Digital Evidence, Fraud & Security

Identifying and managing the hidden electronically stored information as potential evidence

3 & 4 November 2008 ♦ Grand Millennium Kuala Lumpur, Malaysia

MgDelxis "Anti-Fraud" Week, 3 - 7 November 2008 ♦ Contact Us Now for Group Discount!

Platform Facilitator:

Mr. Seamus E. Byrne

COO

eDiscovery Tools

"An international lawyer with extensive forensic technology and electronic discovery experience"

In conjunction with MgDelxis "Anti-Fraud" Week, we have invited a panel of experienced fraud specialists to facilitate the "Corporate Fraud Risk Management" Series:

- *"Digital Evidence, Fraud & Security" on 3 & 4 Nov*
- *"Forensic Interviewing Techniques" on 5 Nov*
- *"Forensic Financial Statements" on 6 & 7 Nov*

'Societe Generale lost $7 billion in trading fraud.
The trader had "breached five levels of controls" and was "a computer genius". According to SG officials, the trader hid his unauthorized transactions by using his colleagues' computer access codes and falsifying emails and other documents. He was able to dodge internal monitoring systems with his knowledge gained from working for five years on the bank's security systems.'

If you are the first responder at the above digital crime scene, how do you identify "potentially relevant" sources of digital evidence? How do you preserve and collect the evidence in a forensically acceptable manner? What do you do in a forensic data analysis? How do you prepare a digital forensic report for internal use and for the Court and provide expert testimony?

As corporate fraudsters continue to embrace the electronic age, IT professionals are increasingly encountering situations where they are required to proactively identify and manage forensic investigations involving digital evidence. IT professionals need to know what to do when they encounter potential digital evidence and how best to collect and preserve such information so as to allow it to be forensically examined at a later stage by a professional forensic examiner.

Capitalise on international digital forensic expert's knowledge to gain practical insights into the vital issues:

- Role of Digital Forensic in relation to Information Technology
- Planning a Digital Forensic Investigation
- Identifying and Collecting Digital Evidence
- Forensic Data Analysis
- Digital Evidence and the Law
- Forensic Report Preparation and Court Presentation

This practical platform combine with interactive demonstration of the latest tools will enhance your knowledge of how to successfully conduct digital forensic investigation within your organization. Mr. Byrne will also cover the relevant laws within South East Asia region.

Involving a mixture of case studies, scenario exercises and breakout sessions, this platform is a must for IT auditors, fraud and security personnel, risk specialists, legal counsels and any professional encountering digital evidence during the course of an investigation.

Organized by: MgDelxis

To register, please contact MgDelxis Group at:
Tel: +65 6841 1379 Fax: +65 6841 6343 Email: registration@mgdelxis.com
www.mgdelxis.com