Cyber Risks Facing Clinics

Text by Dave Gurbani and Dr Chow U-Jin

Dave is the founder and Chief Executive Officer of Cybersafe Pte Ltd, and partner of FinCybersafe, the only healthcare-focused cybersecurity solutions provider in Singapore.

Dr Chow is a doctor-turned-entrepreneur and banker. He looks after all things financial for doctors and healthcare professionals so that they can focus on what they do best.

Digital threats facing clinics have risen exponentially since the outbreak of COVID-19. Globally, hacker groups have been observed targeting healthcare and medical services providers during the pandemic to either steal patient information or to threaten clinics with public leaks in order to coerce them into acceding to the hackers' ransom demands.

According to the Cyber Security Agency of Singapore's (CSA) Singapore Cyber Landscape Report in 2020, the healthcare sector is one of the **top three targets** of ransomware in Singapore, with a 154% collective increase from pre-pandemic days in 2019. In today's context, doctors must be aware of specific digital risks they may face in daily clinic operations and steps that they can take to mitigate them.

Digital loopholes among clinics

Since 2017, CyberSafe has observed that many of these clinics face similar digital loopholes that majorly contribute to their overall cyber risks. These include:

1. Having outdated operating systems on their computers (eg, Windows Vista).
2. Using unlicensed/outdated Office Applications (eg, Microsoft Word 2010 to 2013).
3. Overall poor cyber hygiene practices (eg, using the clinic fax number as the Wi-Fi password).
4. Doctors and nurses not enabling Two-Factor Authentication (2FA) on the Clinic Management Systems (CMS) (eg, no 2FA enabled for doctors/nurses to access Plato CMS).

Many of these commonly seen loopholes can dramatically increase the risk of hacking and data breaches to clinics. One common issue is in the Microsoft Office 2010 to 2013 suite, which possesses a security flaw that will enable certain malicious files to be executed when clicked on. These files will usually be sent via spam or spoofed emails that are specially crafted into tricking the recipient to open attached documents that have malicious code embedded in them. The outdated Office application will then be used as a vessel to execute the malicious code contained in these attached documents to do things like spread viruses to the system or even execute ransomware.

Another critical loophole is having weak or similar passwords, such as adding a few digits after the clinics' name or using contact information that can be found online. Using such passwords for accounts like clinic emails and CMS would be akin to simply handing over sensitive clinic and patient data to potential hackers. A notable example of this would be the SingHealth breach in 2018. The Personal Data Protection Commission's (PDPC) report on the breach indicated that the hackers gained initial access by infecting a user's workstation which had likely originated via a phishing email. Subsequently, after more malicious tools were installed into the workstations, administrator accounts were breached due to having an easily deducible password – *P@ssw0rd*.

When a clinic is breached by hackers, daily operations will become difficult as most do not plan for such situations. In Singapore, breaches and loss of medical related information is reportable to the PDPC within three calendar days of confirmation. Investigations by the PDPC will hinder the daily running of the clinic and its digital systems (eg, laptops, desktops, CMS) as investigators will attempt to ascertain the cause and damage of the breach. The Ministry of Health has released a set of guidelines via the Healthcare Cybersecurity Essentials to complement data protection obligations set out by the Personal Data Protection Act. Doctors must take an increased emphasis in meeting these obligations to protect patient- and employee-related information.

Simple cyber hygiene practices

With the rise in the use of digital systems post-pandemic, doctors should be aware of the above four most commonly found security loopholes that severely increase the risks of being hacked or, even worse, having patient information stolen. These security loopholes can be easily identified and remediated, improving the overall cyber defence posture of your clinics.

Remediation includes:

1. Changing all passwords of accounts used in the clinic to passphrases (eg, Wh0sTh3r3!?) that utilise:
   - Uppercase and lowercase letters
   - Numbers and symbols
   - Minimally eight characters long
2. Using a password manager to help generate and store complex passwords (eg, Nordpass, Lastpass).
3. Checking to see if your Microsoft Office Applications are outdated and required upgrading (https://bit.ly/3yhN5kv).
4. Learning how to enable 2FA on your CMS.
   - Contact CMS Vendors to ask for documented steps. Most cloud CMS have 2FA features available.
   - Explore the settings page of your CMS and look for a security tab that will contain steps to enable 2FA to either a mobile phone or a third-party app like Google Authenticator.
5. Reading PDPC's guide on Managing Personal Data (https://bit.ly/3biMp57).

With technology changing every day, it can be difficult to navigate the many angles of risk they include. However, some risks can be easily managed by following these simple cyber hygiene steps. These steps would provide an added layer of confidence to your patients; knowing that your clinics have taken steps to ensure the safety of their information. ◆

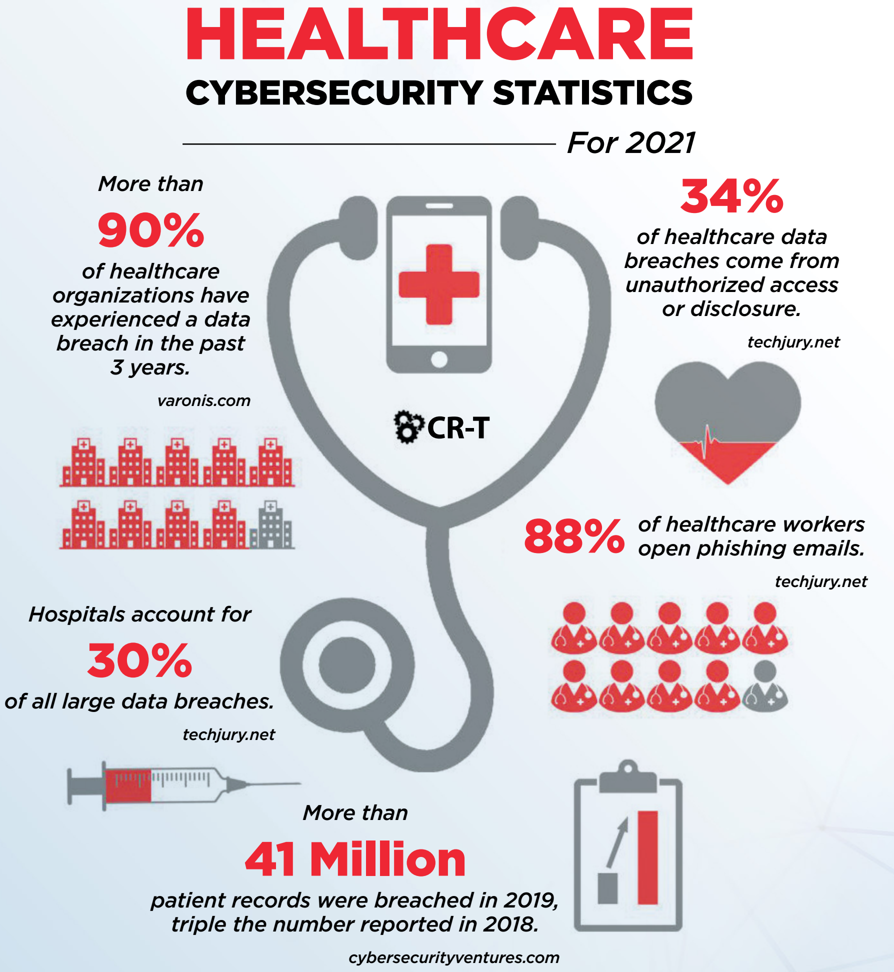
HEALTHCARE
CYBERSECURITY STATISTICS
For 2021
More than
90%
of healthcare organizations have experienced a data breach in the past 3 years.
varonis.com
34%
of healthcare data breaches come from unauthorized access or disclosure.
techjury.net
CR-T
88%
of healthcare workers open phishing emails.
techjury.net
Hospitals account for
30%
of all large data breaches.
techjury.net
More than
41 Million
patient records were breached in 2019, triple the number reported in 2018.
cybersecurityventures.com

Figure courtesy of cybersecurityventures.com