RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 020 – 13 February 2019

SingHealth Cyber Attack: Learning from COI Findings

By Shashi Jayakumar

SYNOPSIS

How do we protect our critical information infrastructure from evolving threats? What steps do we need to take to prepare for future adversaries who are continually refining their methods? How can these steps be applied to the health sector?

COMMENTARY

NOW THAT that the dust has settled, it is possible to draw some conclusions from the findings of the Committee of Inquiry (COI) into the SingHealth cyber attack. The overall impression that emerges from a deep reading of the COI report is that of a culture of complacency at SingHealth and Integrated Health Systems (IHiS), the Ministry of Health's IT arm.

There were multiple and egregious failures in awareness and incident reporting. But there was another form of complacency, not dealt with in depth in the COI report but worth remarking on. This was a basic lack of awareness as to what was going on in the wider world. Threat scanning of the most basic kind will show innumerable attacks against health systems elsewhere in recent years.

They Should Have Seen It Coming

Academics in Singapore had also on at least one occasion prior to the attack publicly warned of the risk of attacks against the healthcare system.

Cyber criminals (some possibly working in concert with, or at the behest of larger actors like states) have found healthcare data extremely lucrative as a target. The well-known 2017 United Kingdom National Health Service Wannacry hack comes to

mind, but there have been many attacks against healthcare providers in the United States as well.

(According to a 2016 Accenture report, cyberattacks against US health systems alone will cost hospitals US$305 billion over the next five years, and one in thirteen patients will have their data compromised by a hack).

In other words, SingHealth and IHiS should have seen this coming.

"Defence-in-Depth": The Only Option

So where do we go from here?

There is no option but to move towards the "Defence-in-Depth" approach which features prominently in the COI recommendations. This is a layered concept. It involves highly-trained defenders arming themselves with centrally-managed endpoint detection and response systems, layered with advanced behaviour-based analytics which gives real time and holistic (as opposed to historical) perspective on security within the system.

As the COI report acknowledges, the move to Defence-in-Depth will not happen quickly, given the differing cyber security maturity levels in organisations and the trade-offs between operational requirements and costs. This is a key concern.

How long do key sectors and critical information infrastructure (CII) have to move in positive directions, given not just the necessary changes in resourcing but also in organisational culture? Consider two major observations by the COI.

Need to Build Internal Ecosystem of Expertise

First, SingHealth was reliant on IHiS to manage its cyber security risks. The report notes that there should be appropriate cyber security expertise at SingHealth's senior management level, rather than having this capability wholly outsourced. Key sectors and critical CII will likely have to move in these directions.

The other critical aspect of Defence-in-Depth is a trained cadre of cyber professionals. As Prime Minister Lee Hsien Loong observed in relation to the attack: "We have to train up our people, institute robust processes, inculcate the right mindsets and enforce accountability." This will take some time to materialise.

While many government agencies have launched various schemes to beef up the pool of IT and cyber security experts here, creating an ecosystem of trained security professionals will be a multi-year effort. In the SingHealth/IHiS cases, there were resourceful individuals who attempted to get to grips with the intrusions, although even those who displayed initiative during the hack were at times out of their depth against a skilled adversary.

This, however, should be counted as something of a bright spot. States which have faced kinetic threats have made it a habit to quickly promote resourceful individuals, even if they may be junior in years or rank. We should do the same in cyber security.

Future Threats and Our Approach

In some ways, Singapore continues to be lucky. We have not yet had a cyber attack that causes actual damage – for example to Industrial Control Systems or Supervisory Control and Data Acquisition systems. We cannot rule out future attacks targeting critical infrastructure or the vast attack surface of the nascent Smart Nation, in order to try to exfiltrate information and data of the type which tells of a society's core vulnerabilities. This in turn can be used for fake news or disinformation campaigns.

How do we drill for these bewildering new threats and adversaries who are continually honing their methods? This is difficult, but possible. Relevant agencies should take a leaf from the way terrorism drills over the years have become increasingly realistic, drawing in greater number of agencies and greater swathes of the mass public at all ages (think for example school lockdowns). We need the same kind of mass readiness for cyber, to prepare us for a digital Pearl Harbour.

Some CII operators in Singapore have been proactive. The Maritime and Port Authority established a Maritime Cyber Security Operations Centre in November 2018 to monitor cyber threats against CIIs. It has also tapped the confidence and trust it had built up with partners overseas to recently establish a network of ports in Asia and Europe to foster closer collaboration and exchange of information on cybersecurity issues.

The health sector and for that matter all CII operators (including energy and aviation, which might feel somewhat removed from the threat) should consider similar networked approaches with counterparts overseas.

Need For New Thinking

Separately, a vulnerability audit should be conducted, starting with CII operators, in order to have an in-depth, holistic perspective of which operators are reluctant or slow to update their cyber security and more importantly their culture. Following this, sectors that are not technically part of Singapore's cyber CII, such as universities (in particular those parts which work with government and do sensitive research work) should be subject to scrutiny.

It is not clear how long it will take CIIs and other key sectors to fully digest the implications of the SingHealth hack (and also, now, the HIV data leak). Likewise, can the stakeholders fully absorb the full import of the COI recommendations?

Can they understand the essential dictum put forward by the Chief Executive of the Cyber Security Agency, David Koh, at the COI: That cyber security should be a key feature rather than "slapped on as an afterthought", with business efficiency privileged above it, as is often the case now.

If new thinking permeates at all levels, then some good would have come out of an otherwise disturbing saga.

Shashi Jayakumar is Head, Centre of Excellence for National Security (CENS) and Executive Coordinator, Future Issues and Technology at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore. *This commentary first appeared in TODAY, 7 February 2019.*

Nanyang Technological University
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg