A Tale of Waiting and Suspense: The IT Woes of a Junior Doctor

Text by Dr David Yung

It is half-past six on a Monday morning, and a sleepy-eyed Jessica* pulls herself out of her GrabCar and makes her way up the elevator to the ward. Planting herself in front of a computer in the resident's room, she logs in and yawns while waiting for Windows to load her temporary profile, a five-to-ten-minute endeavour that feels longer than the Friday afternoon spine clinic. This new automatic logging-off of unused computers is a policy implemented nine months ago for cybersecurity purposes.

Digital disaster

In fact, the last five years have seen the IT landscape undergoing drastic changes. In 2018, an unfortunate and horrendous event occurred.[1] A user-related lapse in security resulted in the theft of 1.5 million patients' personal data, including a VVIP's. This apocalyptic catastrophe set off a chain reaction that has resulted in a knee-jerk response to create an air-gapped system[2] in which hospitals have their Internet access completely cut off.

Since then, life has not gone back to normal. Many new IT policy changes, particularly cybersecurity policies, have resulted in junior doctors having to adapt to the largely inconvenient new IT practices and at the same time, juggle their clinical and administrative duties.

Email protocols and privacy concerns

Jessica rests her head in her hand as she scrolls through Instagram, looking through UpdateMePRN's latest memes[3] and the social lives of her non-medical friends, frequently glancing up to see if Windows has finally readied itself for use so she may begin reviewing her 30-patient-long list. She used to spend the time checking her work email on her phone, but another new policy has seen the removal of remote access to Hmail, Integrated Health Information System's corporate email platform for the public healthcare sector. Now, she spends more time at work answering her emails, a new daily inconvenience.

This happened at the start of the year. The preceding months had seen a campaign to get healthcare staff to adopt management's new cybersecurity solution, MobileIron's Email+, a corporate mail app designed for data protection. This rather invasive app partitions a section of the hard drive on one's phone for mail storage, enables multi-factor authentication, and disables use of copy and paste.

However, what is not common knowledge is that Email+ is a mobile device management app[4] that grants the administrator the ability to remotely dictate the security settings of one's phone, lock the phone, stop you from using certain apps, and even wipe it. Most junior staff have reluctantly accepted this app on their personal phones, unwilling to be disconnected from email over the weekend in order not to miss out on important information like rostering. Others, like Jessica, have chosen not to opt into the app to maintain her privacy, as she has already given most of her life to her job.

She is not alone. Ironically, data from a MobileIron survey showed that more than 70% of people were uncomfortable with IT and employers seeing their personal emails, contacts, or other personal information.[5] And while, cybersecurity companies like MobileIron promise to uphold end-user privacy by separating personal data from work, this is all dependent on company policy, which is subject to constant change.

Furthermore, this creates a backdoor for future possible invasions of privacy. Bitglass, a rival company offering an agentless alternative, has done a study demonstrating that Mobile Data Management (MDM) apps are able to access personal email inboxes and even Amazon product searches on both iOS and Android operating systems.[6]

Ultimately, this is an issue of trust, even as the cybersecurity paradigm moves towards the concept of "Zero Trust"[7] in their apps, requiring perpetual authentication. However such systems also require trust on the employees' part that companies will protect their privacy. Unfortunately, recent times have made many juniors burnt out and feel that the establishment does not have their back.[8]

Intranet troubles

It does not help that the policy changes tend to be designed around the

experiences of office staff or seniors, who are given corporate laptops with remote access to the intranet. This allows them to check their emails from home. In comparison, the vast majority of junior doctors do not have corporate laptops or devices, save for certain residents in certain institutes.

This has resulted in many insensitive practices, such as when the human resources software changed from Unit 4's Prosoft to SAP SuccessFactors earlier this year. This came with an email that contained a hyperlink to activate one's SuccessFactors account. The catch? It required Internet access, and therefore could not be accessed from any hospital computers. Without remote access to Hmail, many forwarded the email to their personal emails in order to activate their accounts.

This has also happened in many other areas, such as with Medical Officer Posting Exercise applications, e-learning lessons, IT surveys, and New Innovations courses. Other areas of life have been affected as well. In order to upload presentations for various Continuing Medical Education activities, Jessica and many others must now use their personal emails to send the PowerPoint slides to their work emails, a feat that is not helped by the tiny file attachment size of 11mb, considering the large number of clinical pictures that one often requires. This defeats the purpose of air-gapping the system. Access to eDoc, an internal large file transfer system, or encrypted USB drives seem to be institution dependent and normally not granted to medical officers. All in all, Jessica has found herself staying back longer to complete her administrative tasks.

On top of this, Jessica often finds herself having to delete phishing emails sent to her by the IT arm of The Company, her own employer. These emails started at the height of the pandemic and have since increased in frequency. They are glaringly fake advertisements for discount packages on staycations or travels – a rather insensitive topic considering that burnt-out public-sector healthcare workers were prohibited from travelling for two years. Furthermore, the consequences of accidentally clicking these links are rather severe – mandatory e-learning modules requiring an hour to complete, threats of disciplinary action, and for "repeat offenders", a permanent mark in one's file. It has always seemed rather strange to Jessica that she only receives phishing emails from her employer. Just another one of life's mysteries.

Sometimes, while waiting for the IT department to answer her call to unlock her Hmail – having again forgotten the 16-character password with the ever-changing requirements that she has to change very three months – Jessica often wonders, what might be the cause of her technological woes? Technology was supposed to make life easier and more convenient, yet sometimes pen and paper notes seem like greener pastures.

Other approaches

Having spoken to her friend, a cybersecurity architect in the military defence industry, she was quite surprised to find out that there are more data-sensitive industries, like her friend's, with far less restrictive cybersecurity policies than the Ministry of Health. Furthermore, there are less invasive alternatives, such as secure mail apps that have their own encryption at rest, minimising the danger to data if a device is lost, and also run a cloud-like service, where data is only downloaded for the duration of use.

Moreover, what was most shocking was that a great deal of her woes were policy led rather than security issues that required resolution. According to an article written by IT security expert, Christopher Demicoli,[4] companies need not adopt the intrusive MDM policy; instead providing a company phone or laptop with the company's apps might be a solution that would make everybody happy. This is something that Jessica's friends in other industries seem to have.

It was amazing to her that despite being essentially contracted for five years as she slowly pays back her $870,000 bond,[9] she still felt like she was treated as temporary contract staff, only given an allowance of $30 for a mobile phone plan and having to use her own personal devices for work. She often found herself staring at the computer screen while waiting for rounds, wishing for her very own company phone. Perhaps, one day in the future.

Ah well, the computer finally loaded, and Jessica got cracking on, stumbling through the confusing new electronic medical record that she was introduced to since changing posting. The list was long, and there are many over-detailed notes to be copy-and-pasted for rounds, as well as vitals and overnight events to review. She could hear the *Ah Ma* wailing deliriously in the background. The long week ahead was in full swing. At least, her seniors were nice and patient. ◆

**Jessica is a fictitious junior doctor working in a restructured hospital.*

References

1. Tham I. Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack. The Straits Times [Internet]. 20 July 2018. Available at: https://bit.ly/3IDRhhU.

2. Wikipedia. Air gap (networking). Available at: https://bit.ly/3yKSboe. Accessed 15 July 2022.

3. Updatemeprn Instagram page. Available at: https://bit.ly/3IDX5b6. Accessed 15 July 2022.

4. Demicoli C. Never accept an MDM policy on your personal phone. Available at: https://bit.ly/3ciuNab. Accessed 15 July 2022.

5. Gruman G. How IT can spy on your iPhone or Android smartphone. In: InsiderPro Privacy. Available at: https://bit.ly/3Prc0rx. Accessed 15 July 2022.

6. Bitglass. MDMayhem: How MDM Software Exposes Personal Data [video file]. 2016 23 June [cited 2022 15 July]. Available from: https://bit.ly/3ARM7wQ.

7. Vaughan-Nichols SJ. Zero Trust: Protecting your company inside and out. In: InsiderPro Security. Available at: https://bit.ly/3PczbGa. Accessed 15 July 2022.

8. Er VM. Why senior doctors and healthcare administrators should follow doctor meme pages. In: TheHomeGround Asia. Available at: https://bit.ly/3aCcGvy. Accessed 15 July 2022.

9. Updatemeprn. The UMP guide to how much it costs to study Medicine in Singapore – using AY 2021/22 numbers [Internet]. Available at: https://bit.ly/3RARBSH.

Dr Yung is a medical officer and member of SMA's Doctors-In-Training committee. He is currently shuffling around Singapore's public hospitals. When not on call or waiting in line at the Residency queue, he can be found hunting for sushi or creating work on the Rugby pitch.