

# **Understanding & Preventing Electronic Fraud**

**COURSE DURATION:** 2-days

**CPE HOURS:** 16

**LEVEL:** Beginner / Group-Live

**PREREQUISITES:** None

**ADVANCE PREPARATION:** None

Electronic fraud is one of the best-kept secrets of modern business. While it is constantly occurring, most organizations cover up electronic fraud, absorb the loss as a cost of doing business and move on. This not only increases the cost of doing business, but it ensures that the perpetrators can continue their activities, moving from one target to the next without fear of being apprehended, let alone a conviction. If they are caught, the faulty security and shoddy controls enable the defense lawyers to create reasonable doubt. If E-business is to survive, E-fraud and theft must be stopped. It is time to draw the line in the sand and this course will help you do just that.

The instructor will provide the participants with an understanding of the types of E-fraud, how to detect it and how to prevent it. The participants will learn the need for network, application, and server security, as well as the need to build fraud sniffers, monitors, and surveillance applications. They will also learn how to convince management that strong controls must be in place to enable successful apprehension and prosecution of E-fraud cases.

## **WHO SHOULD ATTEND**

This seminar is intended for auditors, security officers, loss prevention officers, and business unit managers. There are no prerequisites.

## **SEMINAR OUTLINE**

### **I INTRODUCTION**

- What is electronic fraud
- Types of electronic fraud

### **II UNDERSTANDING HOW E-FRAUD OCCURS**

- Network penetration
- Traps and other cyber surveillance techniques
- Compromised record management services
- Compromised cards, accounts, etc.
- Wireless LAN connections

### **III HARVESTING THE REQUIRED DATA**

- Internet banking approach
- VPN approach
- Application defaults approach
- Gas station and retail outlet approach
- Vendor application flaws
- 401K approach
- ERP, CIS, billing systems
- Purchase and use of "Spy Gear"
- E-mail approach

### **IV MOVING THE FUNDS**

- Wire and funds transfer systems

- Cash concentration systems
- Setting up "real" business entities
- "Milking" Internet bank accounts
- Defeating fax back and other confirmation systems
- Using refunds and credits to access cash

### **V PREVENTION THROUGH NETWORK SECURITY**

- Network vulnerability assessment
- Identifying breach points
- Network device security
- Network monitors
- Honey pots
- Intrusion detection systems
- Automated alerts

### **VI PREVENTION THROUGH SERVER SECURITY**

- User and account security procedures
- Windows operating systems
- UNIX and Novell
- AS/400 and Mainframes

### **VII PREVENTION THROUGH APPLICATION SECURITY**

- Vendor default installations
- Transaction risk analysis

- Identifying and eliminating fraud prone practices
- Automated alerts
- Transaction delay and approval
- Audit software
- Identifying unusual trends

### **VIII PROSECUTION VS COVER-UP**

- Let's play judge and jury
- Reasonable doubt
- Adverse publicity/customer confidence
- Prosecution

### **IX PUTTING IT ALL TOGETHER**

- Preparing an E-fraud risk assessment
- Creating an effective management briefing
- Staffing and funding
- Building an effective E-fraud squad
- Implementing preemptive anti-fraud techniques
- Staff and customer awareness programs