

TECHNOLOGY TRANSFER PRESENTS

EOGHAN **CASEY**
DARIO **FORTE**
LUCA **DE GRAZIA**

COMPLIANCE AND AUDIT

MANAGERIAL AND LEGAL ISSUES

OF HANDLING SECURITY BREACHES

ROME NOVEMBER 24 2008

NETWORK

INVESTIGATIONS AND

INCIDENT RESPONSE

ROME NOVEMBER 25-28 2008

VISCONTI PALACE HOTEL - VIA FEDERICO CESI, 37



info@technologytransfer.it
www.technologytransfer.it

ABOUT THIS SEMINAR

It is fundamentally important for an organization to prepare for severe Security Breaches of their computer Networks. Understanding the implications of, and appropriate responses to, such breaches are necessary to reduce the harm to employees, clients and customers whose data may be at risk and to ensure that the same perpetrator does not strike again. In addition, financial institutions and telecommunications companies are required to preserve certain data for regulatory purposes.

In this seminar you will learn about managerial and legal aspects of preparing for, and dealing effectively with, Network Security Breaches. The instructors have extensive experience conducting the digital investigations and have worked with many organizations to enhance their incident response and Digital Forensics capabilities. This seminar is suitable for Compliance officers and auditors in your organization, as well as managerial and technical personnel who are responsible for handling critical incidents. Legal issues impacting organizations in Italy and throughout Europe are presented and discussed in the context of Case Studies. For maximum benefit, it is recommended that organizations have representatives from internal audit, legal, and IT also attend the technical Network Investigation and Incident Handling hands-on workshop to help them work together on security incidents, teaching each group what is needed by the other.

Topics covered include:

- Forensic readiness in a large organization
- The role of Audit and Compliance in Forensic preparedness
- Managing a complex Network investigation
- Incident response life cycle and investigative methodology
- Conducting an internal investigation without breaking the law
- Overview of relevant Italian legislation and EU directives
- How to manage reporting and notification obligations
- Involving law enforcement to apprehend offenders
- The importance of having a data map

SPEAKERS

Eoghan Casey, Dario Forte, Luca de Grazia

ABOUT THIS SEMINAR

Digital Forensics is becoming an integral part of information assurance, enabling organizations to handle Security Breaches, policy violations and legal compliance preservation obligations more effectively. Whether your organization is faced with employee malfeasance, computer intrusions, civil disputes or government and regulatory inquiries, you need to know where to find digital evidence on your Network and how to preserve and utilize it.

In this technical workshop you will learn to prepare for, and deal effectively with, severe Security Breaches that result in the exposure of sensitive data. This workshop is suitable for individuals who are interested in or are already performing technical aspects of digital investigations in your organization. This technical workshop will also be of interest to managers, lawyers, compliance officers, and auditors who need to understand the types of digital evidence that is available on computers. Hands-on investigative scenarios and exercises are used throughout this workshop to teach practical technical skills and to help IT managers, lawyers, internal auditors, compliance officers, and technical staff. Using actual data, including memory dumps and Network logs, attendees will learn the wide range of skills needed to preserve and analyze volatile digital evidence when Networks are compromised and sensitive data are exposed. Procedures and tools for properly collecting and examining volatile digital evidence from high-availability systems and Networks are covered. Additionally, state of the art Forensic Analysis techniques and associated tools are presented, and the value of correlating Network-level evidence from IDS systems, Firewall, and other Network devices and monitoring systems is demonstrated through investigative exercises and Case Studies. All attendees must bring a laptop computer running Microsoft Windows to perform hands-on exercises. In this manner, you will learn the strengths and weaknesses of various Forensic tools and techniques, improve your ability to manage a complex investigation, and develop the necessary skills to preserve, analyze evidence and combine data from multiple sources in an organization. Furthermore, for maximum benefit, it is recommended that organizations have representatives from each of these groups attend this seminar, including internal audit, legal, and IT.

Topics covered include:

- Forensic examination of live systems
- Preservation and examination of memory contents
- Remote Forensic examination and acquisition
- Detailed analysis of compromised systems
- Safe inspection of Malware
- Best Practices for handling digital evidence on Networks
- Network traffic as a source of evidence
- Using logs on a Network as evidence
- Forensic examination of Network devices
- Network correlation and reconstruction
- Court admissibility of live analysis
- Using the Internet as an investigative tool
- Building a solid case

Team exercises and instructor demonstrations will help you develop the skills to process evidence on remote computers, and combine data from multiple sources on a Network to develop a more complete understanding of an incident. In addition, you will learn about important legal issues relating to Network monitoring and covert internal investigations.

SPEAKERS

Eoghan Casey, Dario Forte

EOGHAN CASEY

Eoghan Casey is one of the leaders in the field of Digital Forensics and high-technology crime investigations. He co-manages the firm's technical operations in the areas of computer forensics, cyber-crime response, incident handling, and electronic discovery. He maintains an active docket of cases himself and has extensive experience managing complex investigations and preserving, harvesting, and analyzing relevant digital evidence. He has performed hundreds of Forensic acquisitions and examinations, including e-mail and file servers, handheld devices, backup tapes, database systems, and Network logs. He has regularly applied Digital Forensics in response to Security Breaches to determine the origin, nature and extent of computer intrusions and has utilized Forensic and security techniques to secure the affected Networks. He is the author of the widely used text book "**Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet**", now in its second edition. He is also editor of the "**Handbook of Computer Crime Investigation: Forensic Tools and Technology**", and co-author of "**Investigating Child Exploitation and Pornography: The Internet, The Law, and Forensic Science**" and "**Malware Forensics: Investigating and Analyzing Malicious Code**".

DARIO FORTE

Dario Forte, CFE, CISM, is Security Advisor for the newly-formed European Electronic Crimes Task Force (EECTF) supported by the U.S. Secret Service in Milan. He has been active in the field of information security since 1992. He is 34 years old, with almost 15 years as Police Investigator in the Drug and Organized Crime Enforcement, CyberCrime Unit. Mr. Forte is a Member of the Computer Security Institute of San Francisco/USENIX and Sage, publishing technical articles all over the world while contributing at numerous international conferences on Information Warfare, including the RSA Conference Europe, the Computer Security Institute NETSEC, Computer Associates CAWorld and the Digital Forensic Research Workshop. He teaches classes and presents lectures on Information Security Management and Incident Response/Forensics at universities and other accredited institutions worldwide. He is an Intrusion Instructor for the Department of Homeland Security Internet Forensics Training Program given at the Federal Law Enforcement Training Center. For more than 10 years, Mr. Forte has worked with many government agencies worldwide including NASA, and the U.S. Army/Navy, supporting them in incident response and Forensics procedures while solving many important hacking-related investigations. Now he provides security/incident response and Forensics consulting to the Government, Law Enforcement and corporate world and is also involved with InfoSec projects at the international level.

LUCA DE GRAZIA

Luca de Grazia, Italian Supreme Court Lawyer, DFLabs consultant on national compliance matters. Considered one of the top Italian experts in Legal Compliance, de Grazia looks after the company's highest projects. He is the author of numerous scientific publications and presentations delivered at both legal and computer science conferences. Together with Dario Forte, he co-wrote "**Handbook of Infosecurity Management**", the first Italian book dealing with topics like Information Security Management.

OUTLINE

1. Legal Implications of Security Breaches

- Legal framework for Security Breaches
- “E-privacy” 2002 EU directive
- “Data Retention” directive (2006/24/EC)
- Italian legislative decree 259/2003
- Italian law (196/2003, 231/2001)
- Italian legislative decree no. 155 27 July 2005

2. Digital Forensics and IT Security Management

- Forensic preparations for Security Breaches
- The role of Forensics in IT Governance
- The role of Audit and Compliance in Forensic preparedness
- Forensic issues relating to COBIT and ISO/IEC 17799
- Balancing Forensic needs with Business goals
- Enterprise Architecture implications
- Data storage and disposal considerations (encryption, backup tapes)
- Metrics for tracking progress and Compliance
- Policy, procedure, and disaster recovery implications

3. Managing Security Breaches

- Digital Forensic Best Practices for a Security Breach
- Limiting the cost and disruption of Security Breach investigations
- The importance of having a data map
- Legal pitfalls of internal investigations
- Governance and audit of internal digital investigations
- Oversight and segregation of Forensic duties in an organization
- How to manage reporting and notification obligations
- Involving law enforcement to apprehend offenders
- Security Breach Case Studies

OUTLINE

1. Overview

- Anatomy of a Security Breach
- Investigating theft of data
- Hacker tools and techniques
- Data extrusion examples
- Network Investigations methodology

2. Live Host Analysis

- Isolating the subject system
- Remote Forensic inspection and acquisition
- Extracting volatile data
- Analyzing memory contents
- Assessing exposure of sensitive data

3. Windows Intrusions

- Windows Security Breach example
- Processes, log files, and state tables
- Detailed examination of live Windows systems
- Reconstructing theft of valuable information
- Investigative exercise

4. UNIX Intrusions

- UNIX Security Breach example
- Processes, log files, and state tables
- Commands and tools for examining live UNIX systems
- Challenges collecting evidence of intrusions
- Investigative exercise

5. Memory Forensics

- Memory structures on Windows and Linux systems
- Tools for examining memory dumps
- Utilizing memory dumps in Security Breach investigations
- Hands-on analysis of memory dump

6. Utilizing Evidence on Networks

- Best Practices for handling digital evidence on Networks
- Review of Network protocols
- Network traffic as a source of evidence
- Recovering stolen data from Network traffic
- Intrusion Detection Systems as evidence
- NetFlow and Argus
- Network Forensic Analysis Tools

7. In-depth Forensic Analysis on Networks

- Correlation of host and Network activities
- Using logs on a Network as evidence
- Network correlation and reconstruction
- Reconstructing data extrusion
- Forensic examination of Network devices
- Automated and dynamic modus operandi
- Crime scene characteristics

8. Malware Forensics

- Safe test lab considerations
- Static analysis tools and techniques
- Dynamic analysis tools and techniques
- Malware case example

9. The Internet as an Investigative Tool

- Picking up the scent of an intruder
- Remote information gathering
- Tracking tools and techniques
- Remote evidence gathering
- Case examples with combined searching of Web, Usenet, and IRC

10. Building and Presenting a Solid Case

- Court admissibility of live analysis
- Behavioral analysis and profiling
- The role of private investigators
- Performing experiments and testing
- Presenting technical findings
- Structure and format of complex reports
- Qualifying conclusions

WHO SHOULD ATTEND

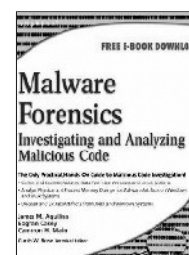
IT Managers and technical Staff, Lawyers, Compliance Officers, Internal Auditors

Required Equipment

Laptop computer with CD-ROM and network card.

DOCUMENTATION

Attendees will receive copies of these two books by *Eoghan Casey*: **Digital Evidence and Computer Crime** 2nd Edition and **Malware Forensics**.



INFORMATION

<p>PARTICIPATION FEE</p> <p>Compliance and Audit € 700</p> <p>Network Investigations and Incident Response € 2000</p> <p>Special price for the delegates who attend both seminars € 2500</p> <p>The fee includes all seminar documentation, luncheon and coffee breaks.</p> <p>VENUE</p> <p>Roma, Visconti Palace Hotel Via Federico Cesi, 37 Rome (Italy)</p> <p>SEMINAR TIMETABLE</p> <p>9.30 am - 1.00 pm 2.00 pm - 5.00 pm</p>	<p>HOW TO REGISTER</p> <p>You must send the registration form with the receipt of the payment to: TECHNOLOGY TRANSFER S.r.l. Piazza Cavour, 3 - 00193 Rome (Italy) Fax +39-06-6871102</p> <p>within November 10, 2008</p> <p>PAYMENT</p> <p>Wire transfer to: Technology Transfer S.r.l. Banca Intesa Sanpaolo S.p.A. Agenzia 6787 di Roma Iban Code: IT 34 Y 03069 05039 048890270110</p>	<p>GENERAL CONDITIONS</p> <p>GROUP DISCOUNT</p> <p>If a company registers 5 participants to the same seminar, it will pay only for 4. Those who benefit of this discount are not entitled to other discounts for the same seminar.</p> <p>EARLY REGISTRATION</p> <p>The participants who will register 30 days before the seminar are entitled to a 5% discount.</p> <p>CANCELLATION POLICY</p> <p>A full refund is given for any cancellation received more than 15 days before the seminar starts. Cancellations less than 15 days prior the event are liable for 50% of the fee. Cancellations less than one week prior to the event date will be liable for the full fee.</p> <p>CANCELLATION LIABILITY</p> <p>In the case of cancellation of an event for any reason, Technology Transfer's liability is limited to the return of the registration fee only.</p>
--	---	--

CASEY, FORTE, DE GRAZIA

COMPLIANCE AND AUDIT
MANAGERIAL AND LEGAL ISSUES
OF HANDLING SECURITY BREACHES

Rome November 24, 2008
Visconti Palace Hotel - Via Federico Cesi, 37
Registration fee: € 700

**NETWORK INVESTIGATIONS
AND INCIDENT RESPONSE**

Rome November 25-28, 2008
Visconti Palace Hotel - Via Federico Cesi, 37
Registration fee: € 2000

BOTH SEMINARS

**Special price for the delegates
who attend both seminars: € 2500**

If anyone registered is unable to attend, or in case of cancellation of the seminar, the general conditions mentioned before are applicable.

first name

surname

job title

organisation

address

postcode

city

country

telephone

fax

e-mail



Stamp and signature

Send your registration form with the receipt of the payment to:
Technology Transfer S.r.l.
Piazza Cavour, 3 - 00193 Rome (Italy)
Tel. +39-06-6832227 - Fax +39-06-6871102
info@technologytransfer.it
www.technologytransfer.it

