Addressing the Cyber Resilience of Healthcare Systems During the Coronavirus Pandemic

Rebecca Lucas and Sneha Dawda
Commentary, 28 April 2020
Coronavirus, Cyber, Cyber Security, United States, North America, UK, Domestic Security, Resilience, Technology, Europe

Increased public attention on the digital infrastructure underpinning healthcare systems during this pandemic is an excellent reason to boost its security.

The cyber security of the healthcare sector, both in the UK and abroad, is a longstanding problem that will persist after this pandemic has passed. Due to the current public attention and easy acceptance that this is an important goal, allocating public funding for necessary cyber security measures in the healthcare sector could be more easily justified.

This pandemic has already alerted us to the dangers of ignoring the weaknesses in the cyber resilience of healthcare platforms. There were incidents such as the distributed denial of service (DDoS) attack on the US Department of Health and Human Services (HHS) and several attacks on Czech hospitals. However, there are ways in which the current health crisis represents an opportunity for governments to build cyber resilience in both public and private healthcare.

HEALTHCARE WAS AND IS VULNERABLE TO CYBER ATTACKS

Digital healthcare infrastructure has historically been vulnerable to numerous types of cyber attack. This is partly because of the nature of the sector: healthcare organisations are some of the most likely to hold personal data, with 68% saying they are highly likely to hold personal data according to the 2019 Cyber Breaches Survey by the UK's Department of Digital, Culture, Media and Sport. While this commentary focuses on western infrastructure, the problem is of a global nature: 1.5 million Singaporean citizens had personal data stolen in a 2018 attack on healthcare infrastructure.

The sector as a whole often struggles with tight budgets and scarce resources, reducing its ability to spend on advancing and securing digital infrastructure overall. Cost is cited as one of the biggest impediments for implementing new technology in the UK public health system. In the US, healthcare companies are likely to devote less than 5% of IT budgets to security, a significantly lower proportion than other industries. Meanwhile, 83% of US healthcare organisations reported an increase in cyber attacks in 2019.

In the UK, damage caused by the 2017 WannaCry ransomware attack highlighted insufficiencies in current IT processes. The attack that severely impeded access to National Health Service (NHS) services at the time prompted an investigation of and, ultimately, upgrades to NHS digital infrastructure. This included the formal adoption of the National Data Guardian's 10 data security standards across the NHS, investment in a new Security Operations Centre, and increased auditing and security assessments of NHS organisations. As of 2019, the government had allocated £210 million to improve the healthcare system's digital security and resilience. These measures have significantly enhanced the resilience of UK digital healthcare infrastructure. Still, 67% of healthcare organisations in the UK experienced a cyber security incident in 2019.

CORONAVIRUS HIGHLIGHTS CURRENT VULNERABILITIES

With coronavirus currently dominating daily life, society's reliance on the healthcare system has never been greater. While some threat actors and groups have said they will refrain from attacking healthcare services, others have taken advantage of this reliance. The Intergal Cybercrime Threat Response Team issued a notice alert to law enforcement agencies across 194 countries in order to warn them of the incoming onslaught of cyber attacks on critical healthcare institutions amid the global pandemic. Further complicating the issue is the divide between public and private health infrastructure. Currently, in the UK, private healthcare facilities have been requisitioned in the effort to fight coronavirus, thereby increasing the potential vulnerabilities of the health sector overall. In times of crisis, not only is the cyber security of public health infrastructure imperative, but also the resilience of private healthcare. Since such requisitioning is to be expected in emergencies, the cyber security of public and private healthcare infrastructure must be treated as a whole for the purpose of this discussion.

The US in particular has experienced numerous attacks to healthcare providers and infrastructure as the coronavirus has spread. A string of ransomware attacks that began in 2019 continued to escalate, affecting healthcare organisations across multiple states including Illinois, Texas, North Carolina and New York. In 2020, including the previously mentioned HHS attack, doctors' computers at the Children's Hospital Boston experienced outages in February due to malware. Another attack in February installed cryptocurrency mining malware on the University of Kentucky Healthcare network, causing temporary failures in a system serving approximately 2 million patients. Overall, according to the HHS Breaches database, 143 breaches have been reported so far in 2020 affecting an estimated 3.3 million individuals (not including those affected by the University of Kentucky breach).

While many of these attacks may not be directly related to the coronavirus pandemic, experts have warned that the pandemic presents an opportunity for threat actors. The FBI has warned coronavirus research centres and institutes that they may be targeted by foreign hackers. Multiple cyber attacks on the networks of Czech hospitals have also caused significant international concern. While the Czech systems were very resilient, one hospital had coronavirus testing operations disrupted by a ransomware attack. According to news reports, Czech officials suspected that it might have been the work of a sophisticated attacker. Despite its recent improvements to digital infrastructure, concerns have also been raised specifically about cyber security in the NHS. Across the world, many cyber security processes and risk management assessments designed for 'normal' times are now feeling the strain of a global pandemic. This brings into question the degree of impact a cyber attack may have on current healthcare and whether current defences and incident response procedures can handle the disruption.

PRIORITISING CYBER RESILIENCE IN HEALTHCARE

Cyber attacks on public health infrastructure are a major cause for concern. The increased attention created by the coronavirus pandemic offers an opportunity for policymakers to identify vulnerabilities in public health infrastructure while under significant strain. The pandemic creates a unique opportunity to see how healthcare infrastructure functions in a time of crisis. In time, these lessons may help develop actionable solutions that can better defend the network against future stresses. The UK is currently on the leading edge of cyber resilience efforts, but still has more to do to ensure the security of the digital infrastructure underpinning hospitals, general practitioners and pharmacies throughout the country.

Cyber investment and risk management must not be neglected by private healthcare providers. 65% of Chief Information Security Officers in care services claim they lack in-house cyber security expertise to provide sufficient incident response to a cyber attack. The private sector is a critical component of national healthcare, particularly in the US. Governments across the world must consider policy options to induce investment and action from private healthcare providers, either through regulation, guidance or standards.

Investment in cyber security in a post-coronavirus world is potentially at risk when we face a major economic recession and potential budget cuts. However, the increase in public attention combined with the critical nature of the healthcare system provides policymakers with a justification to focus funding and resources on a sector that has suffered significantly from cyber attacks. Avoiding costly incident response and damage control by investing in cyber resilience will reduce the burden on an economically strained situation. It is imperative that investment in cyber security across public health infrastructure remains a priority in spite of economic strain.

A national healthcare system is only as resilient as all its component parts. Cyber security in the healthcare sector will remain critical long after the damage from coronavirus has been mitigated.

The views expressed in this Commentary are the author's, and do not represent those of RUSI or any other institution.

BANNER IMAGE: A computer is used to operate medical equipment in a hospital. Courtesy of the public domain.

Print

AUTHOR

Rebecca Lucas
Research Analyst, Cyber Threats and Cyber Security

Rebecca Lucas is a Research Analyst in Cyber Threats and Cyber Security. Her current work focuses on managing risks stemming from the... read more

Sneha Dawda
Research Analyst

Sneha is a Research Analyst in cyber threats and cyber security. Her research focuses on cyber security policy and strategy both... read more

Related

ALL COMMENTARY PUBLICATIONS MULTIMEDIA NEWS EVENTS

Trilateral Track 2 Nuclear Dialogues Consensus Statement

News, 4 May 2020

In collaboration with the Center for Strategic and International Studies (CSIS) and the Fondation pour la Recherche Stratégique (FRS), RUSI co-hosted the 2019 Trilateral Track 2 Nuclear Dialogues. These dialogues bring together former senior officials, nuclear policy experts and government representatives from the US, France and UK to discuss nuclear deterrence, arms control and non-proliferation...

Tags: United States, Americas, France, Proliferation and Nuclear Policy, UK, Europe

Coronavirus and International Security: Risks and Opportunities

Commentary, 1 May 2020

Alistair Harris OBE

The Global South is facing new challenges as a result of the pandemic, and these require new approaches, however difficult the current situation is.

Tags: Coronavirus, Global Security Issues, Resilience

Russia's Policy of Passport Proliferation

Commentary, 1 May 2020

Neil Melvin

With new amendments to Russia's Law on Citizenship, the Kremlin is establishing a legal pretext to threaten or actually to use force based on a claim to protect Russian citizens resident in neighbouring states.

Tags: International Security Studies, Russia, Europe

1 2 3 4 5 6 7 8 9 ... NEXT › LAST »