Balancing BYOD & Cyber Essentials Webinar - Questions

Who?	Question	Answers?
Ben Faire 11:04	Which regulations are referring to for CE? Is it the new regs coming out in April?	[CH] I assume most of us are talking about the current, Evendine, question set. The new Montpellier question set will be live from April this year.
Ben Faire 11:14	For CE are we going to be discussing privileged access admin rights?	[CH] I don't believe we had time to discuss any specific elements of the privileged access requirements within the CE framework. HB: Good suggestion for another webinar with a CE angle involving a PAM sponsor, e.g. IIQ/Sailpoint
Michael McLannahan 11:15	What's your Mac/Windows Staff split?	[CH] Around 80/20 towards Windows, which is our primary platform. Although we do offer managed builds on both. HB: Windows to Mac 80/20. Windows main managed platform, managed Mac/Linux available also
Shaun Miller 11:16	Are you all requiring MDM enrolment for BYOD access to services and which products are you using please?	[CH] Yes for all mobile phones and tablets. For iOS we use Jamf and for Android we use Intune. We use the 'personal device enrolment' mechanism on both platforms rather than managing, and having access to, the entire device. HB: No MDM enrolment. BYOD policy acceptance mandated for using own devices to access services. Exploring using Intune for all platforms in the future.
Thierry Delaitre 11:16	did you enforce conditional access for the two third who did not enroll into the MDM?	[CH] Yes, conditional access is in place for all University systems and services. So for those who have not enrolled into one of the MDM solutions, they won't be able to access those services from other devices.

		HB: Conditional access enforced for BYOD, e.g MFA and policy mandated
Anthony Sams 11:16	What controls are in place to stop staff and students accessing software that is only licensed for on premise use?	HB: AppsAnywhere controls in place (On-Site only, On-Domain Only, etc.). Also by AD group
Jon Burt 11:17	Does CE allow fingerprints instead of 6 digit PINs?	[CH] Biometric authentication (such as facial recognition or fingerprints) can be used to 'wake up' the device, ie from a screen lock or timeout. However, when the phone is restarted, or turned on, the PIN must be entered and biometrics are not valid.
Alastair Scobie 11:17	Is it easier for the smaller, younger, Universities to impose stronger policies on BYOD than for the larger, older, Universities?	[CH] I only have my own frame of reference to go off here, but I would be very surprised if there is any institution out there that is not wedded to the idea of BYOD. As referenced during the panel session, the policy change on BYOD was the single biggest challenge that we faced, and although we did manage to make that change as a team, it was a hugely complex and co-ordinated effort. We utilised top down communications, local pitches and discussions to teams and departments, Q&A sessions, multiple trade union visits, lots of one to one discussions and a dedicated support team to deal with any and every query. HB: Agree, I believe we all face the same challenges, perhaps in different proportions, nevertheless key aspects are good comms and an agreed BYOD policy/principles
Mark Watts 11:18	Haigh, Christopher do you forcibly segregate managed devices away from unmanaged ones on the network?	[CH] Yes. Our unmanaged devices can't access any in scope services (that our managed devices can access).
Sam Hannan 11:18	Haigh, Christopher - Do you class PGRs as staff or students?	[CH] It depends on how they have been set up as an identity in our system. But if there is any element of 'staff' about them, then the full suite of CE rules and regulations

		apply to that account, and any devices used by that account.
Ben Faire 11:19	One of the new requirements of the new regs for CE is that ALL software and firmware on the device must be kept up to date. What systems are people planning on using for this?	[CH] We are currently using a combination of Windows Defender and Nessus but are looking at reviewing our approach to this, as we haven't found a straight forward way of doing it yet. HB: Policy driven approach with University provisioned applications version controlled using AppsAnywhere. Separate avenues being explored for BYOD to support policy governance.
Christopher Oderele 11:23	Do you have MFA enabled in all your cloud services?	[CH] We are currently going through our systems to ensure MFA is in place not just for accounts on cloud services that have privileged access, but for all user accounts on those cloud services. HB: Yes we do. May review access on wired/eduroam where appropriate
Mark Watts 11:27	How do you segment exempt devices?	[CH] With our definition of exempt devices, which is a device still subject to CE rules and standards, but is not managed by the University, there is no segmentation in place. This is because the exempt devices are still compliant with CE, so there is no requirements for them to be segmented.
Thierry Delaitre 11:28	did you put in place conditional access for other applications eg M365, finance, etc ?	[CH] Yes we did, for as many services as we could actually. We also utilised an App Proxy solution to extend the reach of conditional access.
Nick Sharratt 11:29	How does deciding to 'take a risk on people' work when it comes to getting CE though? Is it accepted by the assessors to only have controls in place for *most* people?	[CH] No, the CE standard requires that all in scope devices/accounts are compliant, no exceptions. The 'wiggle room' that we were talking about is whether you are using a technical control that you know has 100% compliance, or a process control, where the onus is on the user to comply with it, and you are trusting that the user is complying with the process/action you've requested of

		them. So 'taking a risk on people' in this context, would be like saying please don't lend your login details to someone else. The control is in place for all users, but we can't necessarily enforce it as an institution. HB: We have employed policy controls and they are in place for all, as they need to be for CE compliance.
Shaun Miller 11:33	From a resourcing point of view what has been the impact for supporting CE/BYOD and related things on your Service Desks please?	[CH] For our project, we set up a dedicated support team for Cyber Essentials, to help deal with all the queries and concerns, as well as offer the technical support and listen to where we could make further improvements. This was around a three person team, we received around 2000 calls over a 3 month period, and turned around 95% of calls within 24 hours. HB: Extensive comms supported by the appropriate workshops and guidance has been the backbone of the accreditation project. As we base our approach primarily on policy there is a key requirement to get senior stakeholders on board, they understand the implications of not becoming CE accredited on the business and are therefore advocates of mandating policy principles.
Thierry Delaitre 11:52	have you implemented conditional access for all of your business applications for protecting organisational data?	[CH] Yes we have, for as many services as we could actually. We also utilised an App Proxy solution to extend the reach of conditional access.
	KEY FINAL QUESTION	
Post-discussion	How can you ensure that BYOD devices are compliant with Cyber Essentials?	[CH] There are various approaches you can take to BYOD. One question I've been asked a few times is how can you ensure that BYOD devices are compliant, if you don't manage them yourself. One approach might be to completely block any BYOD – which would be CE compliant, but could limit usability and

		affect staff experience. This is our default position for laptops and PCs. Another approach would be to use a policy based approach, create a user policy that outlines all of the requirements of a CE compliant device, and request that any user on a BYOD device ensure that the device they are using is following those stipulations. This is perhaps the other end of the spectrum, it's not as restrictive on usability or experience, but it's high risk that all of your users will understand what they are supposed to be complying with on their BYOD device. To be successful this requires a good level of understanding and education, but also offers the most freedoms – we'd love to move to this way of working one day, but we aren't ready yet. Another approach would be to use a management agent that enforces technical compliance on the BYOD device. This is more restrictive and potentially obtrusive on a personal device, but lower risk in compliance terms. This is the approach we use for mobile devices and tablets. An illustrative example that I've used previously would be a CE requirement for complex passwords that are not written down anywhere. You can utilise a variety of different ways to achieve that same outcome – you could use pure policy and say please don't ever write down your passwords, and please make sure your passwords have a minimum of 12 characters. As long as that is your policy, and you're confident everyone is following it, then you are compliant from a CE perspective. However, if you wanted additional assurance/confidence, then you could implement a technical control on the password length

		element to ensure that area is being met, but you would still be reliant on a policy based solution for the "don't write it down anywhere" element. HB: An MDM driven approach will probably be the closest you will get to being able to police compliance yourself. However, this requires resource to manage and, by extension, you are taking a level of responsibility for something the user should be managing themselves. An application/desktop virtualisation approach will allow you to adopt a risk-reduction stance, leaving less reliance on the up-to-date status of the device. Nonetheless, for CE purposes, the device still needs to be compliant. The policy driven approach we have employed places the onus with the device owner of maintaining updates and security features. Ultimately this relies on behavioural adoption, however, as users are the biggest cyber risk, it hopefully also encourages the appropriate cyber aware actions beyond device management, to the benefit of the organisation.