246, Aug. 2020.
[83] *NIST SP800-39, Managing Information Security Risk*. Accessed: Jan. 25, 2022. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf
[84] *NIST SP800-30, NIST Risk Management Guide for Information Systems*. Accessed: Jan. 25, 2022. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
[85] *OWASP Top 10 Vulnerabilities*. Accessed: Jan. 25, 2022. [Online]. Available: https://owasp.org/www-project-top-ten/
[86] C. Frenz, "OWASP secure medical device deployment standard," Open Web Appl. Secur. Project, USA, Tech. Rep., 2017.
[87] H. Abdo, M. Kaouk, J.-M. Flaus, and F. Masse, "A safety/security risk analysis approach of industrial control systems: A cyber bowtie–combining new version of attack tree with bowtie analysis," *Comput. Secur.*, vol. 72, pp. 175–195, Jan. 2018.
[88] J. Martin and M. Talabis, "Information security risk assessment: Data analysis," in *Information Security Risk Assessment Toolkit*. Boston, MA, USA: Syngress, 2012, pp. 105–146.
[89] M. McShane, M. Eling, and T. Nguyen, "Cyber risk management: History and future research directions," *Risk Manage. Insurance Rev.*, vol. 24, no. 1, pp. 93–125, 2021.
[90] P. T. Dover, "Evaluating medical IoT (MIoT) device security using NISTIR-8228 expectations," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST IR-8228, 2021.
[91] *Guide to Data-Centric System Threat Modeling*, Standard NIST SP 800-154, National Institute of Standards and Technology, Mar. 2016.
[92] *Information Technology_Security Techniques_Information Security Management Systems_Requirements*, Standard ISO 27001:2013, DIN Deutsches Institut Für Normung e.V., Burggrafenstrasse, Berlin, Germany, Mar. 2013.
[93] O. Tang and S. N. Musa, "Identifying risk issues and research advancements in supply chain risk management," *Int. J. Prod. Econ.*, vol. 133, no. 1, pp. 25–34, 2011.
[94] W. J. Gordon, A. Wright, R. J. Glynn, J. Kadakia, C. Mazzone, E. Leinbach, and A. Landman, "Evaluation of a mandatory phishing training program for high-risk employees at a U.S. healthcare system," *J. Amer. Med. Inform. Assoc.*, vol. 26, no. 6, pp. 547–552, Jun. 2019.
[95] Y.-H. Kim and W. H. Park, "A study on cyber threat prediction based on intrusion detection event for APT attack detection," *Multimedia Tools Appl.*, vol. 71, no. 2, pp. 685–698, Jul. 2014.
[96] NIST SP 800-61R2. *Computer Security Incident Handling Guide*. Accessed: Jan. 25, 2022. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
[97] R. Lund, L. S. Nielsen, P. W. Henriksen, L. Schmidt, K. Avlund, and U. Christensen, "Content validity and reliability of the Copenhagen social relations questionnaire," *J. Aging health*, vol. 26, no. 1, pp. 50–128, Feb. 2014, doi: 10.1177/0898264313510033.
[98] J. Oluwatayo, "Validity and reliability issues in educational research," *J. Educ. Social Res.*, vol. 2, pp. 391–400, May 2012.
[99] D. Straub, M.-C. Boudreau, and D. Gefen, "Validation guidelines for IS positivist research," *Commun. Assoc. Inf. Syst.*, vol. 13, no. 24, pp. 380–427, 2004.
[100] H. Taherdoost, "Validity and reliability of the research instrument: How to test the validation of a questionnaire/survey in a research," *Int. J. Academic Res. Manage. (IJARM)*, vol. 5, no. 3, pp. 28–36, 2016.
[101] M. Chacko, C. Retnakumar, D. Ramakrishnan, L. S. George, and V. Krishnapillai, "Menstrual restrictions among young females in urban slums of cochin," *Int. J. Community Med. Public Health*, vol. 7, no. 1, p. 264, Dec. 2019.
[102] P. Russo, A. Caponi, M. Leuti, and G. Bianchi, "A web platform for integrated vulnerability assessment and cyber risk management," *Information*, vol. 10, no. 7, p. 242, Jul. 2019.

KAMALANATHAN KANDASAMY is currently pursuing the Ph.D. degree with the Amrita Center for Cyber Security Systems and Networks, Amrita Vishwa Vidyapeetham. He is also a Research Associate at the Amrita Center for Cyber Security Systems and Networks, Amrita Vishwa Vidyapeetham. He has seven years of experience in the information technology industry and 16 years of work experience in academia with various cybersecurity projects, including the areas of cloud security, database security, and cyber governance at Amrita University. His research interests include cyber risk assessment and management, medical device security, and cyber threat intelligence.

SETHURAMAN SRINIVAS received the bachelor's degree in applied sciences, the master's degree in computer application, and the Ph.D. degree in information technology, with specialization in information assurance. He has more than 25 years of experience in the information technology industry with a current focus on the cybersecurity domain. He is a seasoned information technology executive with a special focus on information security governance, metrics, and program management. He is currently an Adjunct Faculty with the School of Engineering, Amrita University, for the past seven years, with a focus on the cybersecurity domain. He is also an Advisor to many firms with the San Francisco Bay area in the area of information security. He was recently part of IBM's managed security services for a period of seven years where he specialized as a strategy consultant in the area of security intelligence and operations. He managed medium to large cybersecurity programs in the area of cybersecurity governance, security analytics, big data, intrusion detection and prevention systems, risks, and security metrics. He started his IT career with Wipro's Research and Development. He was a Software Developer for ten years, and other roles held by him were a Configuration Manager, a Software Development Manager, an Oracle Retail Specialist, and an Advisory IT Architect with Computer Sciences Corporation (CSC). He regularly handles classes in the area of application security, database security, and cybersecurity governance. He has published cybersecurity academic articles in peer-reviewed journals (IEEE and ACM). His research interests include security analytics, cybersecurity GRC, privacy databases, risk frameworks, big data, and governance automation.

KRISHNASHREE ACHUTHAN (Senior Member, IEEE) received the Ph.D. degree from Clarkson University, Potsdam, NY, USA. She is an ardent researcher at Amrita Center for Cyber-Security Systems and Networks, Amrita Vishwa Vidyapeetham. She also leads research teams focused on the enhancement of laboratory education through virtual laboratories. She holds 33 U.S. patents and has published over 50 publications in journals and conferences. She has played an active role in several strategic initiatives for the Government of India and served as the principal investigator. Her research interests include cybersecurity and governance, mathematical modeling of systems, cybersecurity policy, the IoT security, public safety, innovation, and educational technologies and entrepreneurship.

VENKAT P. RANGAN founded and directed the Multimedia Laboratory and the Internet and Wireless Networks (Wi-Fi) Research, University of California at San Diego, where he worked as a Professor of computer science and engineering for 16 years. He is currently the Vice Chancellor of Amrita Vishwa Vidyapeetham. He has over 85 publications in international (mainly the IEEE and the ACM) journals and conferences and also holds 22 U.S. patents. He is a fellow of the ACM, in 1998. He is the youngest to achieve this international distinction. He received the President of India Gold Medal in 1984, the NCR Research Innovation Award in 1991, and the NSF National Young Investigator Award in 1993. In 2000, Internet World featured him on its cover page and named him as one of the top 25 Stars of Internet Technologies. In 2012, Silicon India ranked him as one of the 50 Indians Who Redefined Entrepreneurship in the last 65 years of independence. He is an internationally recognized pioneer of research in multimedia systems and internet e-commerce. In 1993, he founded the first International Conference on Multimedia: ACM Multimedia 93, for which he was the Program Chairperson. This is now the premier worldwide conference on multimedia. He also founded the first international journal on *Multimedia* (ACM)/Springer-Verlag *Multimedia Systems*, which is now the premier journal on multimedia.