BioSpectrum
the business of Bio & Health Sciences
ASIA EDITION

Balancing digitalized healthcare services and data security

20 January 2021 | Opinion

In conversation with George Lee, Vice President, Asia Pacific, and Japan of RSA

COVID-19 pandemic has changed the way healthcare, pharma and clinical industry operate and has propelled the pace of digitization exponentially. The surge in virtual healthcare has prompted physicians globally to engage in co-sharing of their medical expertise. Pandemic has a relatively positive impact on the Healthcare and ITC industry with a surge in digitized and personalized approaches. The partnership between Analytics and AI is also optimizing healthcare resource's capabilities. Yet, there remains a digital-risk with the prevailing tele and remote healthcare modules which threatens data security and associated cyber threats. **George Lee, Vice President at RSA securities** who leads the overall RSA business across Asia Pacific shares further insights on novel complex digitized health solutions and their effective management.

What are some of the unseen risks of digitalised healthcare services such as telemedicine, AI-powered healthcare chatbots and cloud-based medical apps?

The global health crisis has undoubtedly accelerated the digital transformation in the healthcare industry, pushing remote and technology-driven healthcare services such as telemedicine into the fore over the last several months. For instance, a recent report by Bain & Company revealed that digital visits to Singapore's MyDoc platform have risen more than 160% in the wake of the pandemic. This shows the changing consumer behavior towards digital health innovations during this unprecedented time where safe distancing has become the new normal for many of us.

While telemedicine, digital health records, internet-connected medical devices, patient wellness apps, and digital third parties entering the healthcare supply chain are becoming more accessible to markets across the Asia Pacific in order to improve patient care and response times, such technologies have also exposed the healthcare industry to cyber attacks.

So far, in 2020, cyber incidents ranked as the most serious business risk globally, with the World Health Organisation reporting a five-fold increase in cyber attacks directed at its staff, and email scams targeting the public at large in April alone. But cyber attacks against the healthcare industry are nothing new because personal health information are highly prized by cybercriminals looking for opportunities at identity theft or credit card fraud. Another industry report found that health sector

breaches are the costliest at US$7.13 million compared to average global data breach cost of US$3.86 million across sectors.

The risk of a cyber attack is also the result of associated risks emerging from this rapid pace of digital transformation, particularly **dynamic workforce risk** and **third-party risk.** The necessary shift to a dynamic, mobile workforce exposes healthcare organisations to the risk of improper worker access and authentication. This is especially concerning when it is also difficult to effectively monitor the activities of every healthcare staff across dozens of internet of medical things (IoMT) devices, with a laggard cybersecurity defense.

At the same time, the healthcare industry's move to telemedicine meant that electronic health records can be accessed by consultants, vendors and other third parties outside of their organisation to facilitate efficient operation – making them attractive targets by cybercriminals. When left unguarded, this could lead not only to exposure of sensitive patient data but also impact a healthcare organisation's brand, reputation, and compliance posture.

What are the challenges involved in securing medical data in digitalised services?

Despite the innovative transformation happening in the healthcare industry, many of them have not fully modernised their legacy IT systems. In May 2019, Microsoft made fixes for a handful of legacy operating systems it no longer supports, which are still widely used by the healthcare sector for a number of medical devices.

This myriad of legacy IT that exists across the healthcare ecosystem is a cause of concern because it exposes them to a multitude of security vulnerabilities, and ultimately becomes harder for cybersecurity teams to protect against the increasingly sophisticated and expanding cyber threat landscape.

In addition to navigating a maze of legacy systems, healthcare organisations need to manage a heterogeneous community of patients, staff, suppliers, insurers, regulators, and a host of other third-party partners. These are diverse stakeholders with varying levels of cybersecurity awareness. Compounding the matter is the ever-growing digital ecosystem of devices and services that they need to deploy, which require strict compliance according to market-specific regulatory mandates.

The confluence of these requirements and characteristics makes managing digital risks and ensuring best-in-class cybersecurity practices extra-challenging. But it does not mean that these challenges are unsurmountable. Armed with the right security tools and measures in place, there is an opportunity for healthcare organisations to build their cyber resiliency as we head into the post-pandemic era.

How can different stakeholders such as the healthcare providers, government and patients work together to ensure the security of medical data?

Managing cyber risks are traditionally the responsibility of an organisation's security teams and for top target industries like healthcare, it is only expected that they should be in place to lead and drive best practices and comply with existing standards. However, to address cyber risks more holistically, it also needs a strong collaboration of various stakeholders, ranging from an organisation's leadership team to the patients themselves, external partners, and the government:

The ownership of a health organisation's cybersecurity must be mandated by the **senior leadership** to ensure that the right resources are allocated to empower not only their security teams but also their own staff in mitigating cyber threats.

Cybersecurity is also be the responsibility of **patients**, and healthcare providers play an important role in educating them on how to secure their own data. It cannot be emphasised enough that security awareness and good security hygiene must go hand in hand for today's digital-savvy end users.

Vendors, insurers and other third parties are not only partners in providing quality healthcare services but also in protecting a healthcare organisation's critical and sensitive medical resources. It is crucial to secure third-party access and ensure that third-party identities are properly governed within the healthcare organisation's security parameters.

The **government** must – alongside healthcare organisations – improve the state of cybersecurity. Singapore's Safer Cyberspace Masterplan 2020 is one example. While government should establish the mandatory minimum framework or standards for security, it is the responsibility of healthcare organisations to ensure compliance and robust implementation.

With the potential of the COVID-19 vaccine becoming publicly available in various countries globally in 2021, we can expect to see an increase of vaccine-related phishing attacks targeted at the healthcare industry. Therefore, cybersecurity defense becomes only effective when every stakeholder has collective ownership for every aspect of the cybersecurity approach.