CYBER ESSENTIALS IN HIGHER EDUCATION:

THE GOOD, THE BAD, AND THE OPPORTUNITY

JORDAN M. SCHROEDER, CISSP, CISM, CRISC
HEFESTIS COO & MCISO

NOV 2019

HEFESTIS CISO-SHARE

HE/FE SHARED TECHNOLOGY & INFORMATION SERVICES

“WE WANT ALL PUBLIC SECTOR BODIES IN SCOTLAND TO COMPLY WITH CYBER ESSENTIALS”

SAFE, SECURE AND PROSPEROUS: A CYBER RESILIENCE STRATEGY FOR SCOTLAND

PUBLIC SECTOR ACTION PLAN 2017-18

CYBER ESSENTIALS

- “Basic” questionnaire
- “Plus” 3rd party assessment
- 5 Controls
  - Malware, firewalls, patching
  - access control, configuration

PRESCRIPTIVE, UNAMBIGUOUS

- Like PCI-DSS
- “80%” of cyber attacks
- Specific, testable controls
- You could **pass** ISO 27001and **fail** CE+

CYBER
ESSENTIALS
PLUS

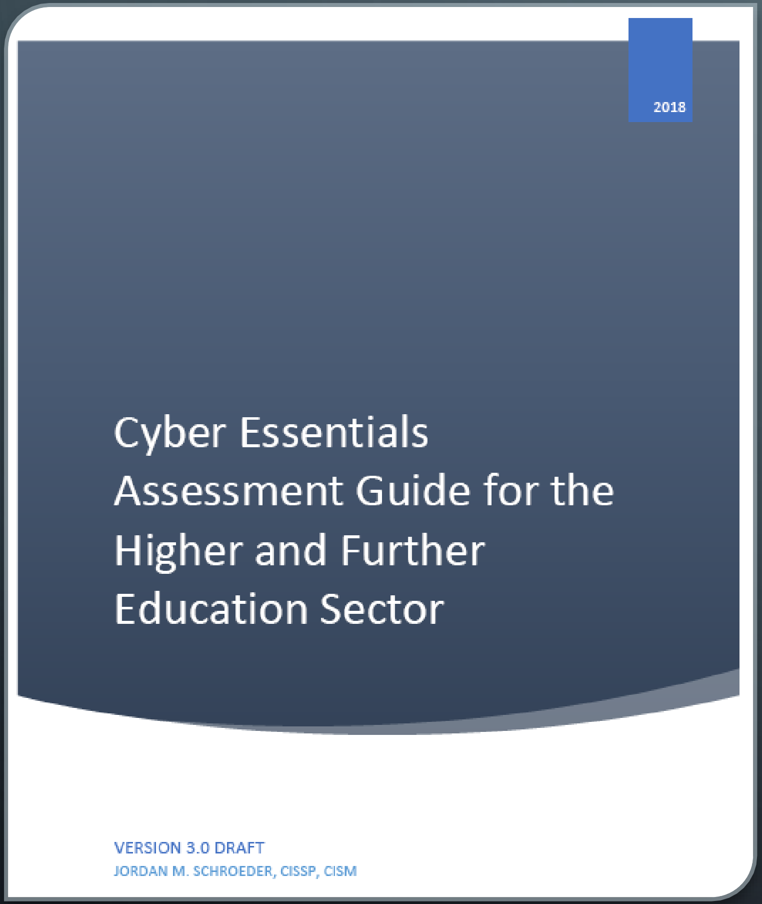
HEI CHALLENGES

- “Heritage systems”, Electron microscopes, etc.
- De-centralized IT, research depts & commercial units
- Cybersecurity courses
- Curriculum needing older software
- Public access and academic freedoms
- Eduroam

CERTIFY A UNIVERSITY??

Yes!

HOW???



2018

Cyber Essentials Assessment Guide for the Higher and Further Education Sector

VERSION 3.0 DRAFT

JORDAN M. SCHROEDER, CISSP, CISM

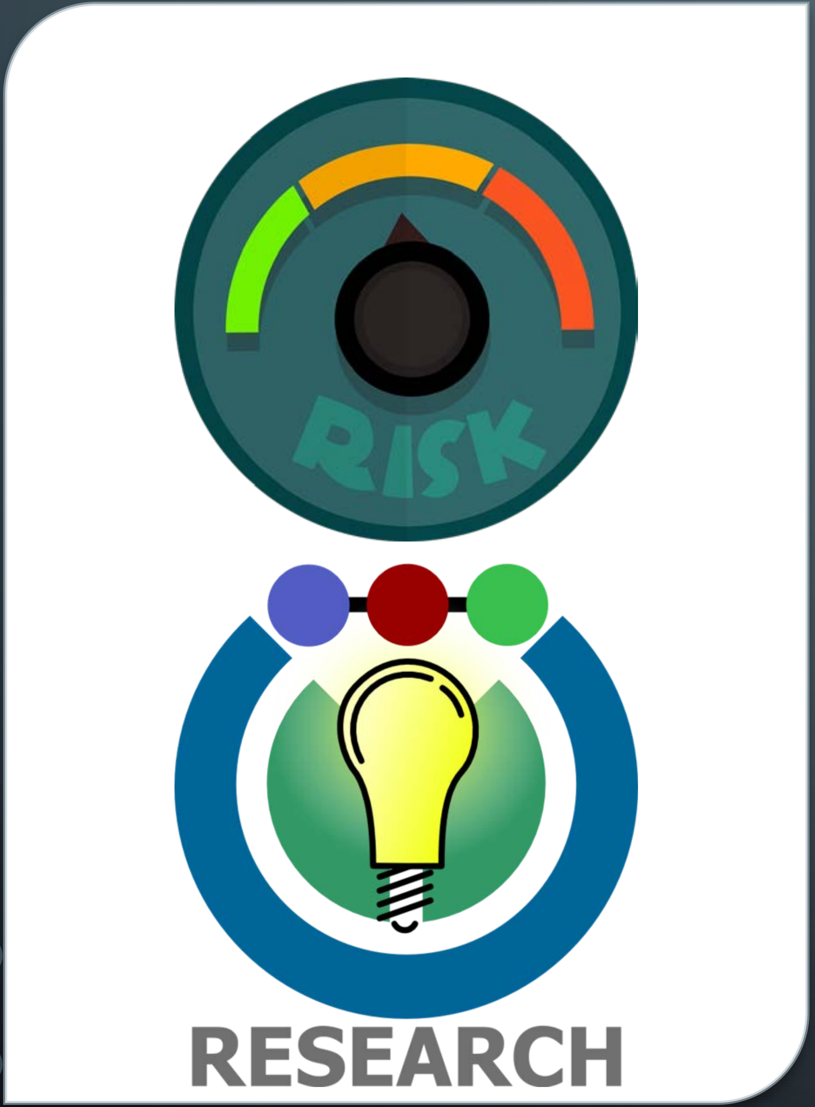
- Worked with Assessing Bodies & NCSC
- Set expectations & devised assessment approaches

SCOTTISH HEI PROGRESS

- Nearly all have certified some core scope
- Almost all are progressing towards full certification
- Around half have certified at least 90% of their estate

OPPORTUNITIES FOR AN HEI

- Clear and unambiguous security controls
- Consistency across the institution
- Break out of siloed system administration
- GDPR “appropriate controls”
- Research funding requirements



OPPORTUNITIES FOR AN HEI

- Reduce Risk
- Capture Research Opportunities

WAR STORIES

- Server set up 15 years ago and left unpatched
- “Please do not turn off…”
- “No”
- “*Every* system?”
  - CCTV

PRO TIPS

- Top-down buy-in and support
- Project manager
- Prepare an Assessor
- Vulnerability scanners are crucial
- It’s all about scope

SCOPING TIPS

- Start with the core administration network
- Cut off non-compliant systems/networks from the Internet and the rest of the network as a whole
  - “Bubble them off”

“BUBBLING OFF”

- In their own “bubble”
- Strictly limit and control access to these systems
- Proxy or 1-to-1 firewall rules
- Segmented or virtualized networks

PATCHING/UPDATING TIPS

- Easily the biggest challenge!!
- Out-of-support software/OS
- Need to incorporate ongoing updates in all procurement & project requirements
- Patch schedules/downtimes
  - Resource them properly!

PATCHING/UPDATING TIPS

Is your decision to not apply security patches when you know they are needed?

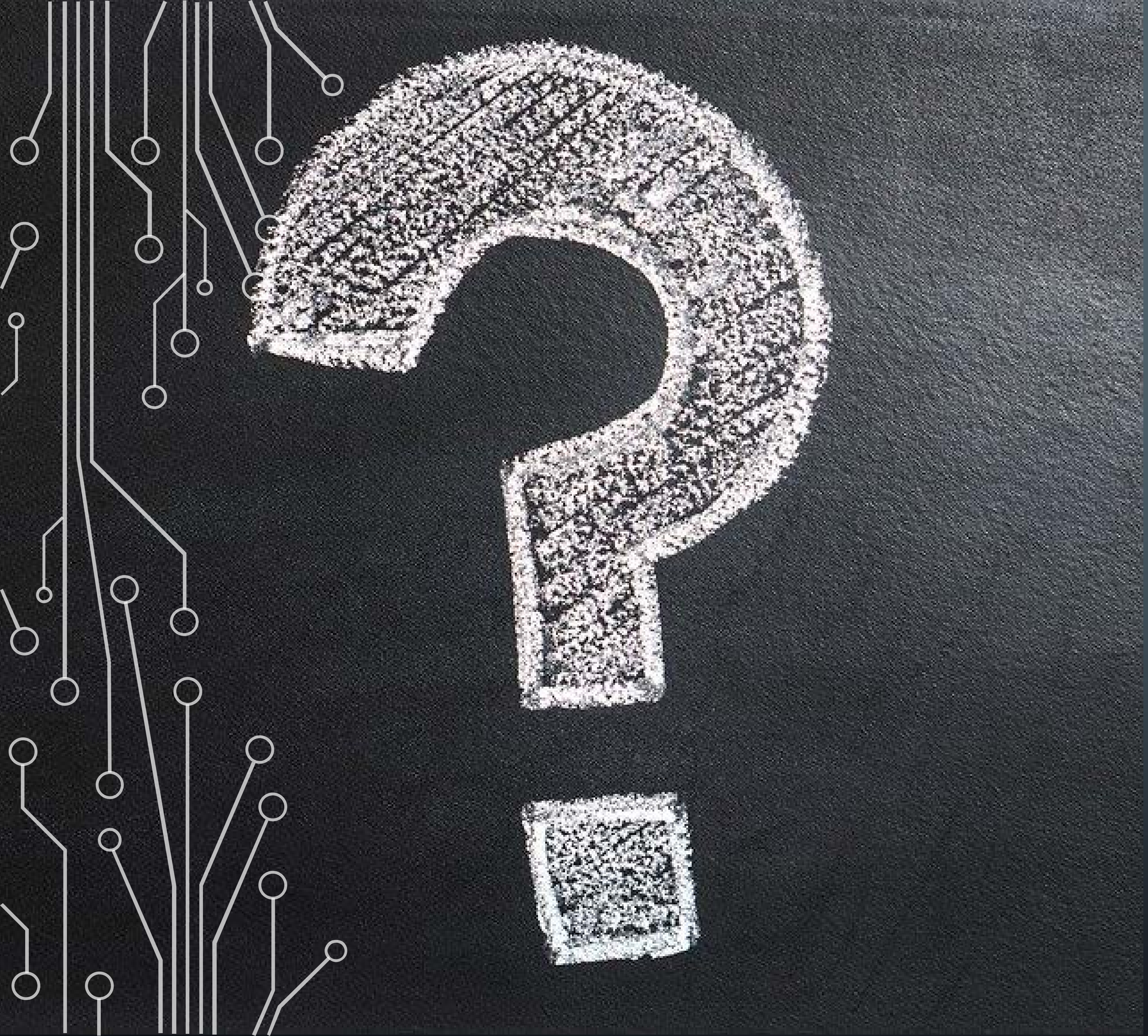
SUMMARY

CYBER
ESSENTIALS
PLUS

- A worthwhile challenge
- Clear and unambiguous security controls
- Rapidly matures cybersecurity processes; reducing risk
- Growing focus on the standard by funding sources

SUMMARY

- It is not just an IT project – bring management in
- Work with your Assessor
- Scope and Bubble
- Plan for network architecture changes
- Plan for major changes in patching/updating



QUESTIONS?

Jordan M. Schroeder
COO & MCISO

HEFESTIS