International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 1, pp 158-167, January-2024

https://doi.org/10.47001/IRJIET/2024.801019

Ransomware Threats Targeting the Healthcare Sector

Deemantha N. Siriwardana

Undergraduate BSc (Hons) in Cyber Security, Sri Lankan Institute of Information Technology, Malabe, Sri Lanka
E-mail: deemanthanayanajith1@gmail.com

Abstract **- Security is essentially a consideration in any computer system which holds sensitive or critical data. Ransomware attacks which are primarily based on encrypting critical data and demanding for a ransom to decrypt them, is one of the best approaches in harvesting money from critical industrial firms rather than damaging the information infrastructure. Even though general ransomware practices include encrypting critical data, sometimes it can come in a form of a threat to leaking of sensitive data to the public. Among the critical infrastructures in the healthcare industry, patient's Personally Identifiable Information (PII) and also the operational data related to mission critical systems are the top concerns. Leaking of PII can cause a huge damage to the privacy of the patients who obtain the healthcare service for that particular healthcare provider. On the other hand, any system delays, malfunctions of inaccessibility or unavailability of operational data related to mission critical systems can cause hindrances to the usual operations of the healthcare provider and eventually will case a life-threatening situation to the patients as well. Through this research review, a comprehensive understanding to the topics; what is ransomware, why ransomware target health industry, what is the damage caused, new ransomware attack trends, mitigative steps and future research scopes are presented to the audience. At the end of the paper, overall conclusion made by analyzing reported incidents is presented with recommendation to mitigate the effects of future ransomware threats, targeted on healthcare industry.**

Keywords: Ransomware, Healthcare Industry, Cyber Security, Cyber Insurance.

I. INTRODUCTION

To cyber-crimes over the past decade due to several healthcare industries is one of the most vulnerable targets reasons. Among the contributing factors, the massive databases of patients' data. Health records, employee records, payment mechanisms, stakeholder network, sophisticated technological equipment, advanced computerized systems and heavy utilization of IoT and cloud services are few of the highlighted reasons.

Although most of the general cyber-crimes involves destruction to information infrastructure, most noticeable thing related to the cyber attacks targeted on healthcare industry is that, majority of the cybercrimes are focused on compromising the availability factor of the data or information in those healthcare systems.

Ransomware is the perfect utility or type of the attack appealing to a cyber criminal who is considered about compromising the availability factor of data in a system without corrupting them. Ransomware is a type of malware which can either lock (encrypt) a device, system, residing data or information within a system and demand a ransom in order to unlock (decrypt) them [1]. Even though the victims cannot be sure of getting their original data back or the decryption key after paying the ransom, it is a vital factor to keep the original data without corruption from the attacker's point of view, if the attacker is willing to infect the ransomware to multiple systems or launching the attack in mass quantities. Once decrypting the content and granting access to the original data without corruption, after the victim pays the ransom, will motivate the other victims to pay the ransom and get their original data back. This will be an advantage to the attacker if the motive of the attack is to obtain a monetary value.

The most compelling reason for making healthcare organizations to be selected as ransomware targets is that these organizations cannot afford to make guesses on whether to or not to pay the ransom and worrying about the receiving or not receiving the decryption key. Since most of the computer systems are playing a vital part for the patients' health, these infected systems should be highly robust in terms of recovery after any downtime. Therefore, most of the times, ransomware targeted on these healthcare systems may succeed in receiving their ransoms depending on the criticality of the infected systems and how sensitive the residing data inside those infected systems.

With the current industrial standards, most of the health organizations in the health industry will face serous legal issues in case if they were unable to protect themselves against these types of data breaches and cyberattacks. The Health Information Portability and Accountability Act (HIPAA) enacted by U.S. Federal government is one of the main international standards which governs the healthcare industry

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 8, Issue 1, pp 158-167, January-2024
https://doi.org/10.47001/IRJIET/2024.801019

and has given guidelines, regulations and charges regarding protection of Personally Identifiable Information (PII) of patients who obtain a healthcare service from a certain healthcare organization [2]. With these types of regulations and standards in place, healthcare organizations cannot simply ignore their computer and data security aspects at any cost because of the fact that, if any ransomware incident occurs, it is not only the ransom that they had to face as a loss, but also they may loose their money on paying for compensations for all the stakeholders, legal fines as well as to regain the reputational loss.

In this review paper, a comprehensive review on ransomware threats targeting the healthcare sector is carried out by analyzing collection of 23 published materials and internet sources in different internationally recognized research journals, conferences, books, reports, articles, websites and the findings are discussed and reviewed under 5 main topics. The reviews are based on different perspectives in relation to the victims, attackers, stakeholders, law enforcement and in relation to the general public which are categorized based on the Covered Entities (CE) based on HIPAA standards [2].

II. RESEARCH STATEMENT

This review paper mainly focuses on the effects posed on major domains related to healthcare sector in case of a ransomware attack. The four main domains include “Health Plans”, “Health Care Clearinghouses”, “Health Care Providers”, “Victims” and “Attackers”. Health insurance companies are covered under the Health Plans domains. Any government or private entity including billing services, repricing company, community health information system is considered under Health Care Clearinghouses. Healthcare Providers are defined as any government or private hospitals, health clinics, doctors or physicians, psychologists, dentists, chiropractors, nursing homes, pharmacies, home health agencies and any other similar health-related service provider. Victim is considered as any individual or organization who is affected by a cyberattack (ransomware in this specific review). Attacker is considered as any individual or an organization with the intention of creating, distributing or damaging confidentiality, integrity or availability of a computer system or resident data within that system with a malicious intention.

All the previously reported major incidents on ransomware attacks on healthcare systems are analyzed and evaluated in both qualitative and quantitative approach under each of the applicable domains mentioned above. Recent trends and fluctuations on the attacks, damages caused to the healthcare systems, impact on wireless healthcare systems, IoT health devices, cloud databases, artificial intelligence (AI), machine learning and utilization of block chain technologies like approaches used in healthcare sector in terms of security perspective are evaluated by analyzing various academic researches, reviews, conferences, journal articles, internet sources and other literature published in the field.

III. REVIEW OF THE LITERATURE

Section 1: What is a Ransomware?

Ransomware is a type of malicious software (malware) which is designed to lock a device, system, residing data or information within a system and demand a ransom in order to unlock (decrypt) them [1]. Depending on the type of the structure, design and the motive, ransomware can either lockout the entire operating system (Locker ransomware) or encrypt individual files (Crypto ransomware) [1]. These types of blackmailing cyber attacks originated about few decades ago and the first recorded ransomware incident of such type was noted as early as in 1989 [1]. The most predominant breakout of a ransomware incident took place in year 2005 in Russia [1] and since then, the incident have increased and escalated up to the biggest ransomware incident in 2017, which is popularly known as WannaCry ransomware [1].

Further to this general understanding, a more comprehensive insight to the evolution of ransomware is given in a research paper written by A.K.Maurya, N.Kumar, A.Agrawal and R.A.Khan on the topic “Ransomware: Evolution, Target and Safety Measures” [3]. The paper gives a compete overview about the evolution from the first reported ransomware to the latest ransomware which was reported at the time of writing the research paper. The ransomware are divided into several types and their characteristics are discussed while providing a case-study on few ransomware attacks. The paper both provides proactive and reactive steps and guidelines to the victims on what steps to be taken in order to prevent a ransomware attack and what steps should be taken in an event of a ransomware attack.

Section 2: Why ransomware target healthcare industry?

Healthcare industry in a country is one of the main measurement scales taken by many organizations on evaluating the social and economic development in a particular country. Whether it is government of private healthcare providers, any citizen living within a country has to obtain services of these healthcare institutions from their birth till death. For such a lifespan of each individual, massive amount of data is collected, stored and processed by these healthcare systems. These data include names, birthdays, addresses, contact numbers, family details, health records, payment information, insurance details and any related information that is specific to an individual and can be used to

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 1, pp 158-167, January-2024

https://doi.org/10.47001/IRJIET/2024.801019

identify an individual uniquely. Despite the social status, wealth or popularity of an individual, these essential information is collected, stored and processed by any health institution when a healthcare service is obtained from them. Because of this reason, most personal or private information like health records and sensitive information like credit card and insurance details are also stored in these healthcare databases. Leakage of such information would cause potential threats to the privacy of the patients and affect their social image.

For a healthcare system, it cannot solely operate only based on patients, doctors and nurses. The system should also should have other connections with stakeholders. These stakeholders can be the health equipment or service suppliers, shareholders, doners and other related individuals or organizations. All these stakeholder data is also obtained, stored and processed in these databases related to the healthcare systems. Leakage of such sensitive data related to these stakeholders might result on loss of trust toward the healthcare organization and may result in loosing their services and impact on the business processes and business continuity of the healthcare provider. Depending on the impact, the healthcare institutions may have to face legal consequences or complementation payments to the stakeholders as well.

Some of the life supporting systems like cardiology and respiratory machines, defibrillators, dialysis equipment, , pulmonary function analyzers, respirators, ventilators, EEG monitors, infant incubators, infusion pumps and controllers, and also other medical equipment and systems like anesthetic equipment, autoclaves, sterilizers, CT scanners, MRI scanners, EtO sterilizers, laboratory equipment, laparoscopy equipment, laryngoscopic equipment, orthopedic instruments, oxygen concentrators, plate developers and processors, ultrasound equipment, x-ray equipment etc. [4] all operates and rely on data and information which are fed to them at some point of their operation by the integrated computer systems. In that case, miscalculations, misinterpretations or data corruptions can pose serious consequences to the life of the patients. A research done by Al Qartah Ayed on the topic "Evolving Ransomware Attacks on Healthcare Providers" [5], had identified and presented several reasons for the healthcare sector being an enticing target for ransomware attacks. Among them, rapidly expanding attack surfaces, lack of adequate cyber defense mechanisms, exploiting the vulnerabilities I human factor and several other critical reasons like absolute necessity to restore the confidential patients' data and medical system in order to minimize the threat to human lives are predominantly discussed [5]. Furthermore, the research had presented some considerable descriptive facts on mainstream ransomware attacks which targeted the healthcare industry in the year 2016, such as the incidents related to Virtual Care Provider Incorporated and Hollywood Presbyterian Medical Center [5]. A complete overview of most common infection methods used by attackers, types and categories of ransomware, different stages of lifecycle of ransomware are also given along with the suggestion to healthcare providers to adhering multi-layered approach in their cyber defense systems and conducting social engineering awareness programs to educate the employees within the institution in order to minimize the risk of a ransomware attack in every possible attack surface.

Due to these reasons, depending on the criticality of information and what potential impact they can cause in an incident, the value of these information get higher. In this case, it is more of an advantage to the attacker to make a bargain for a ransom payment by posing a threat on these information. This fact is also highlighted in a research conducted by Malcolm Harkins and Anthony M.Freed on the topic "The Ransomware Assault on the Healthcare Sector" [6]. It clearly highlights the fact that the ransomware is an inexpensive but still a impactful attack both I terms of the security and the compensational losses. The paper alo highlights the fact that, since ransomware can be introduced to systems through many attack surfaces, most of the attacker use this as an advantage to use this malware type on attacks related to healthcare organizations due to its nature of more variety of exposed attack surfaces to the general public. Among these attack surfaces, mobile apps, remote clinics, online channeling systems, medical sensors, health inquiry and patient inquiry systems, employee management systems, medical equipment handling systems, health insurance systems, medical bill payment gateways, patients' health record storages, backups and numerous other systems and databases can be identified in general.

Unlike other business institutions which operate in businesses and services, primary goal of healthcare institutions is to protect human lives. In that case most of the times, these institutions tend to pay the ransoms without second thoughts in order to reduce the threat to their patients' lives due to information corruption or loss. This is the main reason for the attackers to target healthcare systems more frequently on ransomware attacks due to higher rate of success in obtaining their ransom at most of the times.

Section 3: What is the damage caused?

Since there were numerous ransomware incidents being targeted specifically on healthcare institutions, by far the most damaging ransomware attack was reported to be the WannaCry ransomware attack which targeted the U.K National Health Service (NHS) in 2017 [7].

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 1, pp 158-167, January-2024

https://doi.org/10.47001/IRJIET/2024.801019

According to a research done by S. Ghafur, S. Kristensen, K. Honeyford, G. Martin, A. Darzi and P. Aylin on the research topic "A retrospective impact analysis of the WannaCry cyberattack on the NHS" [8], the impacts of the attack was determined by analyzing the deaths, missed appointments ad fiscal costs attributable to the attack [8]. It was mentioned that, due to the WannaCry ransomware attack which happened on Friday 12 May 2017, more than 600 organizations were affected out of which includes 34 infected hospital trusts which provide acute care, specialized medical services, mental healthcare and ambulance services [8]. These medical institutions were reported to be locked out from their computer systems and medical devices [8]. Another 46 healthcare institutions were reported to be acutely affected due to disruptions occurred due to preventive actions and shared systems and services with infected organizations [8]. It was further reported that, the hospitals infected with the ransomware, had to face a total loss of £5.9 million due to 6% decreased number of admissions and 13,500 cancelled appointments after the ransomware incident [8]. Even though the ransomware attack demand of the WannaCry was just a $300 worth Bitcoins [7], the aftermath of such an attack should not be diminished. Still for today, there's no published decryption key for this WannaCry ransomware and therefor the health records of the patients are still inaccessible even for today. It is not just only loosing the electronic health records, but the expenses, time and the human labor which was spent back on making those electronic records had also made useless by this incident, hence making the urge to go trough the same health checks, lab experiments and other checkup again by the patients and the health staff. This will not only be a waste of time and resources, but also will cause pose a high risk on the lives on patients who need immediate medical attention and medical procedures. Their medical procedures will be delayed due to unavailability of health records and potentially cause a risk to life due to delay in obtaining new records by going trough the same procedures one again for the second time. The emergence of new ransomware as well as trojans which helps to infect these ransomware had also increased with the time according to U.S Cyber Security & Infrastructure Security Agency, which states that a new banking trojan named TrickBot was found to be operating to drop ransomware on healthcare organizations [9]. Ransomware action is a major concerned threat to normal operations of the healthcare institutions, but not only in such situations, but in situation like disaster conditions and pandemics, this can cause great threat to lives of patients. The best example is the Ryuk ransomware which targeted healthcare systems in the COVID-19 global pandemic period. Ryuk ransomware is reported to hold the record of 3 out of top 10 largest ransom demands in the year 2022, which accounts for $5.3 million, $9.9 million and $12.5 million [10]. It was also reported that on September 27, 2020, this ransomware infected hospitals in U.S and U.K which belongs to Universal Health Services (UHS), which is one of fortune 500 healthcare companies [10]. These incidents reported to be continued and the same Ryuk ransomware was found to responsible for the attacks happened on Sky Lakes Medical Center, Oregon located in USA and Lawrence Health System located in New York, USA to take computer systems offline and making electronic health records stored on those systems inaccessible and making diverting these healthcare institutions to a stressful condition in the COVID-19 pandemic since these two institutions were already stressed with influx of COVID-19 patients at the time of the attack [10]. Another similar research conducted by a research team consisted of Lauren E Branch, Warren S Eller, Tom K Bias, Michael A McCawley, Douglas J Myers, Brian J Gerber and John R Bassler, to investigate the ransomware against healthcare service providers in the United States in the period of 2016-2017 shows that there were 49 major ransomware attacks were reported against US healthcare organizations [11]. All these attacks were spreaded over 27 states throughout a period of 18 months within the considered time period for the research which is 24 months [11]. The report further highlighted that 6 of the organizations have reported that they paid the ransom demanded by the attackers while there have been no solid evidence about other 43 organizations about whether they had made the ransom payment or not [11]. This data presented in the report brings the attention to a point where the real picture about these ransomware attacks on healthcare industry is much more larger than the data being available for the investigations. Most organizations are hesitant to report any cybercrime incident happened to their organization due to the risk of loosing reputation and customer trust. On the other hand, according to standards, rules, regulations, and policies of state and federal legislature and industry, the organizations are bound to pay fines and compensations to the victims. In this case, to avoid financial losses and to avoid legal consequences, most of the organizations tend to cover up the security breaches which are tolerable and manageable, unless they are being exposed to the public in an unavoidable manner.

Section 4: New attack trends

Modern healthcare institutions uses technologies like Internet Of Things (IoT) to accelerate the rate of services provided by them. Implementation of IoT in healthcare sector is generally categorized under 4 main categories as "IoT for patients", "IoT for physicians", "IoT for hospitals" and "IoT for health insurance companies" [12]. Since these IoT devices have a large variety of functions and designs, it is a good approach to categorize them under such categorization in order to monitor the behavior and security aspect of them. Today, IoT devices are practically and popularly used for

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 1, pp 158-167, January-2024

https://doi.org/10.47001/IRJIET/2024.801019

healthcare functions like remote patient monitoring, glucose monitoring, heart-rate monitoring, hand hygiene monitoring, depression and mood monitoring, Parkinson's disease monitoring, connected inhalers, ingestible sensors, connected contact lenses, robotic surgical procedures and various other major and minor activities [13]. With such increase in use of these sensors, there can be an immense collection of personal health data and personally identifiable information trough all these IoT devices. It should be always remembered that there is a growing security risk of using these IoT devices since there security is not a primary concern from beginning of their production procedures. Main aim of IoT devices are to be mobile and collect, store, process or distribute the data in a short amount of time in the most efficient way possible. To achieve these goals of mobility and efficiency, many of the technical capabilities have to be compromised. For example, to increase the mobility, the IoT device should be made as smaller as possible. Due to that reason, it cannot house sophisticated high processing power components and long lasting battery cells in it. Therefor the processing power of these IoT devices are very little and the battery life is also considerably low. Therefor the manufacturers are only intended to use these devices only to perform expected task with efficient and simple algorithms which needs very low processing power. Low processing power on other hand consumes less energy for the hardware equipment from the battery cells. Therefor IoT device can function for a longer period of time. Therefor, manufacturers often do not use any encryption algorithms to encrypt the data residing, processing or flowing trough these devices because encryption algorithms uses sophisticated logics and needs high processing power and resources when compared with the available processing power of the IoT devices. This immensely contributes to the high vulnerabilities in these IoT devices.

The issue of non-existence of consistency of security protocols for IoT devices used in healthcare sector and their lack of standardization in production is discusses in a research paper published by Patrick M. and O'Hara under the title "Internet of Things Risks in the Energy and Healthcare and Public Health Sectors of U.S. Critical Infrastructure" [14]. The paper highlights the current vulnerabilities associated with IoT devices being used in healthcare and energy sector involving critical infrastructure in U.S and provides an overview of what rules and regulations are being imposed to govern the security aspects of these IoT devices according to U.S laws. This is a good approach in terms of standardizing all the IoT devices under a comprehensive law suits due to the reason that in current market, there are very few such standards are in existence and unlike for other similar electronic devices, there had been very few or no rules and regulations being imposed on them at all by most of the countries in the world. A similar research was carried out by Pradeep Kumar and Hoon-Jae Lee on the topic, "Security Issues in Healthcare

Applications Using Wireless Medical Sensor Networks: A Survey", which highlights on the privacy issues faced by the patients in using wireless sensors which utilizes Wireless Medical Sensor Networks which is abbreviated as (WMSNs) [15]. The research highlights the major concerns in the security aspects of these wireless sensors in terms of privacy related to patients' physiological data and their diseases which they are hesitant to be exposed in public. Taking an initiative towards productive development of the security aspects of these wireless sensors, the research team propose several security requirements which they have been identified as constructive suggestions towards the security of these wireless sensors.

Section 5: Mitigative steps

Ransomware attacks on healthcare sector is unavoidable due to the type of data and the value of data that these healthcare information systems possess. But these risks can be mitigated either to a tolerable amount or at least to a point where it cause a minimum damage which is not lethal. In an article published by the researchers David P. Paul III, Nikki Spence, Niharika Bhardwa and Alberto Coustasse, under the topic "Healthcare Facilities: Another Target for Ransomware Attacks", fact of showing the importance of having a disaster recovery and backup plans is highlighted [16]. Like any other business organization, it is also a vital factor for healthcare industry to have a disaster recovery plans and backup plans in case of loss of confidentiality, integrity or availability of the data residing in the critical infrastructure belonging to healthcare systems. Without a business continuity plan, the healthcare institute will usually have no idea on what are the next steps to be taken in case of a severe incident like a ransomware attack. It is crucial for having a disaster recovery plan and a backup plan to make decisions on whether to pay the ransom or not to pay the ransom, if the management decide not to pay the ransom, then whether they have any way of isolating the infected systems, whether they have a mechanism of cleaning the infected systems and run the systems with backups etc. Importance of a backup plan, is vital for the continuity of any business in case of unexpected deviations. Specially for a critical infrastructure like a healthcare institution, continuity of processes is vital due to the fact that lives and health conditions of patients' are dependent on these systems and residing data. If the data or systems get inaccessible due to a ransomware attack, the healthcare institutions should have an immediate shift to manual processes to continue the usual line of work without disruption to the services. The actions taken in an event of a ransomware attack or any cyberattack incident should be not

ISSN (online): 2581-3048
Volume 8, Issue 1, pp 158-167, January-2024
https://doi.org/10.47001/IRJIET/2024.801019

reactive. Proactive approaches is always highly effective and in such incidents because the employees have an idea about what to expect next and what steps should be taken ahead to stop the spreading of the attack further more. This fact is discussed in a journal article written by Bruno Kelpsas and Adam Nelson under the topic "Ransomware in Hospitals: What providers Will Inevitably Face When Attacked" [17]. It criticizes the reactive approach in incident response management which is addressed as "new normal security mindset" [17]. The facts that highlighted in the article is valid for any organization with reactive security approach, but is inevitably true in case of a security incident which occurs in a healthcare system. Reactive response in security often tends to reflect the lack of planning and enforcement of security procedures and practices and give the impression of lack of mitigative security of the organization. Reactive response is specially more damaging to a healthcare environment because more time that the organization spend on analyzing the incident after it happens, the more data will be damaged or leaked. This is a considerable impact on the personally identifiable information of patients. The suggestions are given at the end of the article is to impose strict penalties and enforcement guidelines to the security aspects of the healthcare organizations trough legislature in order to prompt them to having a proactive approach in facing the risks and security violations. In proactive approach against ransomware attacks, the early detection of ransomware attacks is vital. For this reason many of the advanced technologies are used today in the industry. A research conducted by Mozammel Chowdhury, Sharmin Jahan, Rafiqul Islam and Junbin Gao on the topic "Malware Detection for Healthcare Data Security" [18], discusses about an approach in detecting malware and classifying them with the help of machine learning approaches. The suggested system in the research show that the attacker behavior can be profiled and the malware can be analyzed in a custom sandbox to mitigate the threats of targeted attacks and halt the spear phishing attacks. This is a more defined and fine grained approach since it focuses more on spear phishing attacks which is unique to individuals and varying of the craftmanship of the malware depending on the victim. Another similar research done by Noor Thamer and Raaid Alubady under the topic "A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research" [19], elaborates on using advanced technologies such as blockchain technology, software define network technology and machine learning in order to perform early detection of these malware targeted on health sector. The effort of the research is comprehensive and an exhaustive survey on ransomware attacks have been performed by the research team.

A similar research done by Kanwalinderjit K Gagneja on the topic "Knowing he ransomware and building defense against it – specific to healthcare institutes" [20], takes a different approach and present the user with background knowledge on the steps involved in ransomware attacks in order to identify and prevent them. It is a good approach to educate the general public specially, including the employees in the healthcare environment about different stages of a ransomware attack because, then the employees can identify any unusual behaviors in systems at early stages and take protective measures to contain the attack to a limited scope before its spread.

Although most of the mitigative steps are focused on preventive and avoidance of risks associated with ransomware, there should be other backup plans as well depending on the situation. Not every ransomware attack is similar and not every outcome of an attack is similar. Therefor the individuals and organizations should be flexible in their response mechanisms in an incident. Most of the times, due to the criticality or sensitivity of data and the urgency of restoration for avoiding severe damages, individuals and organizations tend to pay the ransom to the attackers even without no guarantee of getting access to the data. Two similar researches were carried out to elaborate on the legal aspect and implications that might have to be faced by the victims after making a ransomware payment. The first research was conducted by Ibrahim Nadir and Taimmur Bakhshi under the topic "Contemporary cybercrime: A taxonomy of ransomware threats & mitigation techniques" [21], This paper provide a complete approach to the ransomware payment with a solid background with review of history of ransomware and their evolution with a detailed description about the classification of ransomware depending on their inherent attack vectors. The research also provides an overall view on mitigation techniques that can be used to withstand these ransomware attack. The second article was written by Justin Pope under the topic "Ransomware: Minimizing the Risks" [22]. This paper document is more precisely given focus on the state and federal laws of US government on healthcare providers on the liability of patients' data and the legal issues arises when they are violated. Furthermore, it provides a short yet descriptive guidelines on mitigating the ransomware attacks targeted on the healthcare industry.

Another research conducted by Nikki Spence, David P.Paul III and Alberto Coustasse on the topic "Ransomware in Healthcare Facilities: The Future is Now" [23], show the extent of losses in terms of risks, financial losses and liabilities in order for a healthcare organization to get an idea about to what levels they should reach in developing their business continuity and disaster recovery plans. The paper presents ore of proactive mitigative approaches such as educating employees about the ransomware attacks and also stresses on the importance of maintaining the adequate amount of data

ISSN (online): 2581-3048
Volume 8, Issue 1, pp 158-167, January-2024
https://doi.org/10.47001/IRJIET/2024.801019

backups which could be used in an event of business process failures to regain the momentum of the services provide by the organization.

IV. FUTURE RESEARCH

The research done on the current scope is still shows a knowledge gap in security related areas related to most of the new technologies. Among them IoT, Supervisory Control And Data Acquisition (SCADA) systems, Cloud Databases, Virtual Reality (VR) and Augmented Reality (AR) like technologies has to be severely tested and research should be performed. With IoT sensors and equipment, not only the vulnerabilities of the IoT device itself, but the existing apparent vulnerabilities of utility services used by these IoT devices also has to addressed. For example, IoT devices cannot function by themselves at most of the times, They need a means of communication with other devices, which will probably use wireless connections. Then these connections has to encrypted and secured by using end-to-end encryption mechanisms. Proper laws, rules, regulations and specially international standards should be documented in developing and utilizing these IoT devices for healthcare sector. If these IoT devices are connected to a cloud database, then the security of that cloud database has to be taken into consideration. If a certain health organization utilizes any or the cloud services like Infrastructure-as-a -Service (IaaS), Platform-as-a-Service (PaaS) or Software-as-a-Service (SaaS), they should be configured accordingly to ensure the maximum amount of security and also when selecting a cloud service providers for obtaining such a service, a through analysis should be done in order to ensure that these service providers are adhering to the current industrial standards, rules and regulations of the country and whether they are taking liability and responsibility for any of the service disruptions or data corruptions happened due to any faults occurred from their side.

More research should be done on implementing security on service specific SCAADA systems utilized in healthcare industry. It's not adequate to only secure the internal systems of the health organization, but should also protect the endpoints of the internal systems such as points where it connects to other outside systems like, stakeholders, suppliers, patients, general public, doners, utility services etc. Furthermore, the rising use of VR and AR technologies also tend to create a security risk on services offered by some healthcare organizations like virtual clinics, staff training, medical student training, remote client checkups etc. Therefor, these VR and AR devices should be regulated and governed with specific rules and regulations and also the specific standards has to be implemented if they are specifically used for services provided by healthcare organizations.

V. CONCLUSION

By analyzing all the past ransomware attacks and the steps that were taken by those victim organizations, it is still questionable that reasonable amount of concern had been given on the security aspects of the healthcare industry. Most of the healthcare organizations are reluctant to follow the standards like HIPAA n order to obtain the accreditation, but does not bother to maintain the obtained accreditation further once they receive it. This seems to be the one of the major causes that most of the health organizations fail in protecting their electronic patients' records and also cause impact to their computing infrastructure trough ransomware attacks.

Another thing is that these healthcare organizations are often neglecting the other associated standards which has to adhered when incorporating different services to their domain. The major flaw is that, the payments and transactions made trough the online channeling platforms and mobile applications does not adhering to international standards like Payment Card Industry Data Security Standard (PCIDSS). Another thing to consider is that when developing those other utility platforms to inter-related services to healthcare industry, the expert knowledge has to be incorporated and the standards in those industry vertical has to followed with the accepted latest security measures prevailing in those domains. For example, if a healthcare organization is developing a mobile application to provide online channeling services to the patients, the mobile application has to be developed by using secure coding practices like obfuscation, using modularity, using anti-reverse engineering techniques etc. Also if the mobile application uses a local database in the mobile device, the database security also has to be taken into consideration and they should be implemented accordingly.

Furthermore, the public facing websites and other online platforms should be regularly or periodically should be tested for their bugs and should perform penetration tests on them in a regular schedule to ensure up to date security assurance. Another fact to consider is that, the operating systems and other vendor specific utilities purchased or obtained from vendors, developers or third party organizations has to be patched and updated in a timely manner without a delay as soon as the patches and updates are released by the developers or from that organizations.

The employees have to be trained and educated about identifying and responding to security event and infection. They should be properly trained to identify at least general security threats like phishing emails, smishing, social engineering and other basic cyber security threats to ensure that the organization is safe from every perspective. Since humans are the weakest link in any security system,

ISSN (online): 2581-3048
Volume 8, Issue 1, pp 158-167, January-2024
https://doi.org/10.47001/IRJIET/2024.801019

employees are the major loophole and the easiest to break—trough and gain the access to the internal systems, since the employees are given access to the internal infrastructure of the systems at any point during their daily work routines, making extremely vulnerable attack surfaces which most of the attacker try to exploit in the first hand in most of the cases. It has to be understood that achieving perfect level of security is not practical since any of these healthcare systems are not isolated systems. Therefore, the risks has to accepted in a tolerable amounts without compromising the security at its entirety. Best approach is to go for other approaches like risk mitigation, avoidance, and risk transfer like techniques. In risk mitigative steps, it is always better to give priority and more weight on implementing proactive security measures like business continuity plans, disaster recovery plans, backups etc. But that does not mean that the reactive approaches should be neglected. Every attack incident is different from one another. Therefore, there is no standard template to face the upcoming attacks. For an instance, an exploitation of a zero-day vulnerability might overrun all the proactive procedures in facing a security breach. In such an instance, strong and flexible reactive response plans should also be there to identify the attack and make better suited correct and quick decisions in more effective manner to mitigate the further spread of the attack within the internal network and thereby containing the attack before it could damage the other systems and residing data.

There will be no use if the consumers of these digital services offered by the healthcare organizations acts in an unsecure manner. The consumers, which are patients also have a some amount of access to these systems. Also their personal data is also stored in their mobile devices. If the patients are not considered or oblivious about the security of their own devices, leaking of personal data could happen trough the consumer-end. Whether the leakage of personal data happens from the service provider's side or whether it happened from the consumer's side, the outcome would be same which is the loss of confidentiality. Therefor the consumers or the patients who are obtaining these healthcare services should also be educated about their data privacy and security and a general understanding and awareness should be provided on identifying basic types of cyber attacks and what should be the steps that they should follow if they become a victim of such an attack.

Finally, the governments have to change and re-enact proper laws, policies, standards, rules and regulations to address the current mismatches of laws associated with the new technologies and has to be updated in a timely manner with the evolving and emergence of new technologies.

ACKNOWLEDGMENT

I would like to thank with due respect, to my lecturer in-charge of Security Economic Analysis (IE4022) module, Mr. Kanishka Yapa from Department of Computer Systems Engineering, Faculty of Computing, Sri Lanka Institute of Information Technology (SLIIT), Malabe, Sri Lanka, for gifting me with this precious knowledge in the field of Cyber Security and guiding me always in the correct path.

I would like to thank Mrs. Aathika Salam, Lab instructor, Sri Lanka Institute of Information Technology (SLIIT), Malabe, Sri Lanka, for gifting all knowledge and for the continuous support provided at lab works.

I would like to thankfully appreciate the opportunity provided by my university for studying such a precious subject field while providing me with the best of available knowledge and facilities trough the entire process of this academic journey. I would like to thank all the academic and non-academic staff at Sri Lankan institute of Information Technology (SLIIT), Malabe, Sr Lanka for helping me with tremendous support whenever requested.

Finally, I would like to thank all my collogues at Sri Lankan Institute of Information Technology (SLIIT), Malabe, Sri Lanka, for keep motivating me throughout this research work to make this effort, a success.

REFERENCES

[1] Kaspersky, "What is Ransomware?," Kaspersky, 2022. [Online]. Available: https://www.kaspersky.com/resourcecenter/threats/ransomware. [Accessed 16 May 2022].

[2] U.S. Department of Health & Human Services , "Health Information Privacy," U.S. Department of Health & Human Services , 2022. [Online]. Available: https://www.hhs.gov/hipaa/index.html. [Accessed 16 May 2022].

[3] N. A. R. A.K.Maurya, "Ransomware: Evolution, Target and Safety Measures," International Journal of Computer Science and Engineering, vol. 06, no. 01, pp. 80-85, 2018.

[4] J. F. Dyro, Clinical Engineering Handbook, NewYork: Academic Press, 2004.

[5] A.Q. Ayed, "Evolving Ransomware Attacks on Healthcare Providers," Utica College ProQuest Dissertations Publishing, New York, USA, 2020.

[6] A.M. Malcolm Harkins, "The Ransomware Assault on the Healthcare Sector," HEINONLINE, 2018. [Online]. Available: https://heinonline.org/HOL/LandingPage?handle=hein.

ISSN (online): 2581-3048
Volume 8, Issue 1, pp 158-167, January-2024
https://doi.org/10.47001/IRJIET/2024.801019

j ournals/jlacybrwa6&div=16&id=&page=. [Accessed 16 May 2022].

[7] R. Brandom, "UK hospitals hit with massive ransomware attack," THE VERGE, 12 May 2017. [Online]. Available: https://www.theverge.com/2017/5/12/15630354/nhshospitals-ransomware-hack-wannacry-bitcoin. [Accessed 16 May 2022].

[8] S. K. K. H. G. M. A. D. P. A. S. Ghafur, "A retrospective impact analysis of the Wanna Cry cyberattack on the NHS," npj Digital Medicine, p. Article number 98, 02 October 2019.

[9] Cybersecurity & Infrastructure Security Agency, "Ransomware Activity Targeting the Healthcare and Public Health Sector," Cybersecurity & Infrastructure Security Agency, 28 October 2020. [Online]. Available: https://www.cisa.gov/uscert/ncas/alerts/aa20-302a. [Accessed 16 May 2022].

[10] TREND MICRO, "What Is RYUK Ransomware?," TREND MICRO, 2022. [Online]. Available: https://www.trendmicro.com/en_us/whatis/ransomware/ryuk-ransomware.html. [Accessed 16 May 2022].

[11] W. S. E. T. K. B. M. A. M. D. J. M. B. J. G. J. R. B. Lauren E Branch, "Trends in Malware Attacks against United States Healthcare Organizations, 2016-2017," GLOBAL BIOSECURITY, New South Wales, Australia, 2019.

[12] M. J. M. Dr. Rajashekhar Karjagi, "What can IoT do for healthcare," wipro, [Online]. Available: https://www.wipro.com/business-process/what-can-iotdo-for-healthcare-/#:~:text=IoT%20has%20applications%20in%20healthc are,physicians%2C%20hospitals%20and%20insurance%20companies.&text=They%20can%20track%20patients'%20adherence,connect%20with%20the%20pati. [Accessed 16 May 2022].

[13] ordr, "10 INTERNET OF THINGS (IOT) HEALTHCARE EXAMPLES," ordr, [Online]. Available: https://ordr.net/article/iot-healthcareexamples/. [Accessed 16 May 2022].

[14] P. M. O'Hara, "Internet of Things Risks in the Energy and Healthcare and Public Health Sectors of U.S. Critical Infrastructure," Utica College ProQuest Dissertations Publishing, Eisenhower Parkway, Ann Arbor, USA., 2019.

[15] H.-J. L. Pradeep Kumar, "Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey," Sensors, vol. 12, no. 01, pp. 55-91, 2011.

[16] N. S. N. B. A. C. David P. Paul III, "Healthcare Facilities: Another Target for Ransomware Attacks," in 54th Annual MBAA Conference, Chicago, USA, 2018.

[17] A.N. Bruno Kelpsas, "Ransomware in Hospitals: What Providers Will Inevitably Face When Attacked," The Journal of Medical Practice Management: MPM, vol. 32, no. 01, pp. 67-70, 2016.

[18] S. J. R. I. a. J. G. Mozammel Chowdhury, "Malware Detection for Healthcare Data Security," in International Conference on Security and Privacy in Communication Systems, Cham, Denmark, 2018.

[19] R. A. Noor Thamer, "A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research," in 2021 1st Babylon International Conference on Information Technology and Science (BICITS), Babil, Iraq, 2021.

[20] K. K. Gagneja, "Knowing the ransomware and buildng defense against it - specific to healthcare institutes," in 2017 Third International Conference on Mobile and Secure Services (MobiSecServ), Miami, FL, USA, 2017.

[21] T. B. Ibrahim Nadir, "Contemporary cybercrime: A taxanomy of ransomware threats & mitigation techniques," in 2018 International Conference on Compting, Mathematics and Engineering Technologies (iCoMET), 2018.

[22] J. Pope, "Ransomware: Minimizing the Risks," National Library of Medicine, 01 December 2016. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5300711/. [Accessed 16 May 2022].

[23] D. P. I. A. C. Nikki Spence, "Ransomware in Healthcare Facilities: The Future is Now," in Academy of Business Research, Fall 2017, Atlantic City, New Jersey, USA, 2017.

AUTHOR'S BIOGRAPHY

Deemantha N. Siriwardana, (Undergraduate in Cyber Security, Sri Lankan Institute of Information Technology) currently follows academics in final year of BSc (Hons) in Cyber Security program related to Department of Computer Science and Engineering at Sri Lankan Institute of Information Technology (SLIIT), Malabe, Sri Lanka. He joined SLIIT in the year 2019 and the degree was dated to be completed by the end of year 2022. He is currently following the academics in the fields of Security Economic Analysis and Cyber Forensic Investigations and

ISSN (online): 2581-3048
Volume 8, Issue 1, pp 158-167, January-2024
https://doi.org/10.47001/IRJIET/2024.801019

Responses. Currently his research works focuses on Cryptographic algorithms and incorporating behavioral biometrics and anti-forensic techniques in mobile and IoT security.

Citation of this Article:

Deemantha N. Siriwardana, "Ransomware Threats Targeting the Healthcare Sector" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 8, Issue 1, pp 158-167, January 2024. Article DOI https://doi.org/10.47001/IRJIET/2024.801019

****

