What can healthcare orgs do to prepare for a cyber attack?

Paul Charnley, digital lead, Cheshire and Merseyside Health and Care Partnership, speaks to IT Pro 20/20

As we've seen in the past few months, cyber attacks are unfortunately on the rise in every industry and public service sector, and no organisation is immune to the threat. It's unsettling that even several years after WannaCry, a ransomware attack on Ireland's health system led to computers being down for at least a week. The result of this was operations being cancelled, patient records blocked, cancer treatment delayed, and other services compromised – all against the backdrop of the pressures of COVID-19.

For any company or organisation that's hit by a cyber security issue, whether the criminals' intent is malicious reputational damage or to gain a financial pay-off, there is a disruptive outcome. But when the target is a national healthcare service, it affects the lives and health of millions of people, with potentially fatal results.

Cheshire and Merseyside Health and Care Partnership is an integrated care system (ICS), covering an area of nine councils in the North West, with 31 NHS organisations including 13 hospitals and nearly 400 GP practices. In short, we are a complex partnership.

We set up a cyber workstream after the WannaCry ransomware attack a few years ago, and one of the things we wanted to do was to run an in-person cyber security planning scenario. But when the pandemic began that event was put on hold and instead we pivoted to an online exercise.

Although each NHS trust in the partnership has its own policies and procedures for incident response – covering issues such as problems at a nearby petrochemical plant, civil unrest, or a major crash on the motor-

Training scenarios that demonstrate the dangers of phishing are particularly useful for preventing cyber atttacks

way – we knew we needed to test how we could work together to respond to a potential cyber attack in a unified way.

A cyber breach can affect a large geographic area very quickly and so a speedy coordinated response is vital. Using guidelines from the NHS' emergency preparedness, resilience and response (EPRR) framework and working with specialists in cyber security from Gemserv, we ran a scenario to test how we would respond to a number of different actions. And in fact to make it more realistic, the scenario included several elements that none of us knew were coming.

It began with the premise that a clip had been shown on breakfast news apparently showing local NHS leaders criticising a COVID-19 vaccine; we were being bombarded with calls from the press and the central health comms teams; the vaccine maker's share price dropped 10%; and we had to figure out if the video was real and who created it.

With new problems added intermittently, we ran the gamut of contending with damage limitation, finding the source of the video leak, and tackling a malicious attack. Over the course of the simulation, we discovered that one of our executives had been spear phished and the video was a deep fake, but the spear phishing would have meant we were also potentially vulnerable to a ransomware attack.

It was a really helpful and salutary exercise to pinpoint things we need to be aware of, and the realism of the event made it all the more engaging. Although it was a simulated situation the adrenaline was flowing, and that heightened sense of urgency really helped us focus and take on board what we needed to do.

We've since developed a partnership-wide incident response plan so we know how to prepare, and how to communicate quickly and effectively so we can mitigate any issues. We learned that having clarity on who does what, and what the chain of command is – both up and down the NHS hierarchy – is critical.

Having outside help on this was certainly important. Getting experts on board to steer the scenario who have expertise in carrying out cyber security arrangements across many different industries meant that they were able to throw curveballs at us that we might not have anticipated. It was a sobering experience, but well worth doing.

At Cheshire and Merseyside, we'll now be running these sorts of scenario planning events on a regular basis. It's not enough to do it once; cyber criminals will keep finding new ways to target organisations, so we'll need to keep testing our responses so we can be as prepared as possible for any attack.

Of course, you can never tell what will be round the corner, but I think that every integrated care system should run these sorts of scenarios as training exercises. And neighbouring ICSs should think of how they can work together, to plan and prepare, and to form a joint response to reduce the impact of a breach.

There also other practical and legislative aspects to consider. The government wants shared care records in place this autumn; and from next year, ICSs will have statutory powers. The upshot is that ICSs will not only need to address any technological issues, but will need to configure an organisational governance response to a cyber attack. With structured policies and procedures in place, we should all be stronger and more resilient. ■