AGENDA:
Cyber Essentials: The UK Government
Scheme to improve cyber security
(Dexter House, Royal Mint Court, London, 17 July 2014)

www.itgovernance.co.uk

Time		Session
09:00 - **9:30**		**Registration** Tea and coffee Networking
09:30 - **09:35**		**Welcome to Cyber Essentials 2,** and introduction to guest speaker, Richard Bach (Michael Shuff, IT Governance Ltd).
09:35 - **10:30**		How the Cyber Essentials Scheme is likely to work – and what to do next: **Richard Bach, Assistant Director - Cyber Security, Department for Business, Innovation and Skills (BIS),** will bring news about the UK Government Cyber Essentials Scheme. Following on from the BIS Call for Evidence on a preferred organisational standard for cyber security conducted last year, industry representatives and BIS have collaborated on the development of a scheme for basic technical protection from cyber attacks. The Scheme comprises a set of requirements for technical controls, and a draft assurance framework on which the BIS are seeking feedback. Richard will outline how the Cyber Essentials Scheme identifies the security controls that organisations must have in place within their IT system in order to have confidence that they are beginning to mitigate the risk from Internet-based threats. He will answer your questions and be available to speak to delegates over lunch.
10:30 - **11:30**		**Keynote speech: Alan Calder** on the importance of HM Government's analysis of continuing attacks, which was the impetus behind the Cyber Essentials Scheme. Feedback from industry vulnerability testers has identified that a number of security controls are still not being applied. Organisations are vulnerable due to a lack of essential security controls. They continue to be at risk from threat actors on the Internet with low levels of technical capability, meaning that when the breach occurs, it will be embarrassing to admit just how easy it was for the hackers to succeed.

			Alan will show that companies who are good at cyber security can make this a selling point – demonstrating to their customers that they take the responsibility for safeguarding data seriously throughout the organisation. Alan is a leading authority on implementing cyber security best practice and IT governance. He is founder and executive chairman of IT Governance Ltd, the Cambridgeshire-based single-source provider of products and services for IT governance, risk management and compliance. His talk will look at Cyber Essentials as the starting point for protecting confidential data and your organisation's reputation from cyber threats. In particular, he will focus on the governance of cyber security: people, processes and technology, and why you need to manage cyber security using a standards framework.
11:30	**-**	**12:00**	**Networking break – Tea and coffee.**
12:00	**-**	**12:45**	**Sarb Sembhi, ISACA, on Assessing Cyber Insurance Risks**: how the Cyber Essentials Scheme could become a requirement of insurers seeking evidence of good practice.
12:45	**-**	**13:45**	**Buffet lunch** and networking opportunity.
13:45	**-**	**14:30**	**David Clarke** is a former Detective Chief Superintendent with the City of London Police. He has served in the UK, Middle East and Eastern Europe, and has led international police operations as part of the United Nations Mission in Bosnia Herzegovina. As a member of the UK Government's Fraud Review, David was responsible for designing and delivering ground-breaking counter-fraud services, including the National Fraud Intelligence Bureau, National Fraud Reporting Centre and the Lead Force for Fraud. Today, he is a Trustee Director of the UK's Fraud Advisory Panel charity where he is engaged in initiatives to protect UK businesses from fraud, and pioneering activities to help fraud victims recover their losses. He's also a board member at Today Advisory Services in London, working as a specialist in preventing financial crime in multilingual supply chains.

David's talk, '**The real evidence that cybercrime is on the increase**', is based on his experience of frauds that have taken place in the City of London in recent years, combined with reliable statistics that he knows represent an accurate picture of the growth in cyber crime and its impact on UK businesses.

David knows why you don't always hear about cyber breaches in the media, and believes that corporate culture must change.

14:30	**- 15:15**	**Kevin Olver, ISO 27001 Auditor, SGS**

ISO 27001:2013 - a proven international framework for building, implementing and monitoring an ISMS

SGS is a world-leading audit and certification service helping you to gain business improvement and competitive advantage. The organisation is recognised as a global benchmark for quality and integrity, employing 75,000 people and operating from a network of 1,500+ offices and laboratories around the world. Kevin's presentation will cover the following topics:

- The role of the certification body.
- Increasing demand for ISO 27001.
- Why has ISO 27001 changed, and what has changed?
- ISO 27001:2013 controls relevant to the Cyber Essentials.
- The impact of mobile devices.
- How ISO 27001:2013 certification can help.

15:15	**- 15:45**	**Networking break – Tea and coffee.**

15:45	**- 16:30**	**Geraint Williams, Senior Consultant and Trainer, IT Governance Ltd**

The Cyber Essentials Scheme provides guidance to help organisations of all sizes measure their defences against common forms of cyber attack.

The systems that fall under the scope of the Cyber Essentials Scheme include Internet-connected end-user devices (e.g. desktop PCs, laptops, tablets and smartphones) and Internet-connected systems (e.g. email, web and application servers). By implementing the Cyber Essentials, organisations are mitigating against the following common types of cyber attack:

1. Phishing: malware infection through users clicking on malicious email attachments or website links.

2. Hacking: exploitation of known vulnerabilities in Internet-connected servers and devices using widely available tools and techniques.

Geraint Williams, a senior consultant with IT Governance, will look at how the technical tests required under the Cyber Essentials Scheme will go a long way to protecting your organisation from these threats by identifying vulnerabilities.

Demonstrations of **vulnerability scans and penetration tests** will take place in the break-out area during the day, delivered by an ethical hacker who is part of Geraint's team.

16:30 - 17:30		**Panel discussion**

'What are the real challenges of implementing Cyber Essentials?'

Chaired by: **Tony Drewitt** (Head of Consultancy, IT Governance Ltd)

Panel members:

- **Alan Calder** (Founder and Executive Chairman, IT Governance Ltd, and leading authority on cyber security)
- **David Clarke** (Board member at Today Advisory Services in London, and founder of the National Fraud Intelligence Bureau)
- **Sarb Sembhi** (Chair of the ISACA Government and Regulatory Advocacy Committee, and a member of the ISACA Relations Board)

The panel will consist of some of the leading practitioners in the field of cyber/information security compliance and best practice methodologies.

From 16:00, you will also be able to attend a one-to-one advice surgery – see below.

16:00 - 17:30   **Cyber Essentials and ISO27001:2013 consultancy advice surgeries**

Confidential one-to-one advice sessions where delegates can ask the experts.

In addition to the formal talks and workshops, there will be an opportunity to meet IT Governance Ltd's expert consultants on a one-to-one basis and ask questions that will help you to identify which compliance objective/regime is suitable for your organisation, and how best to support and deliver this. This advice has already helped 150+ organisations to achieve certification to ISO27001.

Please book your advice surgery via the registration desk.

Cyber security product showcase 'Cyber Security Expo 2014' – the IT Governance roadshow that you need to attend

IT Governance Ltd, in association with our partners, SGS, ISACA, and the IISP (the Institute of Information Security Professionals), invites delegates to attend our cyber security exhibition, to watch and take part in live demonstrations of:

- **IT Governance: Cyber Security Risk Assessment Service** – consultants will help you to assess your current level of risk.
- **IT Governance Security Services –** qualified ethical hackers will give live demos of vulnerability scanning and penetration testing.
- **IISP (Institute of Information Security Professionals)** – members will be on hand to discuss the benefits of joining IISP.
- **ISACA**

Representatives from accredited certification body **SGS** will be on hand to discuss the process and costs involved in achieving ISO27001 certification.

17:30   -   Closing remarks: Michael Shuff of IT Governance Ltd.

Event ends.

Find out more about our speakers:

Alan Calder is a leading authority on cyber security. He is an acknowledged international author on information security and IT governance issues, and is the founder and executive chairman of IT Governance Ltd, the single-source provider of products and services in the IT governance, risk management and compliance sector.

Geraint Williams heads the Technical Services team of consultants at IT Governance Ltd. The activities undertaken by Technical Services include penetration testing and PCI DSS consultancy, along with infrastructure architectural reviews and other cyber security activities. Geraint is a highly experienced technical professional (CREST Registered Tester). He is also a PCI QSA and leads all PCI QSA consultancy activities for IT Governance. In addition to his role at IT Governance, he is a visiting fellow at the University of Bedfordshire.

Tony Drewitt, Head of Consultancy at IT Governance Ltd, has been a business continuity management practitioner since 2001, delivering BCM systems for a wide range of organisations in the private, public and voluntary sectors. Tony is a member of the Business Continuity Institute (MBCI) and acts as the technical expert on BS25999 for a UKAS-accredited certification body.

Sarb Sembhi is chair of ISACA's Government and Regulatory Advocacy Committee, and a member of the ISACA Relations Board. Sarb is a regular speaker at information security conferences around the world, including EuroCACS, RSA Europe, InfoSec, HITB, BCS, ISACA, ISSA, ASIS, IPSec, IFSec, Gartner, Richmond Events Security Summit and Econique CxO Dialogue.

Richard Bach is Assistant Director for Cyber Security at the **Department for Business, Innovation and Skills**. From the age of eight, inspired by the Enigma story, Richard wanted to break codes or catch spies. Appropriately, his chosen career path has been spent in the UK Government's security community.

In earlier years he was a technical advisor on export controls, before moving into international relations, representing the UK's information assurance interests in the EU, the UN and the OECD.

In a similar capacity in NATO, he was one of the main architects behind NATO's Infosec Framework. For the last six years Richard has brought his expertise to bear in cyber defence, and in late 2011 he became head of planning and delivery for the UK Government's operational cyber defence posture for the London 2012 Olympics.

David Clarke is a former senior police detective with the City of London Police and is government vetted to DV level security clearance. He now works as an adviser on multilingual risk management, counter-fraud and translation security assurance for Today Translations. David is a Trustee of the UK Fraud Advisory Panel charity. As a member of the UK Government's Fraud Review, he was responsible for designing and delivering the UK's National Fraud Intelligence Bureau and Lead Force for Fraud.

Ethical hacker/Penetration tester: Alexandru Apostol, IT Governance Ltd Technical Services, will demonstrate penetration testing – a service that can help you evaluate computer and network security by simulating an internal or external threat by attacking a computer system or network. The process involves an active analysis of the system for any potential vulnerabilities that could result from poor or improper system configuration, both known and unknown hardware or software flaws, or operational weakness in process or technical countermeasures.

Our sponsors and supporters: