LOCKING UP

Cyber security is a growing issue for the NHS as it moves to electronic systems. But how big is the threat and how can NHS organisations protect their data? Seamus Ward reports

SHUTTERSTOCK

The words 'cyber crime' conjure up the Hollywood image of a hacker, a hooded figure in a darkened room up to no good, whether the motivation is mischief, malice or money. Governments and corporations, even individuals such as US presidential candidate Hillary Clinton, have been targeted. But what of the NHS? After all, in the private sector, an entity with a £100bn plus turnover and a mass of sensitive, business-critical information would be a prime target.

It's an issue that would be easy to sensationalise, though IT and security professionals believe it's a case of when, not if, an NHS organisation is hit by a serious cyber attack. While the NHS does not appear to have been directly targeted, and there are no official figures, a number of Scottish health boards and at least one English trust have been hit. Given the sensitivity of the subject it is not surprising that trusts do not wish to speak openly about cyber security, though many recognise it is an area where they could improve.

There is growing concern from national bodies. The report on data security, consent and opt-outs from Dame Fiona Caldicott in July recommended all NHS organisations provide evidence that they are taking action to improve cyber security. While the greatest danger was from staff – through carelessness or lack of proper systems – the report acknowledged the threat from outside the NHS, particularly from basic cyber attacks such as malware in emails, was growing. The Care Quality Commission says it will amend its assessment to ensure the Caldicott recommendations are being met.

A spokesperson for NHS Digital (formerly the Health and Social Care Information Centre, HSCIC) says all organisations, including in the NHS, face an ongoing and increasing risk from cyber-security attacks. And while each NHS body is responsible for its security, the HSCIC this year set up the CareCERT programme to help protect NHS bodies.

'CareCERT has not been set up in response to a particular threat, but in recognition of the fact that risks from cyber attacks are ongoing and ever changing and health and social care information should be protected with the highest possible standards of security,' says the spokesperson. 'Our role is to support individual health and care organisations, who are responsible for the data they hold, to best protect that information and to ensure their own cyber-preparedness. We want to empower organisations to be accountable for cyber security locally, but to support and enable them to improve and enhance what they do.'

The programme includes CareCERT Broadcast, which sends alerts to more than 10,000 health and care professionals responsible for IT, security, networking and information governance. These alerts provide real-time advice on cyber security threats, along with guidance for recommended proactive or remedial actions.

NHS Digital is also testing a national e-learning system that will train all staff on fundamental data security alongside more complex modules for specialists. It will be available to all health and care organisations.

Gary Colman, head of IT audit and assurance services at the West Midlands Ambulance Service NHS Foundation Trust, says the risk of cyber attack is real, though UK NHS trusts have yet to be targeted by serious criminals. 'You're more likely to be caught out as collateral damage – if someone is after a person or organisation and your website is hosted on the same server, for example.'

Common terms

Malware A general name for malicious software, often contained in emails with bogus links to websites or documents. The software is often sold on the internet by developers for others to use. Malware can allow users to take over a computer, encrypt its data or glean information, such as passwords.

Ransomware An app that can lock down or encrypt a computer system, with the criminal demanding a ransom for its release.

Patches Updates from software developers that prevent hackers using vulnerabilities in a programme or app to gain access to a system or network.

A dedicated unit at the ambulance trust provides information security and assurance services to NHS organisations, local and national government and the private sector (manufacturing and healthcare).

'I haven't heard of any significant successful cyber attacks against the NHS, but I think it's just a matter of time,' he says. 'If you consider the amount of money that's going through the NHS – a criminal who hacks into an NHS network could target the payment systems. That's a fair incentive for a cyber criminal.

'If you hack a trust's website, you can change the website and attack anyone that uses it. It can be a staging point to a further breach in the organisation or to patients.'

US healthcare organisations are a major target of cyber criminals and a number have been the subject of ransomware attacks. Mr Colman says this is mostly because they deal with financial information. However, UK patient and staff records contain information such as NHS and national insurance numbers – data that security experts say is potentially way more valuable to those bent on identity theft, for example.

Mr Colman adds that healthcare organisations should take the same care with staff records that contain identifiable information as they do with patient records. 'Both should be treated as highly confidential. If you can get a foothold, a breach in the NHS network, as a cyber criminal you would look to widen that access and take advantage of its payment system.'

Peter Sheppard, senior ICT audit manager and cyber security lead at business assurance services provider TIAA, has been helping NHS clients with cyber security for 14 years. He believes the health service could step up its game. 'It's a real and credible threat, but that doesn't mean we should all panic,' he says.

Boards must acknowledge the threat, he says. 'Some NHS organisations do not have cyber security in the corporate-level risk register. This is deeply concerning as an attack could damage critical systems or make patient records unavailable. We have to be mindful that the potential impact of this type of risk is quite high and could have a detrimental effect on patient care.'

Mr Sheppard highlights much of the risk lies in legacy systems, which can be exploited more readily than modern ones, as the manufacturer may no longer be producing patches updating their security.

Replacing systems

The bad news for finance directors facing a funding squeeze is that the only way to reduce the risk is to replace outdated systems. Indeed, Caldicott and the CQC recommend outdated and unsupported systems are replaced 'as a matter of urgency'. Where new deployments are made, Mr Sheppard adds, security must be designed into the fabric of any new system, not delivered as a bolt-on. 'It is imperative that systems are secure by design when deployed, not as an afterthought.'

NHS bodies should be aware of the risks, particularly for breaches of patient-sensitive information, when decommissioning hard drives and other storage devices. Mr Sheppard is aware of one incident with which TIAA was asked to help, when disks containing NHS data were stolen from a company subcontracted to destroy them.

Mr Colman says there is no single solution to prevent cyber attacks, but basic steps can be taken, such as having an up-to-date IT governance framework that is implemented and regularly reviewed.

'People introduce new systems or devices without realising they can open up a new vulnerability,' he says. 'Patching and updates to systems must also be done – the amount of unsupported systems we see is scary. The situation has improved over the past couple of years, but there are unpatched systems out there.

'User awareness is a massive deal. Staff take information governance toolkit training, which has some element of cyber security, but there is room for improvement. When people are back at work they do not always scrutinise email addresses or websites.'

In at least one of the US cases of ransomware attacks, the healthcare body refused to pay and was able to restore its data from a back-up. Mr Colman says this is the ideal solution, but not always foolproof.

'You may have a back-up, but if the back-up is online and attached to the network, it too could be encrypted. For this reason, you need an offline back-up. I am aware of three trusts that have been hit by ransomware, but basic controls in place limited the impact to a few wards or departments. In each case, the infection was in an email attachment.'

Sophisticated scams

It's often not simply the case of a member of staff clicking on a link or attachment in an email written in poor English. Some scams are more sophisticated. A cyber criminal could send the email from an account that looks like the chief executive's – the address could say @nhs.co.uk rather than @nhs.net, for example. While such emails could be used to deliver malware, they are often vectors for one of the oldest criminal scams – impersonation. The 'chief executive' could attach an expenses claim form, for example.

'I am aware of some instances of pretty large payments that have almost been made but picked up at the last moment,' Mr Colman says.

Educating users and limiting high-level access to NHS networks are vital, Mr Sheppard says. 'Staff may not be tech-savvy, so they will not be aware they are doing something risky or wrong.'

He is aware of one non-NHS organisation that, like many employers, including some in the health service, allowed staff during breaks to access the internet using their network. A staff member viewing personal email clicked on a bogus link, and, within minutes, their employer's server was encrypted by malware.

Moves to give patients and the public wifi access in hospitals poses a threat if strong barriers between hospital and public networks are not put in place, Mr Sheppard says. 'One of the biggest threats to our cyber security is ourselves. We are the weakest element, but we need to think about cyber security holistically, not just in terms of firewalls. It's not about stopping people getting on with their digital lives, but the NHS needs to think about it sensibly, particularly when most people now have smartphones for their email.'

While the traditional method of gaining assurance about network security, by undertaking 'penetration' testing (paying an outside body to try to hack your system) – is helpful, Mr Sheppard insists it shows the vulnerability or strength of a system only on the day the test is done. New exploits or weaknesses will be found subsequently, so it cannot be done and forgotten.

Other practical IT solutions are useful. Simple logging and monitoring of who is accessing the network can aid security, but is not always performed in NHS organisations, he says. Implementing data loss prevention software can also help detect actual and attempted breaches before they cause serious damage.

There is no single solution to NHS cyber security, but it must start with staff being more aware of the dangers.

"A criminal who hacks into an NHS network could target the payment systems. That's a fair incentive for a cyber criminal"
Gary Colman, West Midlands Ambulance