Decision Group would like to announce the new training class on "The Escalation of Modern CyberWarfare" featuring Dr. Ying-Chiang Cho. This New training class will be included in our Cyber Crime Investigation Course. This training class will highlight the recent shutdown of Sony Pictures by computer hackers, and what this means for the future of the internet and new requirements for international cybersecurity. The theoretical underpinnings of cyberwarfare will be addressed, as well as the tactical activities that comprise both offense and defense in cyberspace. Known strategies of cyberattack will be covered, as well as proven strategies for protecting cyberinfrastructure.

Ying-Chiang Cho is an Assistance Professor with the Advanced Network Technology Laboratory Department of Electrical Engineering, National Chung Cheng University, Chia-Yi, Taiwan, R.O.C. Dr. Cho has a PhD of Electronic Engineering from National Chung Cheng University and he is an expert on Network Security and Data Mining techniques.

The Escalation of Modern CyberWarfare

OUTLINE

1. Introduction to Computer Hacking
2. Recent Incidents – the Sony Pictures Shutdown
3. What Is Cyber Warfare?
4. The Realities of International CyberWarfare
5. CyberWarfare at the Theoretical Level
6. CyberWarfare at the Technical Level
7. CyberAttack Strategies in Action
8. Defending Against CyberAttacks
9. Recognizing CyberWarfare in Practice
10. Conclusion – CyberWarfare is the Future, and the Future has Arrived

Introduction of Cyber Crime Investigation Course from Decision Group

Combined with theory and real practice of case study, this program will provide you lot of information on cyber crime investigation by 4 aspects:

Cyber Crime: New Challenge to Mankind Society

** Introduction to the Nature of Cyber Crime and its Investigation Process

The Nature of Cyber Crime: 1. Cyber Fraud 2. Procedure of Lawful Investigation on Cyber Crime 3. Case Study on Internal Threat and 4. Information Security Issues

The purpose of this program is to give all attendees a clear picture of the nature of cybercrimes and how to investigate such crimes with new technology and procedures. Since new cybercrimes arise by a leap of development of telecommunication and information technologies, investigators must face such challenges with creative reasoning and technical skills.

We provide this training program not only with newly developed technologies and skills, but also, with case studies on the methodology to apprehend such cybercrimes in real-world environments by experienced cybercrime investigators. Attendees, after taking this training program, will understand the basics of cybercrime, effective ways to investigate it, and most important, first-hand lessons from real-world cases.

1. The Nature of Cyber Crime

The most distinct nature of cyber crime from traditional one is borderless and anonymous. By the help of pervasive network technology, cyber crime is ramping over areas, regions, and countries. For investigators, it is really hard to get the true picture of the whole crime process because of dispersed elements in different places. In this session, we will present the true profile of cyber crime in terms of process, technology behind, behavior model and mind set. Dr. KC Wu is emeritus professor in Department of Information Technology, National Central Taiwan University, and has full experience and study on development of information technology in crime.

2. Cyber Fraud

Cyber Fraud is the most common and significant type of crime, and cover versatile facets, such as fraud in cyber auctions, VoIP phishing, identity stealing, ...etc. In this session, we will present you with different types of real-world cybercrime cases, how it happens, and profiling the criminals. The most important point of the course is that we will give you a better understanding of cyber fraud and their weaknesses. You may easily find the crime model when you deal with cyber fraud, know how to investigate it, and keep all evidence legally valid. Richard Chuang is Chief of the Cybercrime Prevention Squad in the Criminal Investigation Bureau of the Taiwan National Police Agency, and had led many investigations in cybercrimes for the past 5 years.

3. Procedure of Lawful Investigation on Cyber Crime

After investigating a cybercrime, collecting all the evidence, and preparing to submit the evidence to the court, are you sure that all the evidence in your hand is valid and legal? Without a lawful procedure in the cybercrime investigation, your effort will be fruitless. In this session, you will learn the formal investigation procedures in cybercrime, its difference from legacy crimes, and legal requirements of evidence in the court. Dr. Chien is the expert in this field, and has also published several research papers on this topic.

4. Case Study on Internal Threat and Information Security Issues (Case Study Exsample)

In the previous sessions, we covered cybercrime in many different aspects, but most of the cybercrimes we mention were external threats. Cybercrime from internal threats will be presented in-depth in this session. Traditionally this kind of cybercrime has been neglected by the public. We will highlight it with many case studies and show how to deal with it. With much experience and academic accomplishments, Dr. DG Kao will give a detailed understanding on internal cybercrime, how to prevent, and how a law enforcement agency can collect evidence for a lawsuit in the court.

In this training program, a certificate will be presented after passing the qualification process. The recipient will have the knowledge and skill to investigate cybercrimes.

Please check out more information on http://www.edecision4u.com or contact with us at decision@decision.com.tw
Thank you very much!
.....................*^_^*............
Thank you and best regards,
Casper Kan Chang / Group CEO
DECISION GROUP
Email: decision@decision.com.tw;
Tel.+886-2-2766-5753; Fax.+886-2-2766-5702;
www.edecision4u.com

Decision Group Inc.

Cyber Crime Investigation Training Program by Decision Group

WHY TO LEARN

Cohost with National Taiwan Central Police University

Understand the nature of cyber crimes, how to take effective investigation by high tech equipment with appropriate skills, administrative and legal procedure for conducting cyber crime investigation, and data analysis.

WHO SHOULD ATTEND

Staff of Law Enforcement Authority and Intelligence, Corporate IT Security Officers and Auditors.

WHAT TO LEARN

This course will cover the topics as following:

1. Introduction to Digital Forensics
2. Cyber Investigation on Cyber Fraud Crimes from Telecom
3. Cyber Investigation on Cyber Fraud Crimes from Internet
4. Vulnerability of ICT Systems for Criminals
5. Data Analysis for Crime Investigation
6. Legal Procedure for Cyber Crime Investigation and Digital Evidence Collection
7. Digital Evidence Presentation and Report
8. Case Study and Workshop
9. Seminar and Panel Discussion with Senior Field Cyber Inspectors in Taiwan Crime Investigation Bureau

WHO ARE SPEAKERS

They are senior inspectors from Cyber Investigation Team of Taiwan Police Department with more than 10-year experience, and professors from National Taiwan Central Police University

HOW LONG
5 WORKING DAYS

LANGUAGE
ENGLISH

FURTHER INFORMATION
www.edecision4u.com

CONTACT : decision@decision.com.tw