

Corporate Insecurity: Pillaging Information Assets, Destroying Established Reputations

COURSE DURATION: 2 hours

CPE HOURS: 2

LEVEL: Intermediate / Group-Live

PREREQUISITES: None

ADVANCED PREPARATION: None

Corporations, governments, and universities have one thing in common. They have all been targets of hackers and dishonest employees. Bank of America and Wachovia had client data sold by staff. Citi Group, City National and Time Warner lost electronic media; Card System Solutions, USC, California State University Chico and ChoicePoint had customer data taken. All of these institutions not only had to perform costly remediation, but their issues were widely reported in newspapers across the land and around the world. Clearly, traditional control structures have failed! Servers, databases and even outsourced operations are exposed to pillagers!

Executive management is not only embarrassed, but they feel that they have been deceived by incorrect assurances from middle managers, security staff and even auditors that their systems and data were safe. They provided management with a false sense of security based on testing and verifying antiquated controls that are not effective against the skilled cyber-thief. In this highly charged and controversial presentation, Gordon Smith, President and CEO of Canaudit Inc., will demonstrate how old-style controls can be easily defeated. Section by section, control by control, he will demonstrate how easy it is to defeat control structures. This is a session that must not be missed!

WHO SHOULD ATTEND

This seminar is intended for executives and senior managers who need to understand how control structures are defeated. It is also intended for senior information security and audit staff members. There are no prerequisites.

SEMINAR OUTLINE

I Overview

- State laws require disclosure
- Recent embarrassments
- Beating controls: Easier than stealing candy from a baby
- A new approach to risk assessment
- Testing the absence of control
- Changing the corporate mindset

II Defeating Physical Security

- Breaching the Fortress-type security
- Scamming key card access systems
- Fooling security staff
- Social engineering employees and contractors
- Accessing confidential documents
- Gaining access to data files
- Acquiring a valid and authorized access card and badge

III Account and Password Capture

- Beating Active Directory
- Defaults and service accounts

- Administrative accounts through DoS
- Web mail and VPN tricks
- Sniffers in gathering places
- Self Help – the great new beginning
- When all else fails, make donations

IV Gaining Access to Data

- Gleaning “insider” information
- Shared drives and files
- Courier and dispatch services
- Consultants and outsourcers
- Trading partners
- Exploiting database and operating system flaws
- Personal information storage and storage services
- Social engineering
- Not-so “public” information

V Hitching a Ride on the Information Superhighway

- Trusty old techniques still work
- Executive and home networks
- Corporate internet cafés

- Compromising laptops
- Defeating intrusion detection and prevention
- Inside-out outside-in exploits
- Cell phone and VOIP issues
- External links and services

VI The Internet: An Open Door

- Defeating VPN security
- Utilizing vendor backdoors
- Web applications: Gateway to the data
- Extranet exploits
- Defeating the firewall

VII Staff and Contractors

- “Purchasing” employees and contractors
- Public postings
- Hiring and contracting practices
- Portable data
- Fear of the auditor
- Scratching the surface

VIII The Canaudit Security Squadron

- We’re looking out for you