There may be troubles ahead

Healthcare

November 2016

In footballing terms, it was the archetypal game of two halves; with the pessimism and worries of the first half slowly replaced by the optimism and ambition of the second.

As 40 or so digital health innovators, technologists, security experts and senior executives gathered for KPMG's second event on innovation and information protection in digital health on 23 September, I don't think that any of us were under any illusions as to the scale of the challenge facing the digital health innovators.

If we were, those misconceptions were soon blown away by our opening presenters' talks on the burden of regulation, the difficulty of building trust with patients and carers and the growing threat of highly organised criminal groups.

Over the course of the day, I found fears for the future receding, thanks to the insights provided by the entrepreneurs already operating in this sector and a group-wide consensus on the need to incorporate security and privacy into the very foundations of the digital health business model. The days of tacking it on as an afterthought to the latest amazing idea are surely gone.

By the end, I felt several themes emerged. Firstly, there was the afore-mentioned requirement to build security and privacy in from the outset, making it a core part of every single digital health proposition.

Secondly, there was a point on trust. Securing consumers' trust will, I think, flow from being able to evidence the presence and effectiveness of security and privacy measures. The complicating factor here is that there may be differing perceptions in play as to how much privacy and security those consumers expect or require.

This neatly segued into the third theme of the prevailing data culture within digital health organisations. By this, I mean the respect which people show for the data which their organisation holds. Understanding what that data is, and isn't, how it can be used and how this affects customer trust is something which will require a cultural shift within many organisations.

Regardless of the mood in the room at any point in the day, I remained impressed and amazed by the innovation, dedication and passion being shown within this sector. There are elements of digital health which sound like pure science fiction yet they are now quickly becoming reality.

The benefits to the population are obvious. It's down to all of us to make these innovations secure to see them accepted into mainstream and so benefit people.

The lurker in the shadows

No-one likes to hear bad news so we tried to get this out of way early on, with my colleagues Mark Thompson and David Ferbrache talking about the threat which highly organised criminals pose to the digital health sector. You can read David's views on this topic at length here in this separate piece.

David believes that we should now be thinking of the cybercriminal as a business person in their own right. Persisting with the stereotypical image of the lone hacker in pursuit of solely disruptive, anarchistic aims stands in the way of us understanding how these criminals really operate

Like any entrepreneur, today's cybercriminal has a business model, a strategy and clear objectives. He or she knows what they want and why, they know how to monetise the assets they secure (your sensitive data) and they know where and how to secure the services for snatching those assets in the first place.

Identity theft, using the rich personal data sets which healthcare operators hold, is just one avenue open to them but extortion and ransom attacks are also becoming increasingly popular.

The threat which David and Mark talk about is very real. As a sector, we cannot bury our head in the sand and be oblivious to it. The problem here is funding. At a time when the NHS is struggling financially, every spare resource is being spent on survival. Looking for new, proactive ways of protecting data features some way down the list of priorities.

All of which opens up fears of a two-tier system of digital healthcare emerging; one where the latest innovations are only ever available to those who can afford them privately. Those who rely solely on the NHS for their healthcare provision may be left a long way behind. The most innovative – and most well-protected – digital healthcare applications will be out of their reach.

Thankfully, there are some straightforward (and cheap) steps which healthcare organisations can take to protect their valuable data assets. There's also a change of mindset required though. To begin to think of your cybercriminal opponent as you would a more traditional business competitor, is to think more clearly of his or her motivations. What do they want from you and how can you diminish the value of what they're after?

Thinking like a criminal is not something which comes easily to any of us – but thinking like a ruthless, competitive entrepreneur may be somewhat easier and would be the first step in shoring up our cyber defences.

Let the good times roll

From that starting point of fear and concern, the mood was then lifted by a series of presenters who wowed us with their stories from the frontline of digital health. There was Alistair Wickens who turned his Roadtohealth business model completely on its head, providing individual patient risk rankings directly to the general public rather than to insurers. And there was Shaun O'Hanlan of medical records supplier EMIS Health, talking of the importance of security and privacy and having to cope with the awful fall-out when something goes wrong in this area.

From Matthew Johnson of Guardtime, there were stories of the totally paperless Estonian healthcare system and the possibilities being offered up by blockchain security systems. Could they be the security answer we're all looking for?

And from Jonathan Hughes of Reinsurance Group of America (RGA), there was insight into insurers' use of data from wearable healthcare devices. Interestingly, this was where one of the first references to cultural change emerged. Insurers are well versed in the use of gigantic, structured data sets but making the most of unstructured data emerging from wearable devices and social media requires them to think and act rather differently.

We rounded off with Regius Professor Chris Toumazou and Dr Maria Karvela, co-founders of dnaNudge, telling us about the latest developments in genetic testing. We already know of the 23andMe product which allows individuals to map their DNA for evidence of medical conditions which they may be predisposed to. Chris and Maria talked of the development of their alternative application, dnaNudge, which allows users to test themselves and have the results underpin wellbeing advice on how best to manage any particular condition or even prevent it from manifesting. When you think that this advice could extend as far as your dietary and food purchasing habits, we really are seeing the worlds of preventative medicine and consumerism colliding.

Privacy is a core part of this proposition, allowing people to hold onto their personal data and only sharing it as they wish, rather than at the whim of the company doing the genetic mapping.

Sorry; computer says no....

Running throughout all these insights and anecdotes was the advice that security and privacy considerations be accommodated from the outset. It's a hackneyed old stereotype – the dashing innovators being stopped in their tracks by the miserable, unimaginative security enforcers – but it is rooted in reality.

It's somewhat unfair on the security experts though. I too would become rather cynical and more disposed to saying "no" if my concerns were only ever addressed right at the end of a project. As Professor Paul Dorey from Royal Holloway reminded us earlier in the day, security people are not there simply to rubber-stamp whatever the creatives want them to.

Properly incorporated from the earliest possible stage, security and privacy should be part of any digital health sales proposition and therefore a critical part of the marketing of any service or application. Being able to assure consumers that their data is in safe hands – and not used for subversive purposes – will go a long way to building much-needed trust.

As I alluded to previously though, this is not all about big, complex privacy processes or the latest security technology. This is also about the mindset of the people to whom that data is entrusted.

I've seen businesses where their security and privacy processes have to be absolutely leading edge in order to comply with industry regulation. Their biggest vulnerability lies not with those processes failing but with people short-circuiting them, not affording the data the respect it deserves and potentially damaging customers' trust, maybe even irreparably, along the way.

For that reason, I expect to see far more healthcare organisations indulging in people and cultural change programmes in the coming years as they prepare themselves for a more digital existence.

I have no doubt that digital healthcare is going to become a mainstream commercial reality. There is too much technology available and too many interested parties converging on it (healthcare, pharmaceuticals and insurers) for it to be abandoned as a passing fad. The excitable vibe in the room at our event only served to reinforce my conviction on this point.

I haven't been able to mention all our excellent presenters in the course of this summary but I would like to thank every one of them for providing both insight and inspiration during the day. These truly are exciting times.

Caroline Rivett
Director
Information Protection in
Life Sciences & Health
KPMG in the UK

Share your views and join the debate:

Visit us
kpmg.com/uk/healthcare

Email us
publicsectormarketing@kpmg.co.uk

Engage with us
Follow us on Twitter **@KPMGUK**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. The views and opinions expressed herein are those of the interviewees and survey respondents and do not necessarily represent the views and opinions of KPMG LLP.

CRT071395 | November 2016