Nuffield Department of Population Health

UNIVERSITY OF OXFORD

The Pursuit of Cyber Essentials

Information Governance Team
Nuffield Department of Population Health
University of Oxford

What is Cyber Essentials?

- UK Government Assurance Scheme operated by National Cyber Security Centre (NCSC)
- Provides Assurance for Collaborators
- Audit Framework for internal assessment of IT Infrastructure
- Useful baseline towards Cyber Essentials Plus and ISO27001

Benefits

- Used as an audit framework, Cyber Essentials criteria can identify data risks
- Triggers review of process balance between confidentiality vs availability
- Flag to senior management – non compliance is now a conscious decision (wilful negligence?)
- Stops a culture of *‘We’ve not had any issues so far…’*

Examples of Criteria

Five technical controls areas, which can be meet via:

- Password Lockout after more than 10 attempts
- Minimum Password Length of 8 (we moved to 12 characters)
- Software whitelisting
- Software patching within 14 days
- Special Access Privileges removed when no longer required

Challenges/Resistance

- Password Lockout after more than 10 attempts –
  High burden on IT to unlock accounts!
- Minimum Password Length of (we moved from 8 to 12 characters)
  Inconvenient - People will write them down!
- Software Whitelisting
  Not feasible – programmers and statisticians build numerous bespoke software packages, into the 1000s!
- Software patching within 14 days
  Upgrade to current software version may compromise/corrupt the data.
- Special Access Privileges removed when no longer required
  Waiting for a new IT management system to be implemented.

IG Team's Response

- Flag the issues of non-compliance to Senior Management - updated our Risk Register.
- Pursue a management decision – Accept, mitigate etc.
- Be solution-oriented.
- Explain the impact of non-compliance (not about the accreditation, it's about the vulnerability)
- Look for quick wins, equivalent controls, and revisit the standard – Be prepared to "Hold your position *lightly*."

Over to you…

What was your experience of pursuing Cyber Essentials?

How big was the scope of your application - entire IT infrastructure/Department/Project?

How did you overcome challenges/resistance?

Thank you for your time!