NHS cyber security: Scale, cloud and supply chain

Bolstering cyber defences for health and care is a priority, according to the government's latest strategy on the subject. Sectra's Chris Scarisbrick gives his views on some immediate priorities that could make a big difference, without placing undue burden on NHS teams.

Cyber security in healthcare means keeping patients safe. That's the message from Lord Markham, in his foreword to the government's 2023 strategy for cyber resilience in health and care.

With media reports of crucial healthcare services being halted by cyber-attacks, continually mounting threats from around the world, and recently publicised concerns from government ministers around the security of national infrastructure, the importance of boosting cyber readiness is something few would dispute.

The life and death importance of the services provided, and of the sensitivity of data held, mean that healthcare has become prime target for nefarious actors.

The health and care sector also faces relatively unique complexities that need careful consideration. For example, the new strategy details the potential for "cascading risk". Every point of a full range interdependent and inter-linked health and care services need to be secure for the progression of the patient pathway. For example, if you can't get your scan, or your diagnosis, because of a cyber-attack, you might find further delays in receiving what could be time-critical care.

As the strategy states, some 137,000 imaging events are recorded in the NHS every day. Downtime of just 24-hours to these services could have significant knock-on effects at a time when demand is soaring, workforce challenges are prevalent and healthcare providers are trying to tackle an elective backlog of millions of patients.

So where to begin in addressing the risks faced?

With such importance now placed on reinforcing resilience, the strategy sets out five pillars that cover everything from identifying and responding to the greatest risks, to people and culture, through to response and recovery capabilities, and more.

It is a lot to consider for health and care services that are already under the most pressure they have ever faced, and undoubtedly a lot of work will need to be done by people working within our healthcare services.

But for me, there are three key areas that could deliver significant gains now, without placing additional burden on health and care providers.

Making use of scale

Reassuring is the clarity of responsibility that the strategy begins to establish for several key parties. Logic would suggest further clarity should emerge in the follow-on implementation plan coming later in 2023. But already, the specific role of integrated care systems, for example, is detailed against various priorities.

Focussing on ICS requirements sends a positive message and reinforces one of the strategy's pillars – that health and care must look to harness its scale in order to "defend as one". ICSs are being given a mandate to procure systems at scale, and to strategise at scale. Cyber is being baked into the culture and accountability at regional level, as well as national.

This is not without precedent. One area where cyber security is already being applied at scale within the NHS, is within diagnostics. Imaging networks and pathology networks are procuring digital imaging solutions across large geographies, accountable for the delivery of care for millions of patients. ICSs might look to those networks for learnings. Though these procurements are not for cyber security systems as such, in my experience resilience benefits are emerging from scale of deployments.

Not harnessed well, and scale could pose problems – the bigger you are, in theory the more surfaces you expose to ingress from cyber-attacks. But consolidation and convergence of systems across a region or an ICS into single infrastructures, can enable focussing of resource into better protecting that infrastructure, rather than trying to protect multiple surfaces and potential doorways for malware. In the case of regional diagnostic procurements, many draw on public cloud infrastructures to realise the security benefits of scale. And that brings me to my second point.

Cloud resilience

Cloud, deployed appropriately, offers huge potential to create more secure environments. Surprisingly this isn't given attention in the recent strategy, but health and care organisations could draw on public cloud providers to leverage their resources. Such companies employ the world's leading cyber security specialists. And they continue to invest huge amounts to stay in the race against cyber criminals. If we think about making the most of scale, gaining access to this could be an immediate win to augment in-demand cyber expertise in the health service.

New features that continue to be developed by cloud providers could improve resilience. For example, immutable storage could be a defence against ransomware. This is data, written to disk, that is protected and cannot be over-written, changed, or deleted. And that could be instantly built into a strategy. If ransomware hits, the data held in an immutable store cannot be encrypted, and can be retrieved, supporting the new strategy's vision for health and care organisations to be able to quickly recover from attacks.

Supply chain – suppliers must act

The potential for cascading risk goes beyond health and care providers. The strategy rightly spells out that supply chain risks must also be managed. This goes beyond direct contractors too, with suppliers' own supply chains posing potential vulnerabilities.

Positively the strategy calls on health and care procurement teams to play a role in addressing these risks.

Again, this reflects what we are starting to see in large scale diagnostic technology contracts. In some cases, these contracts have started to call not only for prime contractors to comply with standards including ISO27001, and Cyber Essentials Plus, but for all key subcontractors to also conform.

Alarmingly, it appears that not all major players in the health tech industry have this compliance. This is something that health and care organisations should feel very comfortable demanding from every supplier, and to refuse to award contracts to those that don't. Suppliers and their supply chains should not be the weak link in the cyber security chain.

Part of the strategy's vision is for trust in digital systems to be increased so that innovations can then then be applied with confidence. Technologies like AI continue to emerge and their compliance as part of this is key. One recent contract specified that if 1,000 patients were dealt with by a piece of technology within the space of a contract, then the provider would be considered a key sub-contractor. But arguably all sub-contractors connecting into systems on the NHS network could be a vector for malware or other attacks.

Good cyber hygiene and compliance with at least a minimum standard of cyber resilience, should therefore be something all suppliers are willing to demonstrate.

Action on this area is important. Although emerging in more recent procurements, it has not yet become a consistent requirement. This could be enforced quickly and upfront to harden security of systems in healthcare, with very little work from those in an NHS already under pressure.