



INVESTIGATIONS

Is your company capable of handling an event?

David Bork, CISSP

dbork@bork.us

Introduction

This presentation takes you through the stages a company has to go through in an investigation. This way you can be better prepared for possible investigations.

Where is all the data?

What are the Vectors?

Types of Investigations

Evidence Collection

What Data to Look For?



WHAT ARE THE VECTORS?

Major Vectors

There are many reasons to start an investigation. Some of the most obvious are research for mergers and acquisitions. Fraud based upon regulatory and compliance issues.

Merger

Acquisition

Regulatory

Compliance



TYPES OF INVESTIGATIONS

Investigations

Fraud, financial irregularities, employee and commercial disputes are some of the most complex and challenging issues facing business today. They can result in major financial damage, as well as serious reputational and regulatory risks.

Information Technology is always involved.

- Investigating internal fraud, violations of law, regulations, and company policies
- Gathering evidence in major litigation and commercial disputes
- Locating concealed assets
- Investigating the theft of intellectual property

Corporate
Investigations

Forensic Accounting

Hostile Takeovers

Investigative Due
Diligence

Corporate Investigations

Investigate allegations of civil and criminal fraud, accounting irregularities, intellectual property theft, foreign corrupt practices, embezzlement, electronic crimes, information leaks, undisclosed and related-party transactions, vendor fraud, kickbacks and other conduct.



Forensic Accounting

Investigation to unravel the true financial state of the business, as well as identifying how its accounting systems may have been manipulated to cover up any wrongdoing. The team will also work to quickly ascertain the value of funds that the organization may have lost.





Hostile Takeovers/Proxy Contests

Investigation involving high-profile takeover bids. Be it a proxy contest or tender offer. Having the information needed makes the difference between winning and losing.



Investigative Due Diligence

Investigation involving a wide range of information to generate critical intelligence. These include public sources; people familiar with the sector or business in question (business associates, employees, suppliers, customers, etc.).

Some sample investigations:

- Management style and ethics of key executives
- Unjustified personal and business reputations
- Litigation involving the company
- Unrealistic projections
- Overstated assets and revenues
- Environmental liabilities
- Hidden ownership issues
- Misrepresentation and non-disclosure of material facts





EVIDENCE COLLECTION

Where do you start?

- Run an internal investigation
- Seek third party for assistance with a complimentary set of procedures
- Determine the decision maker.
 - who does the hiring?
Legal vs. IT
 - Finds another firm with forensics activity (legal usually needs technology assistance.)



Third Party Vendors

Plan

Are they tech savvy?

Can they guide you through the stages of an assessment?

What will they do with your data?

How will they protect your data?

How will your data get disposed of once the investigation is completed?

Normal investigations take two to 18 months and can go longer...



Shouldn't you have prepared for this?

Plan

Well defined policy structure

Policy to handle requests

Storage Environment (SAN Preferred)

Key Escrow for Encrypted Data

Administrative Passwords to Gain System Access / Access Encrypted Hard Drives, etc.





Evidence

Follow Chain of Custody

Preservation of Evidence

Focus on Computer Forensics





WHAT DATA TO LOOK FOR?

Where is the data?

This depends on the type of investigation.

- SAN (Centralized Storage)
- Tapes / Backup Media (Collection Takes a Longer Period of Time)
- Local Servers – Could be hundreds
- Laptop / Desktop Computers
- Email Systems



Communications

Legal Department Speaks Differently

- What did these individuals have access to?
- Who are the owners of the data?
- Were the permissions set appropriately? READ vs. WRITE
- Was auditing turned on?





Communications (continued)

Could evidence be present in general use directories [all access areas]?

Correlation between directory permissions and users

Correlation between executives and directory permissions



Questions?

