NICK WILDING– AXELOS

Contact Information:
Nick Wilding
Head of Cyber Resilience, AXELOS
E: nick.wilding@axelos.com T: 07860 950108

Q: When in London will it be released?

A: Announced at live events in DC on June 1st, and on Monday, June 22nd, held at the Guildhall in Central London. June –expect releases on training, self-paced learning, and the exams. The practitioner's certificate will be available by the end of July. Full details to come then.

Q: How can a leader emphasize that Cyber Resilience training (as compared to Cyber Security) is equally important?

A: Information is the key in any guise it resides in. There's a lot of paper still out there with information that people still have to look after. Equally, we have to understand that the nature of the risk that we face, the levels of sophistication and ingenuity, it's more become a case of WHEN we are attacked versus IF we are attacked. The statistic is about 203 days before anyone even realizes they've been attacked. You have to be able to respond and recover to the pending attack which is happening, and recover in a way that brings us back to normal as quickly as possible, and that time is key. People need to be engaged and informed about how to recover.

Q: Interested in the official AXELOS definition of Cyber Resilience - it includes information but wondering if it should be more at a knowledge level as well as including process and assets/capabilities. Asking if the definition is at the right level - thinking knowledge and capabilities as the level that Cyber Resilience should be focused on - information seems to be at a lower level of importance

A: The ability for an organization to resist, respond and recover from threats that will impact the information they require to do business. – Protect and detect. Information at all levels, how systems are configured and vulnerabilities that are there. There are ways to check, but as software gets more complicated it's about the critical information for continued operation.

Q: To what level will Cyber Resilience cover BYOD related issues within the org?

A: The world we operate in is increasingly moving to BYOD (Bring Your Own Device). Again there are some good technologies which will help us to manage that particular vulnerability. But ultimately, they pose the same sort of risk as any other device. We need to manage them accordingly. Just make people aware of how to protect the device.

Q: You mentioned have a strong password. What password advice would you give us for better security?

A; Use a strong password, at least 8 characters, mixture of upper and lower characters and or special characters and or numbers. Also, don't write them down or share them. Simply, use an acronym and spell out a phrase. Don't use dictionary words. Don't use something easily identifiable with you.