BE AWARE – DEPLOY EFFECTIVELY – INFORM - ADVANCE

TRAINING BROCHURE

http://www.zyberglobalcentre.com

5/18/2020

Thank you for your interest in the Zyber Global Centre's interactive workshop training courses.

We are looking forward to answering your queries and collaborating with you.

BE AWARE –DEPLOY EFFECTIVELY – INFORM - ADVANCE

An Introduction to Electronic Evidence (for lawyers)

Length of course: Three days

Tutors: 1 or 2

Whatever area of law you decide to specialise in when you enter practice, you will be required to advise on the ramifications that follow the use of electronic evidence and electronic signatures.

Electronic evidence covers every area of law and given that few legal problems presented to lawyers do not include an element of electronic evidence, it is incumbent on lawyers to provide adequate advice to their clients – otherwise a claim for negligence might well succeed.

Electronic evidence is not a 'niche' area of evidence: mobile telephones and smartphone are ubiquitous, and people now communicate regularly through social networking sites, e-mail and other virtual methods. No area of human activity is free from the networked world – this also means no area of law is free from the effects of electronic evidence.

Level of knowledge of attendees

No knowledge is necessary. The aim is to look at the basic principles, and local laws and regulations will naturally apply.

Content

- *Introduction to electronic evidence*
- *Laying the foundations, challenges*
- *Seizure, authenticity, proof of intent*
- *Digital forensics and forensic tools*
- *Problem areas*

Aims

To alert lawyers to:

1. The importance of electronic evidence and what effect it has on their practice

2. To define 'electronic evidence' and offer practical illustrations and case examples

3. Understand the basic issues of electronic evidence to the extent that the need to obtain appropriately qualified technical advice is recognised when it becomes necessary

4. To recognize and illustrate the importance of awareness and knowledge of the nature of digital evidence in respect of the substantial legal and procedural issues in legal proceedings, and to appreciate that failing to challenge false assumptions can lead to a miscarriage of justice.

BE AWARE –DEPLOY EFFECTIVELY – INFORM - ADVANCE

Security, data protection and confidentiality (for lawyers)

Length of course: Three days
(can be compressed into two days if necessary)

Tutors: 1 or 2

The landscape in relation to security, data protection and confidentiality has changed beyond all recognition for lawyers in the twenty-first century. Lawyers are required to advise their own clients on these matters, but also need to be aware of how these topics affect how they run their practice.

Level of knowledge of attendees

No knowledge is necessary. The aim is to look at the basic principles, and local laws and regulations will naturally apply.

Content

- *Historical introduction – putting the topics into context*
- *Data protection principles and how it affects lawyers and their clients – at a high level of generality*
- *The duty of confidentiality of the lawyer and the duty of confidentiality of the client where they enter into agreements of confidentiality*
- *Security – both physical and electronic security*

Aims

To alert attendees to:

1. Understand the importance of protecting data and the duty of confidentiality, both physically and electronically

2. Understand the technology in protecting electronic data

3. Be aware of the failure of complying with duties regarding the protection and confidentiality of electronic data

4. To identify some of the practical problems that must be dealt with, for both clients and in the legal practice

BE AWARE –DEPLOY EFFECTIVELY – INFORM - ADVANCE

Teaches basic knowledge of cybercrime and digital evidence

An Introduction to Cybercrime and Digital Evidence

Length of course: Can be taught as an ordinary three-day training course or in order to make the training sustainable, it can be taught as a five days' train the trainer course.

Tutors: 2

Level of knowledge of attendees

This is a basic course no knowledge is necessary. The aim is to look at the basic principles, and local laws and regulations will naturally apply.

Content

- *An introduction to cybercrime trends and challenges*
- *An introduction to technological developments*
- *Digital evidence*
- *Substantive law developments / Offences*
- *Procedural law developments / Investigative measures*
- *An introduction to international cooperation*

Aims

1. To demonstrate how law enforcement (prosecutors, judges and defence advocates) and industry can deal with cybercrime and digital evidence.
2. The training will cover which substantive and procedural laws as well as technologies and international co-operation measures can be applied.
3. In order to fully understand the impact of technology on crime, it is necessary to gain an understanding of the fundamentals of cybercrime and how the technology functions.
4. In particular, in cases involving digital forensics in its broadest sense, this knowledge will provide context and enable informed decisions to be made throughout your interaction with the criminal justice system.

BE AWARE –DEPLOY EFFECTIVELY – INFORM - ADVANCE

Cybercrime and Digital Evidence Intermediate Course

Length of course: Can be taught as an ordinary three-day training course or in order to make the training sustainable, it can be taught as a five days' train the trainer course.

Tutors: 2

Level of knowledge of attendees

This is a case scenario driven practical course and attendees should have attended the 'Introduction to Cybercrime and Digital Evidence' course or an equivalent. This training builds on and allows the attendees to put into action what has been learnt in the introductory course.

Content

- *Case Scenario*
- *Developing an investigation*
- *Virtual currency*
- *Dark web*
- *Digital forensics*
- *Public private cooperation*
- *International cooperation*
- *Presenting the case in court*

Aims

1. To demonstrate law enforcement (prosecutors, judges and defence advocates) and industry involvement in a cybercrime and electronic evidence investigation.
2. It covers which substantive and procedural laws as well as technologies and international co-operation measures can be applied.
3. Discussing the dangers and possible problem that can arise when you mix the dark web with virtual currency
4. Applying international and public private cooperation cybercrime and electronic evidence problems

BE AWARE –DEPLOY EFFECTIVELY – INFORM - ADVANCE

Teaches basic knowledge regarding computers and criminal activity on the internet.

Computers and Crime

Length of course: Three days
(can be compressed into two days if necessary)

Tutors: 2

Level of knowledge of attendees

This is a basic course no knowledge is necessary. The aim is to look at the basic principles, and local laws and regulations will naturally apply. There will be hands on computer and internet demonstrations which will be completed as a class so all attendees should have laptops that can access the internet.

Content

- *Basics of computers and networks*
- *The problem with cybercrime*
- *An introduction to the internet*
- *The dark web*
- *Understanding computer forensics*
- *International and regional cybercrime law*
- *Practical evidential issues*
- *Case studies*

Aims

1. To increase knowledge and awareness of the use and impact of computers in criminal activity thus increasing the ability to identify the audit trail of a computer
2. How the existence and history of particular files can be disclosed and details of history of activity on a particular computer can be obtained.
3. This course is a basic general information course teaching a solid basic knowledge of computers, the internet and computer forensics and how criminals use computers.
4. Attendees will be able to identify issues relating to duplicity, corporate liability and jurisdiction and identify ways in which evidential problems can be avoided.

BE AWARE –DEPLOY EFFECTIVELY – INFORM - ADVANCE

International Cooperation and Cybercrime

Length of course: Three days
(can be compressed into two days if necessary)

Tutors: 2

Teaches basic knowledge of computers and criminal activity on the internet.

Level of knowledge of attendees

This is a basic course no knowledge is necessary. The aim is to look at the basic principles, and local laws and regulations will naturally apply.

Content

- *International cooperation on cybercrime*
- *Technology involved in cybercrime*
- *Mutual legal Assistance and police–to-police cooperation on cybercrime and electronic evidence*
- *Private public cooperation*
- *International agreements on cybercrime and electronic evidence*
- *Cooperation in practice*
- *Case scenarios*

Aims

1. To foster cooperation nationally, regionally and internationally as well as encourage public and private cooperation.
2. To provide an overview of the key issues and obstacles that cybercrime raises for those in the public and private arena who have to prevent or respond to it.
3. This module will also examine the borderless nature of cybercrimes, the multiplicity of jurisdictions involved, the challenges in detecting cybercrime and the difficulties in obtaining admissible evidence to support prosecutions.
4. The need for expertise and legislation in this field will also be examined.
5. Some of the solutions available to fight cybercrime will be discussed including public /private cooperation and police-to-police cooperation.

BE AWARE –DEPLOY EFFECTIVELY – INFORM - ADVANCE

The Digital Leader

Length of course: Two days

Tutors: 1

The Digital Leader training is aimed at leaders (or potential /aspiring leaders) within organisations to prepare them for leading in a Digital world. In addition to set presentations, course attendees will be tested through a number of short papers fed exercises to assist their own understanding of the digital environment.

Level of knowledge of attendees

No knowledge is necessary. This course will be of value to public, private and the third sector.

Content

Cybersecurity

- *Cybersecurity and a basic introduction to how access can be protected*
- *Personal responsibility for cybersecurity at work and at home*
- *Exploring of the risks and threats to organisations and individuals of failure in digital security*

Cybercrime

- *Cybercrime including current trends, techniques and current risk and threat*
- *Capability and capacity to help defend against cybercrime*
- *Compromised identity and the motives of cybercriminals including data loss*
- *Basic digital forensics*

Social Media

- *An examination of social media its history, context and design.*
- *Value and engagement created through social media*
- *Exploration of risk and threat particularly through the use of social media*
- *Undertaking forensic investigations into social media*

Aims

1. The aim is to equip leaders with a range of knowledge and experiences to maximise their impact as leader's / future leaders. Building on their existing skills and through presentations delivered within the course they will be able to understand and develop their use of digital skills in the workplace. The course is also aimed at senior leaders/ those who have little experience of cybersecurity, cybercrime or social media who wish to learn more in a safe environment.
2. The course will explore the many aspects of cybercrime and cybersecurity that can impact on a business or organisation and cause loss or waste.
3. It will explore the use and abuse of social media and how it can both enhance and destroy an organisation's reputation and market.
4. Attendees will leave the course having explored a range of issues against their own organisation's ethos and mission and will have been exposed to a variety of skills and techniques to help them understand cybercrime cybersecurity and social media.
5. Attendees will have a much broader view of the digital world through the knowledge and information shared, gain access to international networks and will be much better equipped for leadership in a digital world.
6. Attendees will understand how the threat risk and harm of cybercrime cybersecurity and social media impact across all sectors and partnerships.

An introduction to Live Forensics

Length of course: Three days
(can be compressed into two days if necessary)

Tutors: 1 or 2

Teaches basic knowledge of live forensics and evidence collection

Level of knowledge of attendees

This is a basic course no knowledge is necessary.

Content

- *Introduction to forensic science*
- *Evidence collection*
- *Traditional forensics*
- *Live forensics*
- *Data acquisition tools*
- *Network analysis tools*
- *Memory forensics*
- *Evidence retention*
- *Case scenarios*

Aims

1. To provide the training so that attendees can understand how live forensics can be used to collect and analysis data.
2. To provide the foundations and theoretical underpinnings for an understanding of live forensics so that data acquired is reliable and can (if required) be used as evidence.
3. This training will cover methods for the collection and analysis of digital evidence which will not alter the underlying data and which can be reproduced reliably by others.

The Zyber Global Centre is an independent cybercrime, cybersecurity, digital evidence, leadership and business consultancy that comprises of an extensive team of renown international expert consultants who have worked all over the world with various international organisations.

Esther George the Director of the Zyber Global Centre has held specialist and management positions in the public and private sector and is the lead cybercrime consultant for the Global Prosecutors E-Crime Network (GPEN) which is part of the International Association of Prosecutors.

As a consultant, Esther regularly travels abroad to train judges, prosecutors and law enforcement and has worked with organisations such as the Council of Europe, Commonwealth Secretariat and the United Nations Office of Drugs and Crime.

Previous roles offered Esther the opportunity to work as a Senior Policy Advisor and Senior Prosecutor based at the Crown Prosecution Service (CPS) HQ Policy Directorate, London, UK, where she specialised in internet and computer enabled crime, digital evidence, intellectual property crime and data protection, offering her advice to prosecutors at all levels within HQ and Area CPS offices, police and other Government bodies. Esther was also the project manager for the CPS High-Tec Crime Project during which she developed and designed the CPS national high-tec crime training course for prosecutors, resulting in over 200 cybercrime specialists for the CPS.

Esther has presented challenges and issues concerning cybercrime at conferences and training sessions in the United Kingdom and globally in countries including Australia, Azerbaijan, Bahrain, Barbados, Bermuda, Canada, China, Croatia, Czech Republic, Estonia, France, Georgia, India, Indonesia, Japan, Malaysia, Malta, Mauritius, Morocco, Netherlands, Nigeria, Philippines, Portugal, Republic of Ireland, Romania, Singapore, South Africa, South Korea, Spain, Sri Lanka, Tonga, Turkey, and the UAE.

Esther initiated and designed the Global Prosecutors E-Crime Network (GPEN) which enables cybercrime prosecutors around the world to learn and benefit from sharing information, experiences, and strategies with each other, resulting in enhanced international cooperation. In 2010 Esther was awarded the Certificate of Merit from the International Association of Prosecutors for being the Architect of GPEN.