360 ASSURANCE

BRIEFING PAPER

Assurance with Vision

Cyber Security in the NHS

You will be aware of regular news stories of organisations that have been subject to cyber attacks. The number of attacks, and sophistication of those attacks, are increasing at an alarming rate.

In this paper we set out some issues for you to consider, as part of your ongoing evaluation and assessment of your cyber security arrangements.

Are you the weakest link?

In most cases staff are still the weakest link in an organisation's cyber-arrangements. Humans are vulnerable and unpredictable – you might spend considerable time and money configuring your networks to be as secure as possible, only for efforts to be undermined by a member of staff disclosing a password, leaving a computer logged on or clicking a malicious link.

Weaknesses are not just confined to staff being 'actively targeted' – information and security can be compromised through a simple lack of awareness, for example:

- Have you ever visited a GP and they left their smartcard in the computer and screen logged on when they popped out to get some equipment?
- Have you ever heard clinicians in a lift discussing a patient they are treating?
- Do you recall senior members of government embarrassed by having sensitive documents photographed because they were carrying them in view?

Points to consider: how do you raise awareness with staff of cyber issues? How do you assess whether staff understood the issues, and how frequently (and recently) have you reassessed their understanding?

Once on induction is not enough!

360 ASSURANCE

360 Assurance has a clear vision for the delivery of audit and assurance solutions. Our approach is one of Partnership and Collaboration. We work in partnership with you to provide a cost effective, quality driven service that helps you deliver your key priorities.

In this paper:

Points for Consideration

- Is Information Security and Information Governance considered throughout a project, or bolted on at the end?
- Don't assume systems and data are safe just because they are on N3.

Don't get carried away!

Technology is wonderful – we might all wonder how we got by without a smart phone and the internet. And developments in portable technology and information sharing certainly have the potential to contribute towards efficient and effective patient care. But almost every development introduces a potential information security or governance risk.

It is important that these are recognised, assessed and mitigated as new technology develops – not when a new system is ready to be deployed. There is a risk that some people get carried away with the exciting potential that a new system or technology will bring to their role, and so the do not think about the associated risks.

Points to consider: are your Information Security and Governance staff aware of projects within your organisation and engaged *throughout* the development. Do these staff actually have the capacity to be involved?

Who do you trust?

People often refer to N3 being a secure network. It's worth remembering that it is not necessarily a *secure* network – it's a *private* network. Systems and communications on N3 are much safer than systems and communications on a public-facing network, but there are over a million users and thousands of organisations connected to N3.

Points to consider: have you assumed that N3 is inherently safe, or have you acknowledged that there remains a level of risk from others that have access to this network?

Are you being hacked?

Are you currently being hacked – and if so, how would you know? It is common misconception that if you are hacked you will know about it! You might expect your machine to lock up; you'll receive a ransom -demand; or pink elephants will start to dance on your desktop. But in many instances hackers want to steal data. They might already have access to your network and have downloaded your data, or they might be content to simply sit on the network and watch. Imagine if the information displayed on your screen was being captured and relayed to a hacker, or if they were capturing every keystroke you made. (See below the next section for the points to consider).

Points for Consideration

- No organisation can guarantee that it hasn't been, isn't being and won't be attacked. Is a "no news is good news" approach sufficient?
- Have you received any penetration testing – if so when, and are the limitations of the assurance received recognised?

How hard are you looking?

One of the sessions at the recent *CyberUK* event was led by Cisco, discussing the evolution of security on their systems in response to attacks. This session focused on hardware, but the underlying principles are more generic – the point that they made was *you need to look* for evidence of hacking, and you need to look hard! It isn't enough to have security software in place and to rely on it alerting you to problems. Staff need to be routinely checking logs for evidence of unusual activity. This takes time, which requires resource, which requires money.

Points to consider: do you actively look for evidence of hacking or reconnaissance? Monitoring by exception is not enough. Are you clear who is responsible for monitoring your security posture, and do they have the tools, skills and capacity to perform this role proactively?

Feeling assured?

Those responsible for cyber-security (at an operational level and strategic level) can take assurance from the activities in place to prevent, detect and react to incidents. This includes the ongoing protection that is in place, and specific activities such as penetration testing. One point to note is that penetration testing provides a level of assurance on the day that it is carried out. Assurance is very much time limited, because a new vulnerability or new hack might emerge the very next day.

Penetration testing assesses the system configuration at time of testing. It is almost certain that a new patch or upgrade will be issued for one of your systems following the penetration testing. If you don't apply the patch, you might be potentially insecure. However if you apply the patch and don't repeat the penetration testing, you can no longer take assurance from the penetration testing because it took place on a different configuration.

Points to consider: how frequently do you undertake penetration testing, and what has changed since you were last tested that might impact on the assurance you received at that point.

Points for consideration

- All organisations are at risk from hacking. When your organisation is hacked, what do you plan to do about it to minimise disruption during the attack, and to recover after the attack? How readily can a website be recovered, or systems restored following a ransomware attack?
- Does your approach to security take human behavior into account? Have you consulted staff to assess their views regarding the security and usability of the system?

Hackers - how would you react?

If you are hacked, it is important that you plan how you intend to react during the incident, to safeguard your systems and data, but also to minimise disruption. Your response should be appropriate and proportionate to the nature of incident.

It is also important to return to normality as soon as possible. As with any business continuity arrangements, you should have plans in place that are documented, rehearsed and understood. In the event of an attack, this will help you to minimise disruption and to restore systems and services promptly

Points to consider: Do not think that you can prevent hacking. If you haven't been hacked already it is almost certain that you will suffer a hacking attempt at some point in the future. When this happens, do you have plans that define how you will react, do they define appropriate responses to different levels of attack, and do you also have clear plans for how you will recover following an attack?

We're so secure, we're insecure?

And finally, a point about human behaviours. When designing security arrangements, they may be technically perfect, but if they become so secure that they are time-consuming to work within, staff will work around them. If passwords are too complicated and required to be changed too frequently, staff will write them down. If systems take too long to log off and on again, staff will leave them logged on. Imagine a security scale of 1-10, with 1 being no security and 10 being perfectly secure. A purist might aim for security at level 10, but at some point in the scale human nature kicks in and people start to look for workarounds.

Points to consider: Have your systems been designed to balance security with usability? Do you engage with staff to assess their views of the system, and have you designed something so secure that you are encouraging staff to seek workarounds?

Glossary of Terms

Network - 2 or more interconnected systems, across which information is transferred.

N3 - A large private network, utilized by the majority of NHS organisations in England and Wales.

Hacking - Gaining unauthorized access to a system or network, usually for illicit purposes (e.g. accessing sensitive information, preventing normal usage, blackmail)

Penetration testing - A controlled attack on a system or network which can identify potential security weaknesses.

Security Patch - A software update provided to fix an identified vulnerability.

Assurance with Vision

Contact Us

Call for more information about our services.

0116 225 6114

Visit us on the web at www.360assurance.co.uk

360 Assurance:
Riverside House
Bridge Park Road
Thurmaston
Leicester
LE4 8BL

360 Assurance:
Stapleford Care Centre
Church Street
Stapleford
Nottingham
NG9 8DB

360 Assurance:
Oak House
Moorhead Way
Bramley
Rotherham
S66 1YY

Key Contacts

Annette Tudor, Deputy Director	0116 225 6124
Simon Gascoigne, Deputy Director	0115 883 5305
Leanne Hawkes, Deputy Director	01709 428713