TEG7

PULSE CONFERENCES

Cyber Policy and Standards for Systems Security

25-26 April 2018
Dubai, United Arab Emirates

This 2-day course focuses on the rapidly changing business and technical environment and how the choice of standards and codes of practice can make a significant difference to the success of your organisation. There are a range of existing cyber security related standards, publicly accessible specifications (PAS) and codes of practice. The choice of whether to implement specific standards can have a significant impact on your organisation's costs and performance.

The objectives of the course are to enable delegates to:

- examine the nature and role of standards, publicly accessible specifications and codes of practice;
- review of the security standards landscape;
- understand factors to be taken into account when specifying or implementing standards, both within the organisation and its supply chain.

Course Modules

Module 1: The nature and roles of standards

The module will examine the nature and standing of organisations that produce standards, the types of standards produced and the lifecycle of a typical standard from concept through to its replacement or revision.

Module 2: Understanding testing, validation and verification

This module will examine the use of certification to confirm conformance of organisations, processes, products and services to particular standards. It will examine the assessment processes and the potential pitfalls

Module 3: The security standards landscape

There are a range of security standards available covering organisation, personnel, physical and cyber-security. This module will examine a number of cyber security standards, ranging from those produced by international standards organisations to those developed by industry bodies and professional organisations.

Module 4: Choosing and using standards

This module will use case studies to illustrate the selection and use of standards to address security both within your organisation and in your organisation’s supply chain.

- ***Individuals complete personal review of skills development***
- ***Course summary and take-aways***

About the instructor:

Hugh Boyes BSc(Hons) MBA CEng FIET CISSP
Hugh is a Chartered Engineer, a Fellow of the Institution of Engineering and Technology (IET) and holds the Certified Information Systems Security Professional (CISSP) credential issued by the International Information Systems Security Certification Consortium [(ISC)2]. He divides his time between working as a Principal Engineer at the University of Warwick and undertaking cyber security training and consultancy assignments. Hugh is an industry expert on cyber threats to cyber-physical systems, including those in the built environment, ports and maritime sectors. He has written four guidance documents for the IET covering cyber security in the built environment, ports and vessels. His research work focuses on the protection of control systems, whether traditional industrial controls or employing IoT technologies. He is the co-author of British Standard's PAS 1192-5:2015 [Specification for security-minded building information modelling, digital built environments and smart asset management] and PAS 185 [Smart Cities – Specification for establishing and implementing a security-minded approach]. He regularly reviews standards to assess their handling of security issues and sits on the drafting committee for the forthcoming British Standards BS10754 suite of documents. Hugh is a Member of the Register of Security Engineers and Specialists (RSES).

Key information and registration

Name: Cyber Policy and Standards for Systems Security

Date: 25-26 April 2018

Location: Dubai, United Arab Emirates

Course length: Two days

Price: £1,500

Register for this course:

To register or find out more about this course please email:sanna.lindstrom@pulseconferences.com