BMJ 2017;357:j2390 doi: 10.1136/bmj.j2390 (Published 2017 May 18)

EDITOR'S CHOICE

Beware of geeks bearing gifts

Kamran Abbasi *executive editor*

The BMJ

The NHS is in crisis. That much we knew. That the latest crisis (doi:10.1136/bmj.j2357) was caused by a failure of cyber-security is an unexpected twist in the organisation's struggle against chronic underfunding. WannaCrypt or WannaCry, a Trojan malware or ransomware, disables computer systems by stealing and encrypting data and locking out users. On payment of a ransom in the crypto-currency of bitcoin, your data will be returned to you and your computer unlocked. The ransomware hides in a seductive email and hijacks your computer when you open it. In this era of cyber-threats, beware of geeks bearing gifts.

The attack isn't a surprise in itself. Cyber-attacks on healthcare organisations are common enough, with many recent examples in the UK and US (doi:10.1136/bmj.j2214). Indeed, the UK government has claimed an investment in NHS cyber-security of £1.9bn (€2.2bn; $2.5bn). But the scale of the damage to the NHS, with some 50 trusts affected, casts doubt on whether that money was properly used.

Our editorialists Guy Martin and colleagues argue that the government's approach was akin to a ticking time bomb and that ignoring cyber-security has prolonged the time that the NHS was at risk (doi:10.1136/bmj.j2375). In 2015 the government ended a £5.5m support contract with Microsoft for its vulnerable Windows XP operating system (doi:10.1136/bmj.j2395). Though NHS Digital claims that only 5% of NHS organisations are running older operating systems such as Windows XP, a December 2016 report by the software company Citrix estimated that Windows XP machines were running in 90% of hospitals. NHS organisations spend less on IT than other critical sectors, and only a small proportion is spent on security.

The next problem was that the risk wasn't sufficiently managed. Trusts were advised to upgrade systems and told that support for Windows XP would cease, but there was "no clear accountability at a national level for managing what is self evidently a national problem," say Martin and colleagues. This lack of governance means that responsibility for cyber-security is now an exercise in passing the buck. The result, state our editorialists, is an unprecedented disruption of clinical care that compromises patient safety and erodes public confidence in electronic health records. More attacks are inevitable, but a national inquiry might be needed before adequate funding or governance is in place (doi:10.1136/bmj.j2395).

Solving a cyber-security crisis is outside the remit of almost all clinicians, yet the grief reaction is something we all contend with in our personal and professional lives. This week's Practice Pointer explains that "the concept of stages of grief occurring in a specific order is a popular, yet inadequate representation of what grieving people go through" (doi:10.1136/bmj.j2016). The challenge is to identify patients with disturbed grief and decide on the best management approach. A powerful complementary article by Rosamund Snow (doi:10.1136/bmj.j2012), *The BMJ*'s late patient editor (doi:10.1136/bmj.j850), describes the bereavement she experienced after a spirit crushing diagnosis of type 1 diabetes.

kabbasi@bmj.com