Collective Intelligence

Healthcare Is Disproportionately Susceptible to Extortion

By **Paddy McGuinness**

Brunswick Healthcare & Life Sciences

Brunswick Cybersecurity & Data Privacy

Brunswick Technology, Media & Telecoms

August 22, 2022

BRUNSWICK

Healthcare Is Disproportoinately Susceptible to Extortion

Few doubt that managing down technology risks is critical to the development of effective and efficient healthcare. The aggregation and analysis of data is central to almost every new and prospective breakthrough in the sector: vital to developing personalised treatments; for faster and more accurate diagnoses; and for managing the greatest challenges such as pandemics and antimicrobial resistance. There is then the explosion in virtual consultations during the COVID-19 pandemic, and the need to make up for a backlog in diagnosis and treatment.

Medicine delivered through the internet is now central to healthcare plans in many countries. But these only work if there is trust. Patients must consent to be diagnosed and even treated virtually, which will only happen if they are confident that professionals are practicing good healthcare. At the same time, clinicians must trust the delivery technologies and accept that the ergonomy, efficiency and additional features make up for the loss of face-to-face interaction. Most importantly, all involved must trust in the integrity of the underlying data sets – something that presents a fundamental challenge given the innate vulnerability of healthcare systems to bad actors.

Unfortunately, networked systems in the healthcare sector are generally not well placed to win trust. A complex array of different technologies and many legacy systems make IT a headache in most hospitals and clinics. Outmoded IT infrastructure, excessive costs for any adjustments to an application and stovepiped systems that hamper data sharing result in a chronically old-fashioned user experience that holds healthcare back.

Consumers have been quick to embrace and trust technologies in other parts of their lives. For example, 87% of British households do some shopping online while 76% use online banking. The contrast between those data-enabled user experiences and the clunky nature of healthcare systems militates against trust and consent. This obstructs the aggregation and use of data that should be enabling life-saving treatment and research.

Cloud-native solutions may be being pulled through, but far too slowly. In the UK there have been missteps such as the promised General Practice Data for Research and Planning scheme that was meant to start in 2021 but has been delayed by concerns about data protection and a reported failure to communicate clearly enough about how the data would be used. Amazingly for the 21st century most of the opt-out processes were to be done in hard copy and sent to local surgeries. The contrast with other online services could hardly be greater.

Worryingly, against this background, the threat of data loss and system disruption has gone up markedly. 2020 saw an unprecedented increase in recorded cyber attacks (a subset of the true total because most are not reported). A concerted effort brought the number down in 2021 but levels remained significantly higher than in the pre-pandemic period. The cyber incidents affecting healthcare which I dealt with when in British Government service, such as Dridex malware seeking banking credentials or WannaCry pretending to be ransomware, were not actually targeted at healthcare. Those I deal with now as part of Brunswick's team are specifically targeted at the sector and ruthlessly exploit vulnerabilities whether generic, such as Log4j, or specific to healthcare equipment.

Yes, the pandemic has sensitised criminals to the potential value in the healthcare sector, and, yes, improvement in the cyber resilience of the finance sector has had the Darwinian effect of driving groups to look for other prey. However, there is something more fundamental at play here: healthcare is simply more susceptible to extortion. We see ransomware groups searching networks to find the most impactful

data to encrypt or steal. Disabling oncology servers gives them maximum leverage, so too does threatening to publicise gynaecological or reproductive medical data if payment is not made.

How then to harden healthcare against extortion? There are, of course, strong technical aspects to what needs to happen, and regulators and national technical authorities regularly publish advice in most jurisdictions. The organisational and communications response is not as well understood. It is lacking in the maturity models used by audit and risk committees and too often absent in the lived practice within hospitals, clinics and labs. For wider business continuity purposes, healthcare institutions have a strong contingency planning culture and are hard minded during crisis response.

The most successful institutions have a "when not if" approach to preparedness and are well-organised and practiced about their crisis decision making, their external partnerships, and how they will engage internally and externally when attacked, including in the face of extortion. Those that do not have such plans in place need to catch up – and fast.

To continue the conversation:

Paddy McGuinness CMG OBE is a Senior Adviser at Brunswick Group and former UK Deputy National Security Adviser for security and resilience where he oversaw the response to multiple attacks on UK healthcare. He now supports clients globally when they are attacked. He is co-founder of Oxford Digital Health (OXDH).

