Continuing Education Programme

on

Cyber Security, Cyber Crimes and Cyber Laws

Name of the Proposer: Anil K. Roy and Manik Lal Das

Other Instructors: arranged by CLS, Ahmedabad

Course Objectives:

Information technology has enhanced the communication and has facilitated the growth of trade and commerce. The technology has fastened the e-commerce, m-commerce, e-Governance, net banking, mobile banking, online share trading and other commercial transactions. Cyber Criminals carry out online frauds and other criminal activities such as financial frauds, online defamation, data theft, obscenity, online pornography, phishing and violence etc. The biggest advantage for the offenders committing online crimes is that they can remain anonymous. The regulatory and related technology sphere is still in a nascent stage and continuously evolving every passing day. This objective of this program is to share knowledge of cybercrime, ethical hacking, cyber security, cyber forensics & cyber laws amongst students as well as professionals of various backgrounds such as Engineering, Law, IT, Computer Applications, Management, Commerce, Arts and other disciplines.

The overall goals of this CEP are as under:

- To facilitate understand & critical understanding about Cybercrimes, Ethical Hacking, cyber security, forensics and cyber laws
- Exploration of the legal and policy developments in various countries for cyber space
- To provide in-depth knowledge of Information Technology Act, 2000 including Information Technology Amendment Act, 2008
- Understanding e-Governance, Electronic Contracts, e-Banking & Secure electronic records
- To share knowledge of the regulation of cyber space at national and international level

- To train and prepare candidate to consider Cyber security, forensics and cyber laws as a career option.

Course Duration: Start date: 19 June 2016**; End date:** 24 July 2016

We wish to run it as a weekend program (only on Sundays – 6 hours) for 1.5 months, as we feel it would be helpful for professionals to participate in this program in weekends instead of taking leave from their day-job and remain away for a week or two.

Target Audience:

This course is meant for everyone who uses computers, smart phones, tablets and Internet. Prior knowledge of either law or technology is NOT mandatory.

The said program is open to students as well professionals from various backgrounds like HSC/B.E./B.Tech./BCA/MCA/M.Sc.(IT)/LLB/LLM/CS/ICWA/CA/MBA/BBA/ PGDCA/B.Com./M.Com./B.A./ Diploma Programs/any other disciplines in India.

Fees:

Application Charges: Rs. 150/-

Course Fees: Rs. 10,000/-

Tentative Course Content:

A. Cyber Crimes

- Data diddling
- Data leakage
- Eavesdropping
- E-mail forgery
- E-mail threats
- Internet misinformation
- Internet terrorism
- Password cracking
- Round downs
- Salami Techniques
- Scavenging/Corporate Espionage

- Social Engineering
- Software Piracy
- Spamming
- Super zapping
- Piggybacking
- Trap door
- Trojan Horse
- Virus
- Worm
- Impersonation
- Time bomb
- Logic bomb
- DOS Attacks

B. Ethical Hacking & Cyber Security

- Email Hacking & its security
- Social Media Hacking & its Security
- Web Hacking & its Security
- Mobile Hacking & its Security
- Fake Calls, fake SMS & its Security
- Wi-Fi Network Hacking & its Security
- Windows Hacking & its Security
- DDOS Attack & its Security
- Software Hacking & Reverse Engineering
- Cross site scripting & its Security
- Basics of cryptography, Encryption & Decryption
- Security breaches case studies
- Categorization of Digital Security
- Multimedia Security (Steganography)
- Malware Concepts (Virus, Worms, Trojan etc.)
- Firewall & IDS/IPS Concepts
- Basics of Vulnerability Assessment & Penetration Testing
- Spying & Cyber Reccy

- Email forgery and E-mail Tracing

C. Cyber Laws

- Introduction to Information technology & Cyber Law
- Basics of E-commerce and Computer Fraud Techniques
- Cyber Security Fundaments, Techniques and Core Principles
- Cyber Space, Technology & Issues
- Regulating Cyber Space: International
- Regulating Cyber Space: National
- E-contract & Electronic Data Interchange
- E-signature and E-governance legality under I.T.Act, 2000
- Cyber Contraventions, Compensation & Crimes under I.T.Act, 2000
- ISPs and Websites Legal Liability under I.T.Act, 2000
- Corporate Legal Liability under I.T.Act, 2000
- Adjudication Process For Recovery of Losses under I.T.Act, 2000
- Case Studies and Case Laws

D. Cyber Forensics

- Forensic Imaging & Storage Media Duplication (FTK Imager)
- Windows Forensics Artifacts (Nirsoft/SysInternals)
- Various Case Studies
- Data Recovery (TestDisk/PhotoRec)
- Forensic Investigation of Image (Autopsy)
- Malware Analysis (Static/Dynamic)
- DEFT OS
- Social Media Forensics (FB/Twitter/LinkedIn etc.)
- Multimedia Forensics (JPEGSnoop/ImageHeader Analysis)
- File Header Analysis, Office Files Analysis (FOCA), File Signature
- Smart Phone Forensics (AFLogical, ViaForensics, MobileEdit)
- Timeline Analysis (Event Log Analysis)
- Registry, NTUSER.DAT, USERCLASS.DAT Analysis (Regedit, FRAT, Scripts)
- RAM Forensics (Concepts & Artifacts Analysis)

Lab: There will be adequate hands-on sessions, which will get mapped to lecture sessions.

Collaboration with *CLS- Cyberra Legal Services*

Founded in Ahmedabad in 2003, Cyberra Legal Services is a premier organization in cyber law advisory services, cyber security consulting, training and education. It is the first of its kind of service venture in Gujarat with Key Personnel who are Technology Graduates, Law graduates, Ethical Hackers having specialized in cyber laws. CLS serves its various clients in five cities namely Ahmedabad, Gandhinagar, Baroda, Rajkot and Delhi. CLS, in association with Manan Thakker & Associates (Advocates & Cyber Law Consultants), have filed highest number of cyber fraud compensation matters in the state of Gujarat March, 2016. CLS's key person is appointed as a member in Cyber Security Consultant Selection Committee, GIL, Govt. of Gujarat and Cyber Security Committee of Raksha Shakti Universtiy. CLS also holds membership in GESIA and CII (IWN).

Certification:

The candidates will be evaluated for maximum of 100 marks for which one MCQ (Multiple Choice Questions) Open Book Exam will be conducted on the last Sunday of program. The candidate needs to score at least 40% marks to complete the course and get the certificate.

How to Apply

The application form can be downloaded from **www.cyberralegalservices.com** or **obtained it from the next page.**

You may also write to Program Coordinator on cep_cybersecurity@daiict.ac.in

Alternatively, candidate should write "Certificate Program on Cyber Crime, Ethical Hacking, Cyber Security, and Forensics & Cyber Laws" on the envelope containing Application and send it to below address.

Contact

Ms. C M Thakker (Advocate & Cyber Law Advisor)
Address: CLS - 2nd Floor, Asha Complex,
Bh. Navarangpura Police Station, Navarangpura,
Ahmedabad – 380009 (Gujarat)
M: +91 095101 22995
Landline: 079- 400 300 31
Email: cep_cybersecurity@daiict.ac.in

APPLICATION FORM

Name (in block Letters) _____

Date of birth (d/m/y): _____ age: _____sex: _____

Father's name (in block letters): _____

Phone no: _____, email id: _____

Address for correspondence: _____

_____

_____

Permanent Address: _____

_____

_____

College/university: _____

Qualification: _____

Name of Company:_____ Job Designation:_____

Fee Details: DD no:……Date:……Bank name:…….....

Signature of the
applicant:……Place……Date:……..……..…..

Documents to be attached:

(i) Testimonials of your course (e.g. Mark-sheet/Certificate)
(ii)One Passport photo.

Send the form along with other documents to

Ms. C M Thakker (Advocate & Cyber Law Advisor)
Address: CLS - 2nd Floor, Asha Complex,
Bh. Navarangpura Police Station, Navarangpura,
Ahmedabad – 380009 (Gujarat)
M: +91 095101 22995
Landline: 079- 400 300 31
Email: cep_cybersecurity@daiict.ac.in

SCHEDULE (tentative)

WEEK 1 (19th June 2016):

Module A1: Cyber Security basics (2 hours)

- Security threats, vulnerabilities and attacks
- Confidentiality, Integrity, Availability (CIA) triad
- Network security basics – client server, peer-to-peer, adhoc, and mobile scenarios.
- System Security overview – access control, logs

Module B1: Cyber Forensics basics (2 hours)

- Forensic Imaging, Storage Media Duplication (FTK Imager)
- Windows Forensics Artifacts (Nirsoft/SysInternals)
- Case Studies

Module C1: Cyber Crimes & Laws (2 hours)

- Popular cybercrime techniques
- Cyber Contraventions & Compensation under I.T. Act, 2000
- Corporate Legal Liability under I.T. Act, 2000
- Adjudication Process for Recovery of Losses under I.T. Act, 2000
- Case Studies and Case Laws

WEEK 2 (26th June 2016):

Module A2: Security primitives & properties (2 hours)

- Various Security primitives (symmetric/asymmetric key)
- Platform and Application security and security properties
- Email security – S/MIME, Pretty Good Privacy
- Case studies, hands-on practice, or demonstration

Module B2: Image and Data Forensics (2 hours)

- Forensic Investigation of Image (Autopsy)
- Data Recovery (TestDisk/PhotoRec)
- Case studies, hands-on practice, or demonstration

Module C2: Cyber Crime & Cyber Laws (2 hours)

- Computer Fraud Techniques
- Cyber Crimes and consequences under I.T. Act, 2000
- Cyber Space, Technology and Issues
- E-contract & Electronic Data Interchange

WEEK 3 (3rd July 2016):

Module A3: Cyber Security and Ethical Hacking-1 (3 hours)

- Online security, Certification, PKI (TLS, SSH)
- SQL injection, Cross-site scripting
- Email Hacking & its security
- Social Media Hacking & its Security
- Web Hacking & its Security

Module A4: Cyber Security and Ethical Hacking-2 (3 hours)

- Mobile Security – Android, GSM security
- Mobile Hacking & its Security
- Fake Calls, fake SMS & its Security
- Wi-Fi Network Hacking & its Security
- Case study, hands-on practice, or demonstration

WEEK 4 (10th July 2016):

Module B3: Media Forensics (2 hours)

- Digital Evidence & Forensic Toolkit (DEFT)
- Social Media Forensics (FB/Twitter/LinkedIn etc.)
- Multimedia Forensics (JPEGSnoop/ImageHeader Analysis)
- Case studies, hands-on practice, or demonstration

Module B4: Cyber Forensics (2 hours)

- File Header Analysis, Office Files Analysis (FOCA), File Signature
- Timeline Analysis (Event Log Analysis)
- Case study, hands-on practice, or demonstration

Module C3: Cyber Crime & Cyber Laws

- E-signature and E-governance legality under I.T. Act, 2000
- ISPs and Websites Legal Liability under I.T. Act, 2000
- Regulating Cyber Space: International
- Regulating Cyber Space: National

WEEK 5 (17th July 2016):

Module A5: Cyber Security and Ethical Hacking-3 (3 hours)

- Perimeter security – Firewalls, Routers, Bridges, IDS/IPS
- Data storage, Data leakage – security and privacy implications
- Access control and Trust management
- Basics of Vulnerability Assessment & Penetration Testing

Module A6: Cyber Security and Ethical Hacking-4 (3 hours)

- Windows Hacking & its Security
- Email forgery and Email tracing
- Cyber Spying
- DDOS attack & countermeasures
- Software Hacking & Reverse Engineering

WEEK 6 (24th July 2016):

Module B5: Digital Forensics and Malware Analysis (2 hours)

- Smart Phone Forensics (AFLogical, ViaForensics, MobileEdit)
- Malware Analysis (Static/Dynamic)
- Timeline Analysis (Event Log Analysis
- Case study, hands-on practice, or demonstration

Module B6: Digital Forensics (2 hours)

- Registry, NTUSER.DAT, USERCLASS.DAT Analysis (Regedit, FRAT, Scripts)
- RAM Forensics (Concepts & Artifacts Analysis)
- Case study, hands-on practice, or demonstration

Module C4: Information Assurance and Risk Management (2 hours)

- Basics of ISO 27001
- IT Risk Management
- Security policy, compliance, standards
- IPR issues on Internet
- Disaster recovery planning, Business continuity planning

Examination: MCQ Pattern (1 hour)