



< FOCUS > < DISCOVER > < INTEGRATE > < ADVANCE >

Compliance, Response, and the Technology that Drives Them

Albert Barsocchini, Esq.
Director Professional Services
Guidance Software Inc.
October 06, 2004
1:30pm - 3:00pm

The San Francisco Chapter of ISACA Proudly Announces the 4th Annual:

2004 SF ISACA FALL CONFERENCE

October 4-6, 2004

Legal Disclaimer

- ◆ **This presentation shall not be considered legal advice and is only provided as an informational resource**
- ◆ **Any cited authorities should be verified, updated, and interpreted by your attorney**

The Sea Of Risk

Hacking tools and discovery tools

Unauthorized applications

Unauthorized communications

Counterfeiting/ fraud

Rogue servers and services

Wrongful Termination

Unauthorized users/ intruders

Vandalism

DoS attacks

IP piracy

Fraud

Mishandling and theft of IP

Theft of customer information

Harassment

Possession of Inappropriate material

Computer file deletion/destruction



Corporate Fraud

- 75% of execs of public companies report fraud within their organization
(Source: KPMG 2003 Fraud Survey)
- 49% of companies reported fraud resulting in “theft of assets” and 36% reported “expense account abuse” fraud
(Source: KPMG 2003 Fraud Survey)
- 63% of companies report uncovering fraud as a result of employee tips, 54% “by accident,” and 41% do so by receiving “anonymous tips”
(Source: KPMG 2003 Fraud Survey)

Compliance & Liabilities

- Liability To Customers re Compromised Information
- Liability to Regulators
 - Mandated Incident Response Process
 - Internal Controls Due Diligence
- Liability to Shareholders
 - Loss of IP
 - Internal Fraud
 - Uncontained Security Incident
 - Public Relations Failure
- Downstream Liability
- Spoliation of Evidence **Hot Topic!**



Trend

The need to comply with an array of complex laws will continue to dominate the security agenda. The emphasis will be on policy management, enforcement, benchmarking standards, incident response, forensic investigations and monitoring for insider threats. **It is critical for corporate legal and management to understand the technology used to monitor and investigate compliance from the top down!**

Technology

“The Tie That Binds Compliance!”

Compliance requires legal, accounting, management, to channel data through technology which requires:

1. An understanding of the technology.
2. The ability to audit and investigate.

Keys to Success

- ◆ Control
- ◆ Communicate
- ◆ Monitor
- ◆ Investigate
- ◆ Train

Commitment to Forensic Investigation

The federal government is committed to using computer forensics to investigate computer related fraud and crime. U.S. v. Lloyd, 269m F.3d 228 (3rd Cir. 2001).

Caveat: Are you prepared to do likewise?

The Investigation

- ◆ **Conduct structured investigation**
- ◆ **Properly preserve and secure electronic data**
- ◆ **Minimize cost and business disruption**
- ◆ **Obtain relevant information**
- ◆ **Document and Report**
- ◆ **Share and exchange**

Early Detection and Remedy

- ◆ Intense legislative corporate scrutiny
- ◆ How companies respond to and investigate an incident is critical to determining compliance and any liability that may follow.
- ◆ Companies must demonstrate “real” cooperation with government inquiries
- ◆ Since digital data has replaced its paper counterpart, technology by necessity is the tie that binds regulatory compliance.
- ◆ Corporate legal and IT departments must work together to proactively assess and refine response/investigation procedures and most importantly understand the technology needed to support compliance.
- ◆ A comprehensive audit/response must include a real forensic based investigation to look at the data trail, in an effort to quickly determine the “what, when, and how” of the incident.
- ◆ The DOJ relies heavily on forensic based investigations.

Prevent, Detect, Communicate & Cooperate!

An effective response to corporate misconduct begins well before suspicions are raised or allegations are made. Paper compliance is not enough. Ask yourself does your compliance program really work or is it just form without substance?

Non-compliance cases have one thing in common: a breakdown in communication!

The DOJ's “Thompson Memo”



January 20, 2003, Deputy Attorney General Larry D. Thompson issued a memorandum setting forth factors that should be considered by federal prosecutors in deciding whether to charge a business organization with a criminal offense.

Among these factors is the “existence and adequacy of the corporation’s compliance program”, the corporation’s history of similar conduct, and the level of cooperation with government authorities. A good program may help curtail prosecution against a corporation under a *respondeat superior* theory for the act of a rogue employee.

SEC's "Seaboard Report"

In 2001 the SEC issued a report pursuant to Section 21 (a) of the Securities and Exchange Act.

- ◆ Self-policing
- ◆ Self-reporting
- ◆ Cooperation
- ◆ Remediation

The Seaboard Report notes that public companies should institute effective compliance procedures *prior* to the discovery of alleged wrongdoing, asking: "What compliance procedures were in place to prevent the misconduct now uncovered?" and "Why did those procedures fail to stop or inhibit the wrongful conduct?"

U.S. Sentencing Guidelines

U.S. Sentencing Guidelines Manual § 8B2.1 (2004) (“Guidelines”).

- ◆ **An effective compliance program” is a potential mitigating factor !**
- ◆ **Good Communication and understanding of the program from the top-down**
- ◆ **Immediate response to violations of law**
- ◆ **Due diligence to prevent and detect violations of law**
- ◆ **Promote an organizational culture that encourages a commitment to compliance with the laws.”**

Caveat: If a high-level person was involved in a violation, the Amendment imposes a reputable presumption that effective programs did not exist.

Legislation

- **California, SB 1386/ Civil Code 1798.82**
 - Mandates full disclosure to California residents of any compromised customer data
 - Law is triggered upon an computer Security Incident
 - Identifying and documenting what happened determines compliance
 - Delayed disclosure allowed for referral to law enforcement or reasonable internal investigation
- **Sarbanes-Oxley Act of 2002**
 - Severe liability for destruction of electronic records – up to \$25 million fines, 20-year prison terms
 - Important due diligence mechanism for internal controls
- **NASD Rule of Conduct 3110**
 - Brokers/Dealers must retain all emails/communications with customers
- **ISO 17799**
 - Outlines comprehensive incident response and internal investigation procedures
 - Detailed provisions on computer evidence preservation and handling

Mandated Incident Response Plans

♦ **FTC Safeguards Rule**

- Requires covered entities to maintain information security program that includes “Detecting, Preventing and Responding to Attacks, Intrusions, or Other Systems Failures.” (16 CFR Part 314.4(b)(3))

♦ **Office of Comptroller of the Currency (OCC)**

- Requires subject banking institutions to implement:
- “Response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies.” (12 CFR Part 30, Appendix B, III(C)(g)).

♦ **Health Insurance Security Standards (HIPAA Requirements)**

- Requires subject health care institutions to:
- “Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.” (45 CFR Part 164.308(a)(6))

SARBANES- OXLEY: Internal Computer Investigations Required

§§ 806 & 1107

Protects/Encourages Whistleblowers

&

§ 301

Must receive and Investigate complaints/ allegations of fraud

&

§ 802

Evidence Preservation Duty; Severe Penalties for destruction

=

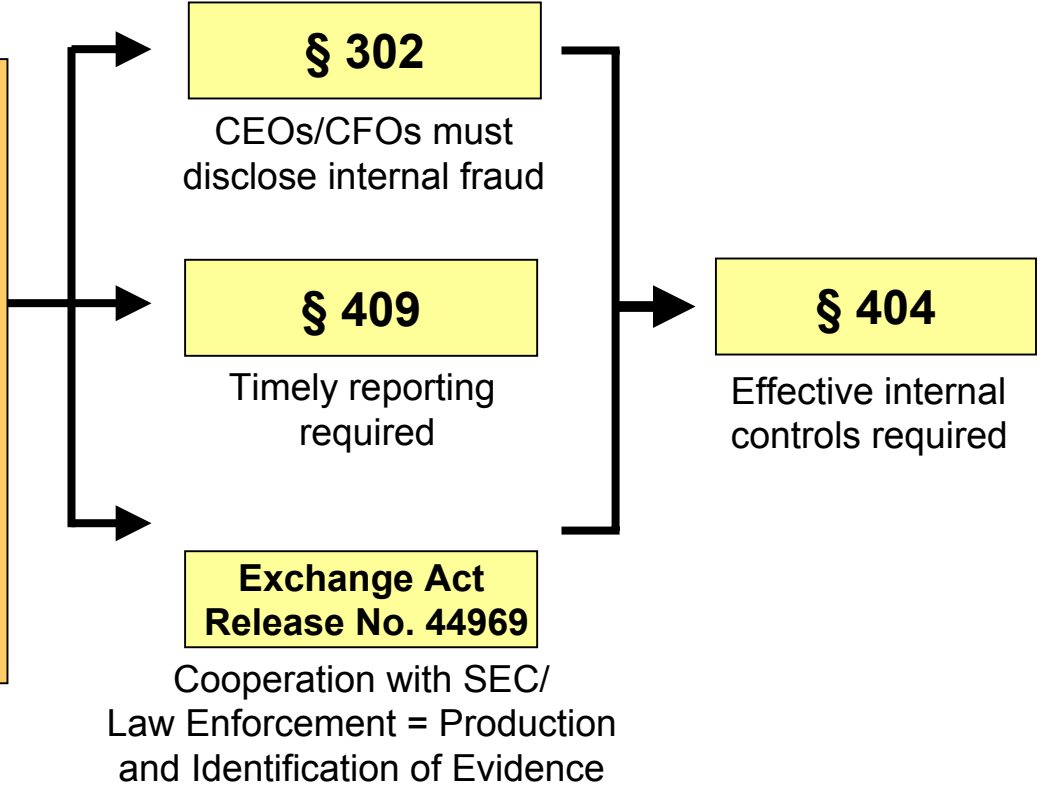
Infrastructure

Internal Investigation Infrastructure



INTERNAL INVESTIGATIONS

- Enterprise Computer Forensics = Best Practices
 - Nearly All Evidence is Digital
 - Government White Collar Crime Investigations Focus on Computer Evidence
 - Data Must Be Recovered, Analyzed and Preserved in a Thorough and Rapid Manner



Legal Issues when Dealing with an Incident

- ◆ Does the incident create potential liability to customers, employees, shareholders, regulators, downstream sources?
- ◆ What level of response / diligence is required to avoid liability?
- ◆ What evidence should be preserved?
- ◆ What are the reporting obligations?

Tip: Consider outsourcing your investigations because internal investigations may raise conflicts, be emotionally difficult and implicate legal privileges.

Challenges of Compliance Investigations

- ◆ Volatile Information may be lost
- ◆ Dealing with foreign languages
- ◆ Determining scope of compromise
- ◆ Restoration of systems and services
- ◆ Resource intensive (people, process, and technology)
- ◆ Chain of custody and evidence handling
- ◆ Containment of potential compromise
- ◆ Controlling release of information about compromise

Understanding the Technology that Drives Compliance

Network Enabled Forensic IR Capabilities

- In Place before Incident Occurs
- Determine scope of breach
- Focus Response Efforts on the Right Assets
- Collect Data on Hundreds of Geographically Dispersed Systems in Seconds
- Rapidly Identify Attack Signature and investigate malfeasance
- Automate Detection of Signature on Systems
- Terminate suspect process / Backdoors
- Business continues un-interrupted
- Evidence preserved quickly
- Reach well-informed decisions sooner
- Conduct Investigations on need-to-know basis
- Follow a repeatable forensic methodology
- Port investigation work product to law enforcement in a standardized format

EnCase[®] Enterprise Edition

- Effective Internal Investigations
- Evidence of Due Diligence
- Cooperation with SEC / FBI / Law Enforcement
- Rapid Response
- Deleted Document Recovery
- Document Preservation / Retention

Network Forensic Response & Investigation

Customer information



Employee Disputes



Corporate Secrets



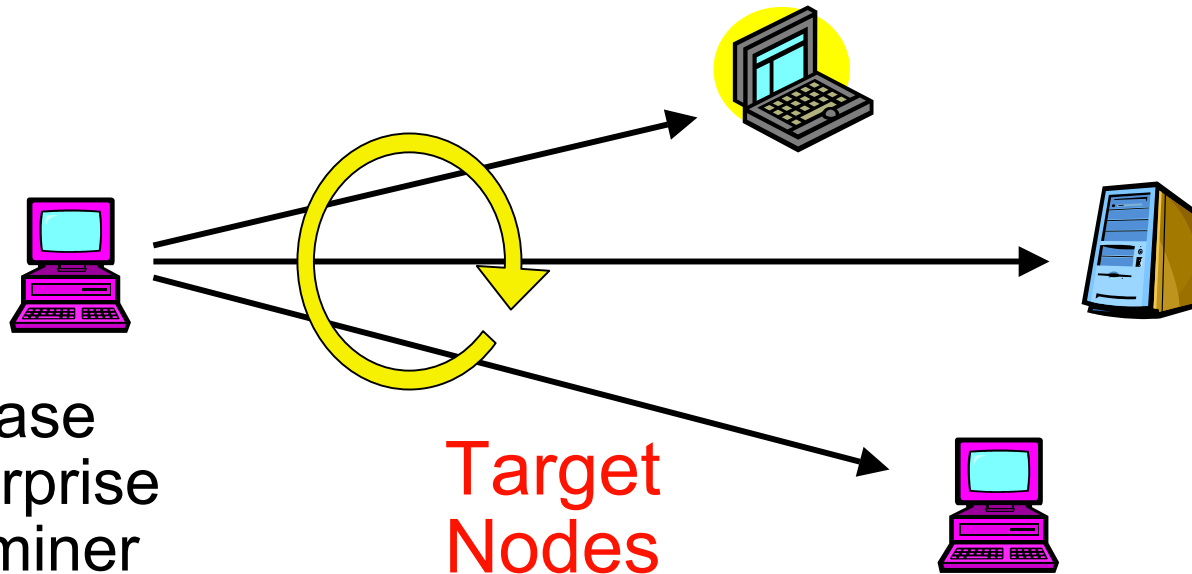
Litigation



Rogue applications



Criminal Activity



Enterprise Incident Response



Incident Response and Forensics

- Respond to alerts and breaches of perimeter systems
- Investigate internal threats
- Forensic analysis
- Quickly contain and mitigate loss
- Support compliance to legislation

- Immediate Response to any Incident on the LAN/WAN
 - Preserves, Recovers, and Documents Evidence
 - Law Enforcement Grade Forensic Technology = Best Practices
- Robust Security with Fine-Grain Controls

Goals

- ◆ **Quickly confirm and determine scope**
- ◆ **Provide accurate, relevant, and timely information**
- ◆ **Implement controls**
- ◆ **Protect individual rights established by policy and law**
- ◆ **Minimize downtime and effect to business and network services**
- ◆ **Cooperation with legal and law enforcement**
- ◆ **Provide upstream recommendations to management**
- ◆ **Understand, correct and protect from future compromise**

Legal Test of Compliance

1. Establish Procedures
2. High-Level Oversight
3. Use Due Care
4. Communicate Standards
5. Monitor
6. Enforce Consistently
7. Response And Prevention
8. Tone At The Top
09. Conduct Internal Control
10. Leadership Accountability
11. Resources And Authority
12. History Of Violations
13. Conduct Training
14. Evaluate Programs
15. Whistleblower System
16. Encourage Employees
17. Risk Assessment

Best Practices

- ◆ **Meet response provisions of legislation, regulations and industry best practices**
- ◆ **Minimize disruption to business and network operations.**
- ◆ **Prevent a disjointed and non-cohesive response.**
- ◆ **Confirm or dispel whether an incident occurred.**
- ◆ **Promote accumulation of accurate information.**
- ◆ **Establish controls for proper retrieval and handling of evidence.**
- ◆ **Protect privacy rights established by law and policy.**
- ◆ **Allow for criminal or civil action against perpetrators.**
- ◆ **Provide accurate reports and useful recommendations.**
- ◆ **Provide rapid detection and containment.**
- ◆ **Minimize exposure/compromise of proprietary data.**
- ◆ **Protect your organization's reputation and assets.**
- ◆ **Educate senior management.**
- ◆ **Promote rapid detection and/or prevention of future incidents.**

Communicate

1. **Tone At The Top** - an organizational culture that encourages a commitment to compliance with the law;
2. **Conduct Internal Control** - standards of conduct and internal control systems that are reasonably capable of "reducing the likelihood of violations of law"
3. **Leadership Accountability** - responsibilities of an organization's governing authority and organizational leadership for compliance
4. **Resources And Authority** - resources and authority for individuals with the responsibility for implementation of the program
5. **History Of Violations** - objective requirement for determining if there is a "history of engaging in violations of law"
6. **Conduct Training** - training and the dissemination of training materials and information within the definition of an "effective program"
7. **Evaluate Programs** - "periodic evaluation of the effectiveness of a program" to the requirement for monitoring and auditing systems
8. **Whistleblower System** - a mechanism for anonymous reporting
9. **Encourage Employees** - system for employees not only to report actual violations, but to "seek guidance about potential" violations, in order to more specifically encourage prevention and deterrence of violations
10. **Risk Assessment** - ongoing risk assessments as part of the implementation of an "effective program."

Questions?

Albert Barsocchini, Esq.
Director of Professional Services
Guidance Software
2100 Powell Street, Suite 100
Emeryville CA 94608-1803
Phone: 415.760.0154
Fax: 510.652.5018