
Holistic Investigations

Lawrence D. Dietz, Esq., COL (R)



Perspectives

- Developers Vs. Users
- Interested Parties and Potential Suspects
 - Insiders & Former Insiders
 - Outsiders

Insiders & Former Insiders

- RIFs or Terminations
- Employee Politics & Personal Reasons
- Theft of IP

Outsiders

- Criminals – Financial Gain
- Competitors - Advantage
- Foreign Governments – Intelligence or \$\$\$\$
- Non-State Actors - ??????
- Litigants – Especially Product Defects Plaintiffs

Application Security Targets

- Intellectual Property
 - Trade Secrets
 - Code to use ‘for free’
 - Reverse Engineering
- The Data

Application Security Damages

- Reputation & Lost Future Sales
- Financial Loss
- Loss of Competitive Advantage

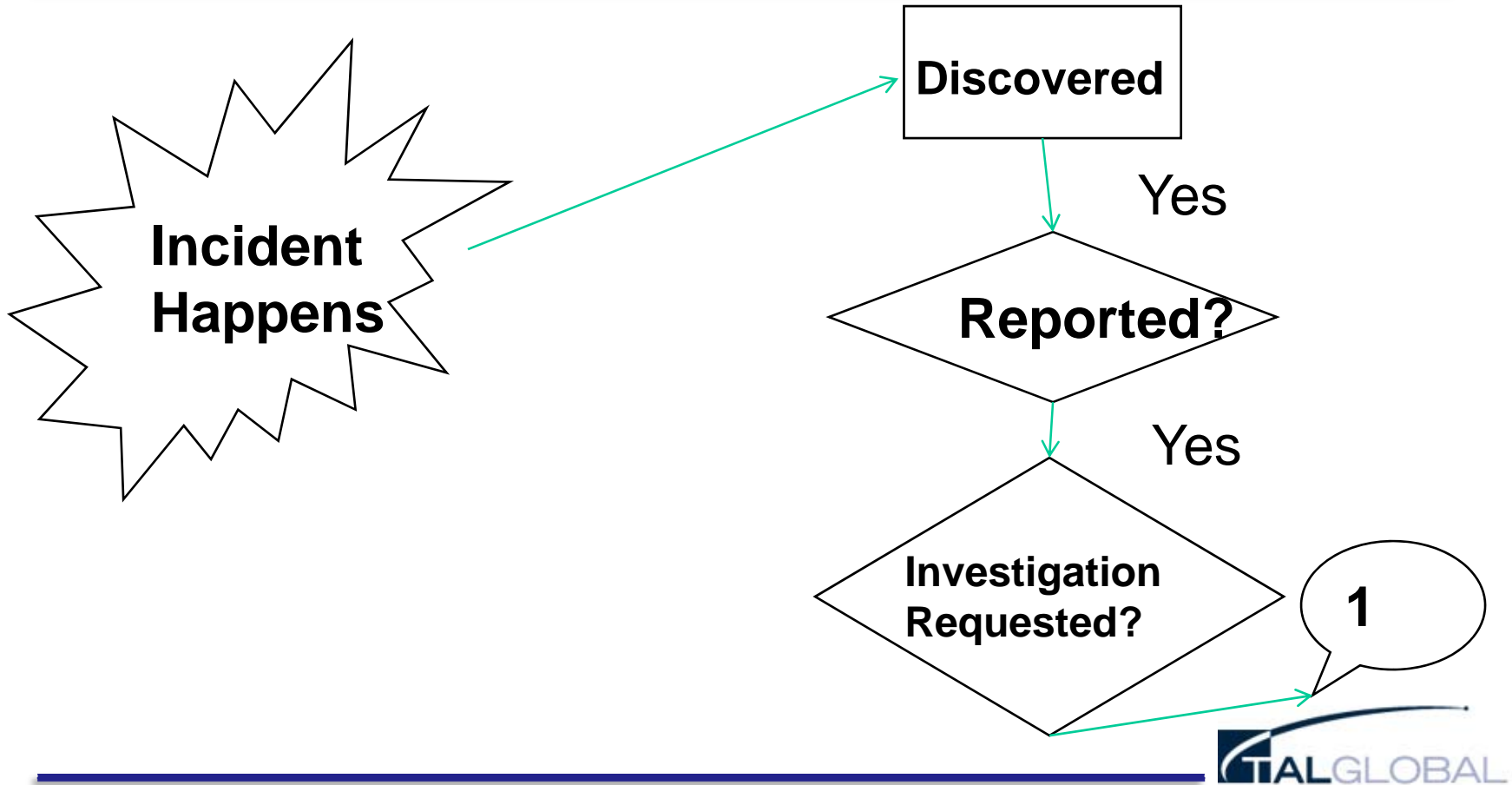
Legal Aspects

- PII Disclosure Requirements
- Investor disclosure for loss of critical Intellectual Property
- Liability of Officers and Directors
- Product Defects Lawsuits

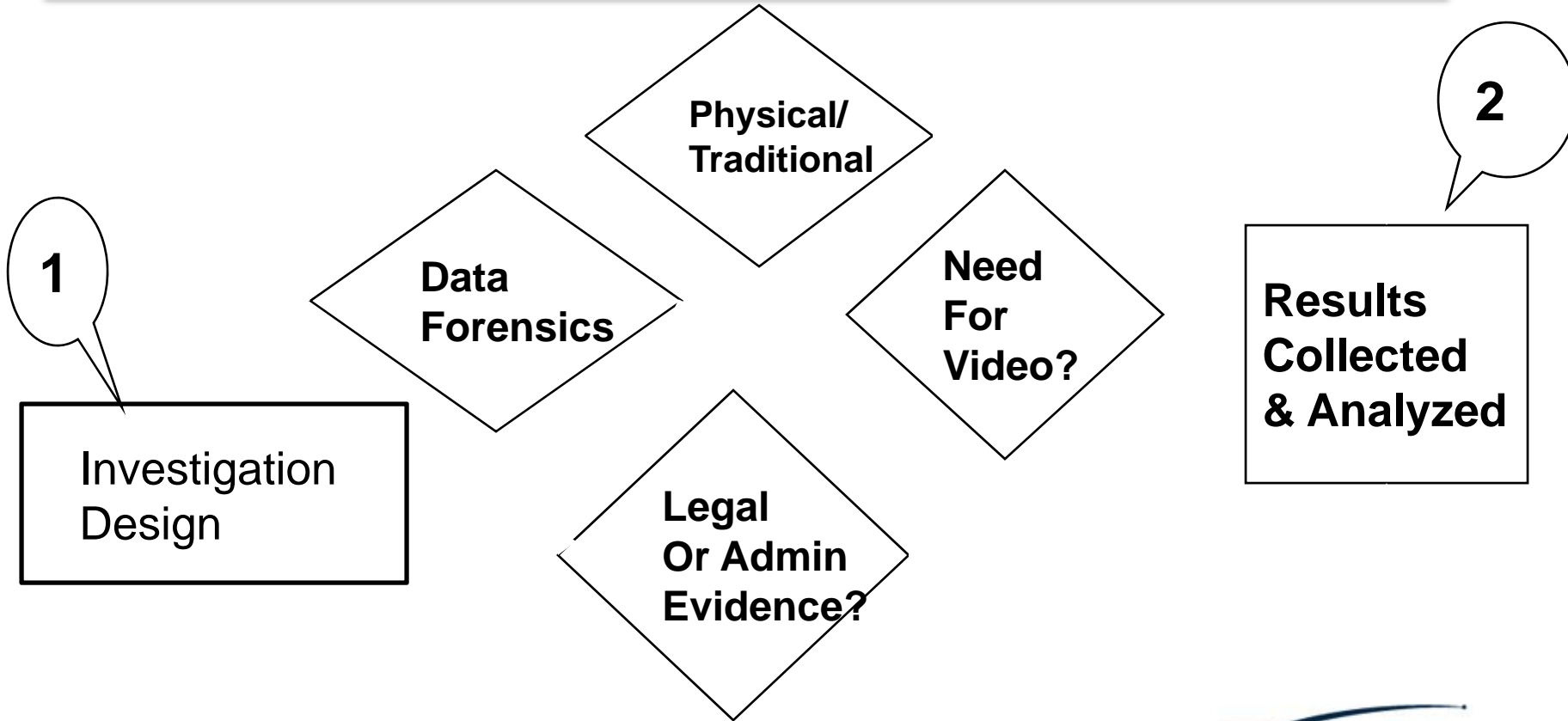
Holistic Investigations

A holistic investigation combines physical and information security procedures and technology to gather and preserve the best evidence of the nature of the breach and successfully prosecute the perpetrators.

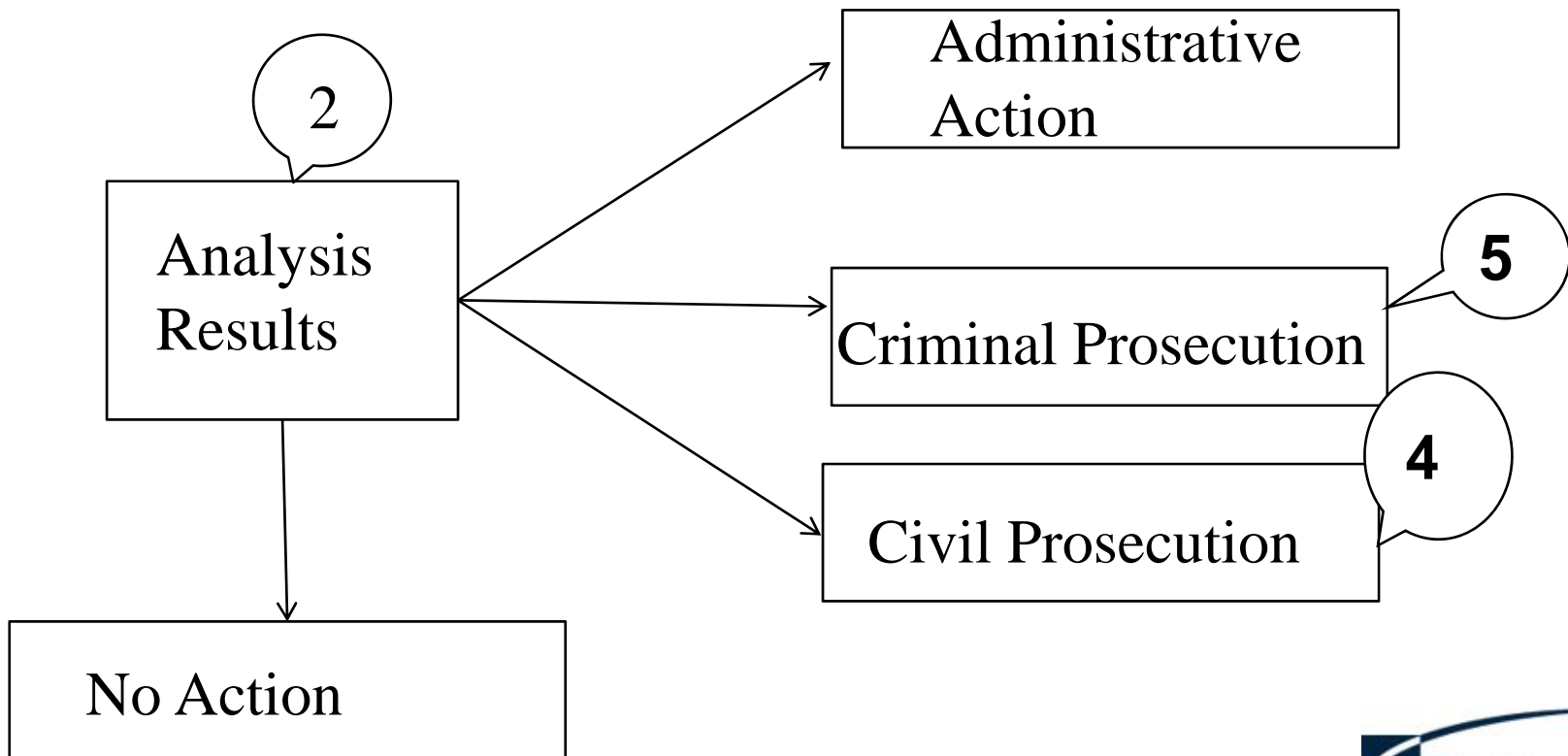
Preliminary Phase



Investigation



Analysis of Results



Criminal Prosecution

5

**Law Enforcement
Engagement Plan**

**Spokesperson/LNO
Assignment
& Training**

**Executive
Protection
Plan**

**Prosecution
Preparation**

TRIAL

6

Civil Litigation

4

**Litigation Strategy
& Planning**

**Jurisdictional
Requirements**

7

**Discovery
& Forensics
Strategies**

Civil Litigation Preparation

7

**Evidence
Analysis**

**Legal
Work Products**

**Revised Discovery
Activities**

8

Case Study #1 – Alpha Industries

Alpha industries is a well funded software start-up. You have been retained by one of their investors to work with the CEO.

The CEO suspects that Ed, one of his founding engineers is planning on leaving the company and taking some proprietary software with him. The CEO believes that the engineer is already doing consulting work for Conglomerate Industries, a \$5 Billion, publicly held software company.

1. What are the top level issues?
2. Is there a possibility of litigation, if so civil or criminal?
3. How is the case complicated if Ed works from home?
4. What if Ed were a sub-contractor and not an employee?
5. What are some of the tasks you might assign a traditional investigator?
6. What factors might induce you to employ Network Forensics?

Case Study #2 – Bravo Bank

You are the CSO for Bravo Bank, a bank located in a suburban city of 130,000. The bank's loan application was compromised and the bank was used as a 'source' in a major phishing attack a few weeks after the compromise was discovered. In your due diligence you find that Bravo is the only Bank in your area to be compromised. You also find out that there has been a noticeable loss of customers to Continental Bank of North America, one of the top 3 banks in the US.

1. How would you go about determine how the system was compromised?
2. How would you try and link the compromise to the phishing attacks?
2. What help might you enlist to find out if these attacks might be an inside job?
3. Do you think these attacks are being caused by the competition? If so, how might you check out this possibility?
4. What other groups or types of individuals might be responsible?
5. Given that there has been a crime or crimes committed, what additional actions should you take?

Case Study #3 – Internet Innovations Software

You are the CIO of a Internet Innovations (II), a software company based in Waltham, MA. II has been in business for 5 years, has revenue of about \$100 million and is publicly held. Their application is a software package for small Doctor and Dentist offices that allows them to pre-book appointments and accept credit card pre-payments. Like many other firms, they have conducted a RIF. The engineering department lost 5 people. One of them was on an H1B Visa and was forced to return to his home country.

Several of your customers have called to say that their patients have reported a rash of identity thefts and that only the patients who used II software were effected.

1. What laws do you need to make sure General Counsel is aware of?
2. Suppose you determine that a flaw was built in to your service and that it appears that PII data has been sent to an unknown location. Further, it appears that the flaw was coded by the engineer who was forced to leave the country.
 - What should you do to the application immediately?
 - What types of checks should you perform concerning access?
 - Is it too late to implement Data Leak Protection technology?

Q&A

- Contact Information
 - Idietz@talglobal.com