Cyber Awareness for Managers

12 - 14 May 2026

Poll results

Table of contents

Cyber Awareness for Managers - Welcome (1/2)

0 0 4

What's the biggest cyber security challenge you have within your organisation?

(1/2)

- In our surgery our biggest incidents tend to be human error, cyber security is something we are learning about more recently. However the NHS as a whole have had cyber threats. Our biggest issue is human error with cyber security and data protection
- Managing a remote team Instilling the wider impact a lack of cyber security keeping up with advancements Small team but with multiple partner businesses, managing / guiding these external companies Understanding what needs to be in place for correct data storage
- We do a lot of work with MoJ and MoD so need to make sure our documents and information is secure at all times so this training is more preventative
- I am coming from a university, so for us, one

Open text poll

Cyber Awareness for Managers - Welcome (1/2)

0 0 4

What's the biggest cyber security challenge you have within your organisation?

(2/2)

big issue is the integrity and the

biased information.

Cyber Awareness for Managers - Welcome (2/2)

004

What Cyber Incidents & Near Misses have you had in your organisation and personally?

- In our surgery our biggest incidents tend to be human error, cyber security is something we are learning about more recently. However the NHS as a whole have had cyber threats. Our biggest issue is human error with cyber security and data protection
- Staff being contacted by scammers, purchasing vouchers Links being sent in PDFs Scams becoming more convincing
- One of our team clicked a link, put their password in and there was an email breech - luckily one of our clients spotted it but we had to do a lot of work quickly to get it under control
- Incident about the student privacy and research data circulation.

Evaluate Current Cyber Controls (1/3)

006

How do Cybersecurity controls HINDER your work?

- blocking non-approved tools restricting access to cloud platforms Delays in accessing digital resources during lectures
- Computer restarts, software updates breaking things, slower login.
- it can take time to access some portals. some staff have issues and need assistance from IT which takes time. Not always popular with staff if they are not the best at IT.
- Sometimes difficult to access / forgotten passwords / unsure where passwords are stored New mobiles - have struggled to re-install apps with 2FA because the 2FA is on the old device Lack of knowledge, sometimes don't know you're doing something that could expose the company to risk
- I don't think they do once you get used to them
- Can make access frustrating.

Evaluate Current Cyber Controls (2/3)

006

How do Cybersecurity controls HELP your work?

- research data isn’t stolen or corrupted protect student data
- Using latest software. Protection from suspicious communications. Controlled sharing. Differentiating org data from personal data.
- we have the confidence our work stays confidential. and this gives our patients confidence.
- Ensure a level of security and protection is implemented Peace of mind Compliance of services agreements
- Ensure everyone gets into a habit to be more aware of things they can do
- Confidence.

Evaluate Current Cyber Controls (3/3)

006

What changes would you like to see made to your organisations Cybersecurity controls?

(1/2)

- Fewer forced password resets
- Less disruptive updates - OS, Apps, Firmware lost time.
- we need to have better procedures in place for home working particularly for staff dealing/speaking with patients. we do not provide work mobiles so this is often done on personal devices which needs to be looked at.
- More responsibility with individuals, not resting on a singular person or couple of people to implement or educate everyone or keep up to date, particularly when their role is not technical More robust cyber security, more proactive monitoring, more IT company involvement More budget assigned to ensuring proper protocols are in place
- People being more aware of what can go wrong

Evaluate Current Cyber Controls (3/3)

0 0 6

What changes would you like to see made to your organisations Cybersecurity controls?

(2/2)

and everyone implementing preventative measures without even realising

- None ATM .

Measuring Cyber Security (1/4)

006

How do you Measure Cyber Security at the moment?

(1/2)

- Percentage of devices patched within required timeframes (e.g., 14 days). Click rates, reporting rates, repeat offenders. Percentage of staff completing mandatory cybersecurity training.
- Processes and best practices guides Onboarding / leavers training IT support and monitoring e.g. malware monitoring / antivirus
- a lot of our cyber security is dealt with by our IT team.

I complete risk assessments and spot checks around the practice, eg do people lock their PCs when they are unattended, this is particularly important when GPs leave their rooms as they can be accessed by anyone.

- Monthly reviews of patch status and security alerts.
- I don't think we do measure it - we have systems in place we hope prevents

Measuring Cyber Security (1/4)

006

How do you Measure Cyber Security at the moment?

(2/2)

attacks but I am not sure how we review these systems or the impact of them

- We have a training platform which we monitor and send out reports to Line Managers. Also simulated attacks. We also have a company do penetratin testing once a year.

Measuring Cyber Security (2/4)

What are you not measuring?

006

- Accessibility barriers for neurodivergent or disabled users Unapproved cloud storage (Google Drive, Dropbox, WhatsApp)
- Password strength Updates / patches being done within appropriate timescales Connected devices and whether these are up to date Firewall protection Device set up e.g. purchased from different providers / set up differently in different teams
- at practice level we do not measure near misses. this is something we receive updates about from our locality
- Shadow IT
- Possible attacks or attempts on breaches that weren't successful
- Probably Something - though not sure what!

Measuring Cyber Security (3/4)

006

What's one thing that absolutely needs to be measured?

- suspicious login attempts
- MFA being used
- something we can measure at practice level is near misses, eg hacker emails that come into the practice. we can use this as a training tool for staff and new staff to look out for.
- Device and App compliance.
- Unsure
- Access control / priv rights.

Measuring Cyber Security (4/4)

How can you measure that?

005

- how long attackers had access
- Ask IT support to check what devices are protected Issue mandatory training and regular checks - but unsure how these could be measured remotely
- record the number of emails we receive a month/quarter as this is not something we currently do. We receive updates from our locality but we do not do this at practice level.
- Automation essential rather than measurement.
- Ensuring protocols are follwed and recorded.

Cyber Culture (1/3)

006

What do people think about Cyber in our organisation?

(1/2)

- If they do think about it, it's likely more tick box exercise or that they don't think it's their responsibility. That it's confusing, too technical. Very reactive, only really consider how important it is when something goes wrong or when its a requirement to win a tender.
- Staff think that cyber threats are serious, but they often believe that “IT will handle it.”
- there is a clear divide between those who are capable at using IT and those less capable.. Those who are less capable make cyber risks/data breaches more likely so more training for some staff is important.
- A few years ago the response would have been "we are not a bank", now through training and awareness people understand why we would be attacked.
- They are aware we

Cyber Culture (1/3)

006

What do people think about Cyber in our organisation?

(2/2)

don't have a blame culture and we're here to help them.

- Unsure - we probably need to be better at asking or assessing

Cyber Culture (2/3)

How do we promote healthy Cyber habits?

(1/2)

006

- Engaging training sessions and quizzes - so it becomes less of a tick box exercise Give real life examples and explain consequences e.g. disciplinary / misconduct / misuse of IT etc / wider impact on your company of being the reason there has been a breach e.g. operationally causing a standstill
- gather feedback on what works highlight success stories
- Promote a learning culture if people make mistakes. mistakes are learning points to be shared with everyone so it doesn't happen again in the future.
- Automated communication of alerts has been incredibly useful for raising awareness, but does sometimes cause friction.
- Training, gameification - fun excerices. We share incidents accross the comapny - how we delt with them and what to look out for.
- Incorporating changes into

Cyber Culture (2/3)

How do we promote healthy Cyber habits?
(2/2)

006

every day habits to make them
become part of what they need to
do anyway rather than over and
above

Cyber Culture (3/3)

How does this become part of our everyday?

006

- More regular discussions - like what Adam said about a regular compliance meeting Education from 3rd party sources
- Make secure behaviour automatic
- share weekly/monthly updates of relevant things that have happened. dont name and shame staff just share the facts
- We are looking st setting up informal communication channels where people can share knowledge and experiances.
- Making it part of the culture and our shared responsibilities to each other to stay safe.
- Educating people in what can go wrong, the changes that have been put into place that they may not be aware of that they are doing anyway

Action Plan - Make a list of the things you're going to do from today

0 0 6

(1/4)

- More research and teaching ideas from the training today 1. How interface design, transparency, and communication shape trust (research) 2. What students think they know vs. what they actually know (teaching- Cybersecurity literacy) 3. When do humans trust or distrust automated decisions? (research) 4. How do usability, cognitive load, and organisational culture shape everyday cybersecurity behaviour in hybrid work environments? (research)
- 1. Find out more about current set up in terms of monitoring / proactive resolutions 2. Complete questionnaire from potential alternative IT provider to be able to proceed with level of support required 3. Review all partners to ensure all appropriate protections are in place e.g. MFA / 4. Review current suppliers / potential dormant accounts that need to be removed 5. Gaining a better understanding of how to implement regular monitoring from a remote point of view 6. Discuss how

Action Plan - Make a list of the things you're going to do from today

(2/4)

006

current IT provider could help us with more proactive monitoring and reporting 7. Book 30 minute call with Cyber Essentials advisor to understand gaps 8. Understand whether there is a need to split M365 tenancies – what are the risks / reasons to stay in this set up 9. Create separate AI policy 10. Review training policies are reflective of cyber security protocols 11. Review and update current IT use policy and IT Security policies

- 1. Review all current SaaS applications compliance with Cyber Essentials 2. Come up with "Mover" processes to complement start and leaver processes 3. Put additional effort into application management 4. Investigate making policies more accessible via alternative (AI-generated) versions 5. Set up an informal cyber communications hub
- 2. Policy review – esp. WRT AI. 3. Seek staff feedback on

Action Plan - Make a list of the things you're going to do from today

0 0 6

(3/4)

training, policies and overall management, how employees feel about cyber security. 1. Outline clearer responsibilities to staff and, as an employer, our responsibilities to them. 4. Take a look at the Cyber Assurance qualification.

- Additional training for staff not just mandatory training. Make training more personal to staff, find the gaps in knowledge Sharing examples of scam emails with staff so they know what they need to look out for and they should report every scam email they believe they see, this is so we can report them to our IT team and the ICB to share with other practices. Try and change our culture. We should not have a blame culture in the practice, we need a learning culture. This will have to happen over time, I feel we may be missing things as staff are afraid to hold their hands up to mistakes being made.
- 1. Educate everyone

Action Plan - Make a list of the things you're going to do from today

0 0 6

(4/4)

within the business about the impact of a cyber breach 2. Educate everyone on what restrictions we have in place that are preventative measures 3. Run reports to understand how many potential breaches have been stopped because of the measure we have in place 4. Add new policies - A1 5. Update company induction to include all of the above to ensure a more robust section on cyber security in the hope that all procedures and awareness will become second nature to new starters

- Policy review – esp. WRT AI. Seek staff feedback on training, policies and overall management, how employees feel about cyber security. Outline clearer responsibilities to staff and, as an employer, our responsibilities to them. Take a look at the Cyber Assurance qualification.

Action Plan - The One Thing (1/3)

006

What's the ONE thing you're going to by the end of today?

- Reporting suspicious activity is the single strongest behaviour that predicts a resilient security culture. Start recording it.
- email management colleagues with points from this course that we need to look at going forward, eg, monitoring scam emails going forward.
- Obtain April 2026 Cyber Essentials requirements
- Look into renewing cyber essentials
- Put in a mtg w/ Ops Dir. to discuss AI policy.
- Review current IT use policy and IT Security policies - identify areas for improvement

Action Plan - The One Thing (2/3)

006

What's the ONE thing you're going to do tomorrow?

- Add one cyber-awareness reminder to tomorrow’s meeting.
- look at what our mandatory training covers in regards to cyber security, ask other practices in our area if there is further training they offer to their staff which we could also offer to ours.
- Come up with process for identifying SaaS usage
- Look into Cyber Assurance and DCC
- Look at surveys for staff to get a feel about what they thing re secuirty culture.
- Create separate AI policy

Action Plan - The One Thing (3/3)

006

What's the ONE thing you're going to do next week?

- Clean up one device or account, remove old apps, update software, and delete unused logins.
- Ensure we have an up to date list of our provides and what access rights they have. if this is not already done, begin to build and keep updated going forward. We have a quarterly staff newsletter, we can include near misses and learning points in our newsletter
- Discuss additional SaaS controls
- Update, educate and inform everyone within the business
- Look at the Cyber Assurance qual.
- 1. Find out more about current set up in terms of monitoring / proactive resolutions