Written evidence submitted by Chandrashekar Subbarao, Dr Suresh Renukappa, and Dr Subashini Suresh, Faculty of Science and Engineering, University of Wolverhampton

Ransomware Cyber Attacks in the Healthcare sector

Executive Summary

- In an increasingly connected world and a very rapidly evolving technology landscape, the threat to cyber security is exponentially increasing. The healthcare sector is one of the most attacked sectors in the world. Between 2020 and Q2 2022, the volume of ransomware attacks peaked in Q2 2021 with 188.9 million attacks. There have been continuous attacks on the healthcare systems since long, a significant recent one being in the month of August 2022.
- Attacks to the healthcare system can literally be a matter of life and death. It causes severe disruptions to the processes and directly affects the quality of service thus endangering lives.
- NHS manages more than 250,000 outpatient appointments on an average per day and operates 1229 hospitals across UK. All of these are connected technically in some way or the other. Any disruption to their systems can potentially be disastrous to the patients.
- All healthcare organisations therefore should necessarily have strong cyber security measures in place so that patients' data is protected and more importantly, it is fundamental to delivering high quality and safe services to patients.
- Digital healthcare has to be especially robust in its handling of security as it involves personal and sensitive data of patients, which should be protected from being compromised. This obligates the health systems to be able to repel all security threats, ransomware being the foremost of such threats. Ransomware is next only to phishing as a means of data breaches and leaks.
- Ransomware attacks have been spreading like wildfire and will only worsen as more and more devices, people and systems are getting connected.
- Healthcare services and its systems use many critical medical devices and equipment – such as MRI scanners, ultrasound scanners, blood analysis devices, heart health monitors etc. These are all connected to the internet and therefore become vulnerable. It may be noted that the WannaCry attack had indeed affected many such devices.
- As digitisation of the health systems is imperative, with digital or smart systems being the solution for effective delivery of services at scale, an extremely robust security policy has to be defined and implemented by all service providers.
- Ransomware (as the name betrays) attacks could be a monetary drain if ransom has to be paid. Data breaches, especially of personal health data can also lead to serious legal issues.

Written evidence

- Evidence is provided by conducting a survey of available material in public domain on ransomware and other cyber security attacks on healthcare systems. The WannaCry ransomware attack that affected many NHS service providers in 2017 was perhaps the most significant attack in the UK. There have been many more reported, the last significant one being in August 2022.

- According to a study by a leading security company, more than 80% of UK healthcare organisations have been subjected to a ransomware attack in the last year, 2021. Also, a survey of 100 cybersecurity managers in the healthcare sector found that as many as 38% have resorted to pay the ransom to recover their files/systems. The study also noted that about 44% had refused to pay ransom, but ended up losing the healthcare data. Losing of healthcare data is not just disruptive to the systems, but is a serious data security breach of patient data.
- The healthcare industry has generally been slow to catch up with the industry with regard to security measures. This lag has caused the healthcare industry to be a prime target for data theft. The healthcare industry therefore, also has to follow other industries in clearly defining cyber security policies and duties.
- The National Cyber Security Centre (NCSC) has published the Cyber Essentials Plus standard, which should be adopted by all the healthcare organisations. In addition, specifically for data security, there are data security standards recommended by the National Data Guardian (NDG). This should become the basis for all healthcare organisations in order to reduce the vulnerability to attacks.
- Constant technology upgradations, not using very old software, following basic cyber hygiene like using good passwords, not sharing passwords and a general organisational and systems-usage culture that is tuned to data security are key to reducing vulnerabilities to cyber-attacks.
- Post WannaCry attack in 2017, the UK government had published a very detailed ‘Lessons learned’ along with a number of recommendations. These recommendations span across the organisational structure, processes to manage incidents, people and technology. These have to be reviewed and adherence has to be ensured.
- As people are central to any security, all users working with the healthcare provider systems have to be fully trained from a security perspective. This training will need to be constantly upgraded and delivered at frequent intervals. Henceforth, making this training mandatory to up keep with the threats of cyber-attacks. There has to be a strong people centric approach to cyber defence as most malware (ransomware) makes its way through injudicious use of the systems by individuals.

15 December 2022