POLYONICS®

Counterfeit Electronics: Strategies for Fighting Counterfeit Electronics

Dr. James Williams, Chairman, Founder

POLYONICS, Inc.

Overview

- Background information
- Scope of the problem
  - Anecdotal
  - Study by International Chamber of Commerce
  - Recent study US Dept of Commerce
- What to do about it ?
  - “Findings” and “Best Practices”
- Types of strategies

My Perspective

I’m a “Product ID guy”

My job… deliver Brand Protection Technologies by means of product identification

I am a “technology agnostic”

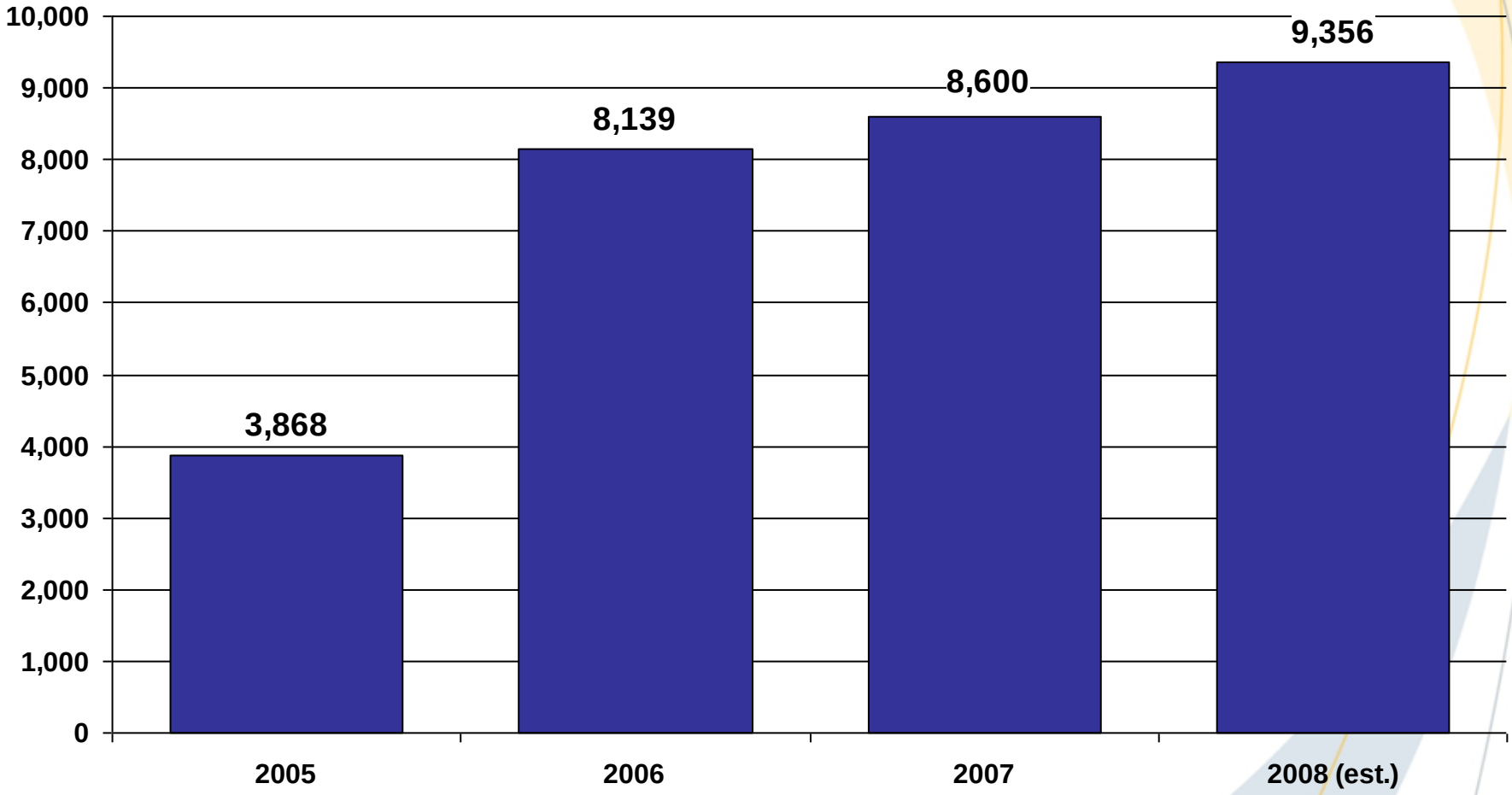
Counterfeit Electronics -Broad Definition

- **An electronic part that is not genuine because:**
  - **An unauthorized copy**
  - **Does not conform to original design, model, and/or performance standards**
  - **Not produced by the OCM or is produced by unauthorized contractors**
  - **An off-specification, defective, or used OCM product sold as "new" or working**
  - **Has incorrect or false markings and/or documentation**

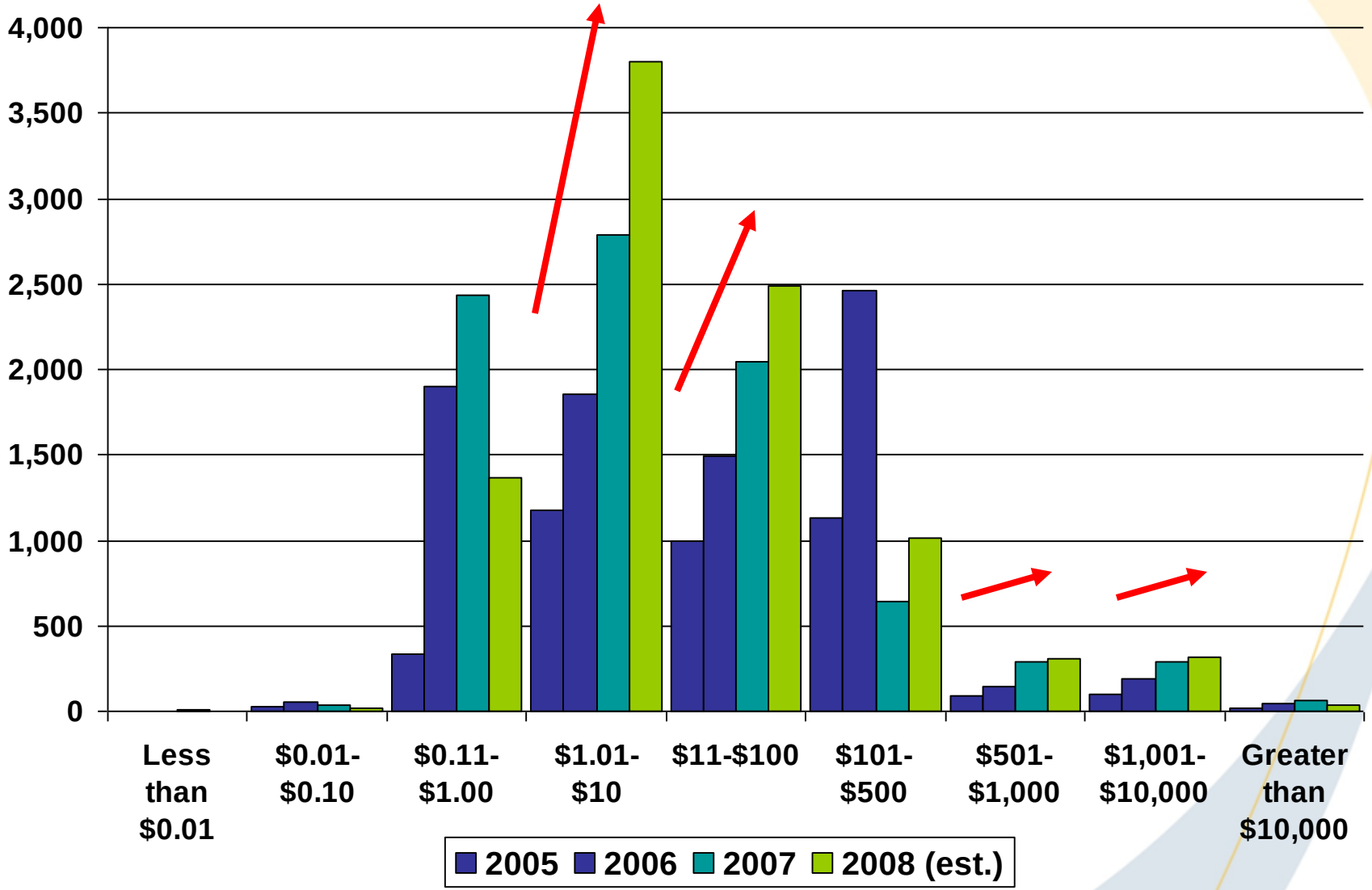
Department of Commerce
Office of Technology Evaluation

- Contact bbotwin@bis.doc.gov
- *"Defense Industrial Base Assessment:Counterfeit Electronics"*
  - *Survey completed /available January 2010*
  - *387 Surveys*
    - *83 OCM*
    - *98 Parts Distributers*
    - *32 Circuit Board manufacturers*
    - *121 Prime and sub- contracters*
    - *53 DOD Organizations*

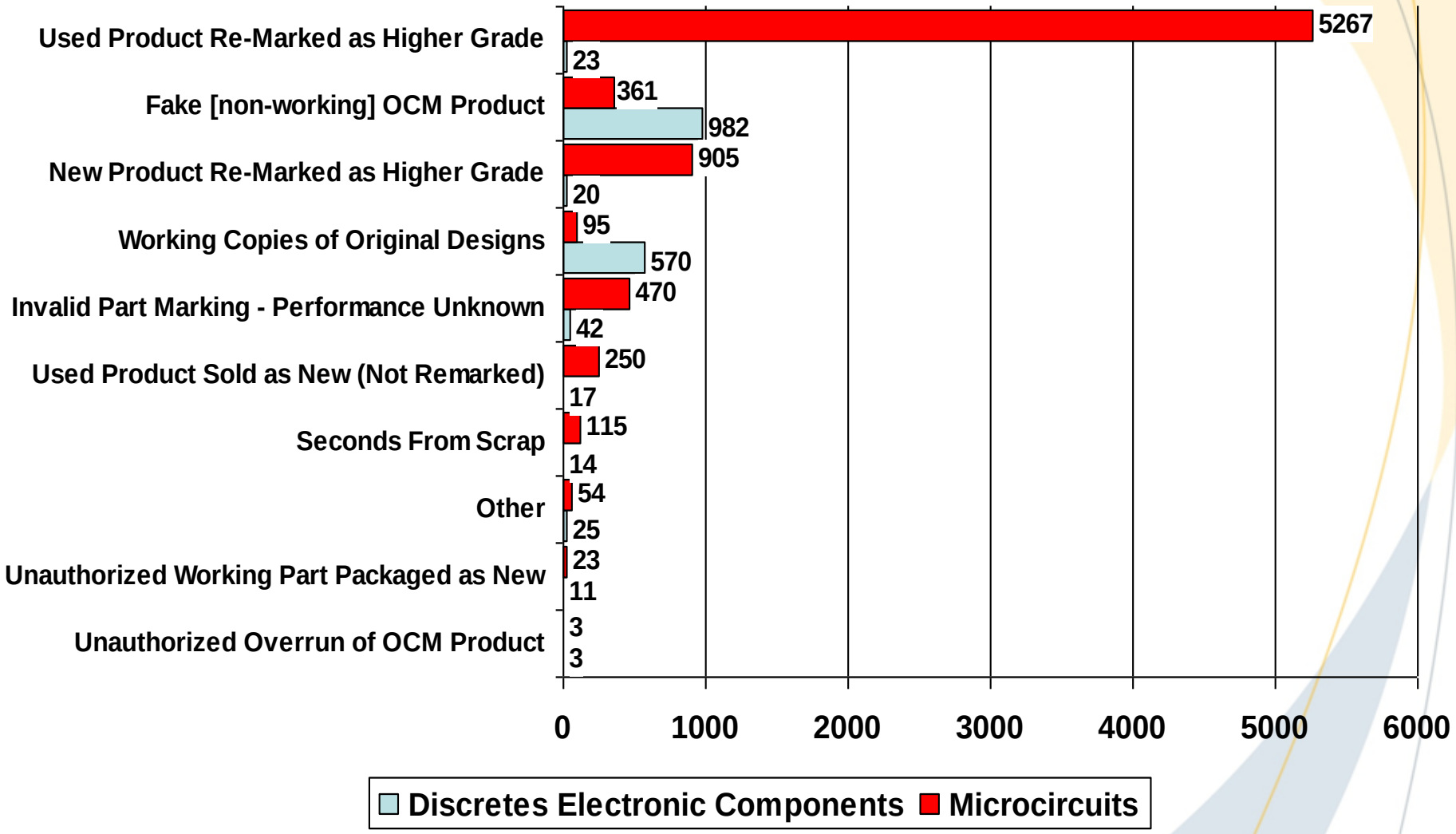
Total Counterfeit Incidents: OCMs, Distributors, Board Assemblers, Prime/Sub Contractors 2005 - 2008



Counterfeit Incidents by Product Resale Value: (2005 - 2008)



Counterfeit Incidents by Type (2008 est.)



REASONS GIVEN for Increase in Counterfeit Goods

Reason	Number of Companies
Less Stringent Inventory Management by Parts Brokers	179
Greater Reliance on Gray Market Parts by Brokers	168
Greater Reliance on Gray Market Parts by Independent Distributors	152
Insufficient Chain of Accountability	141
Less Stringent Inventory Management by Independent Distributors	139
Insufficient Buying Procedures	124
Inadequate Purchase Planning by OEMs	117
Purchase of Excess Inventory on Open Market	113
Greater Reliance on Gray Market by Contract Manufacturers	107
Inadequate Production by OCM	105

Internal Actions Taken

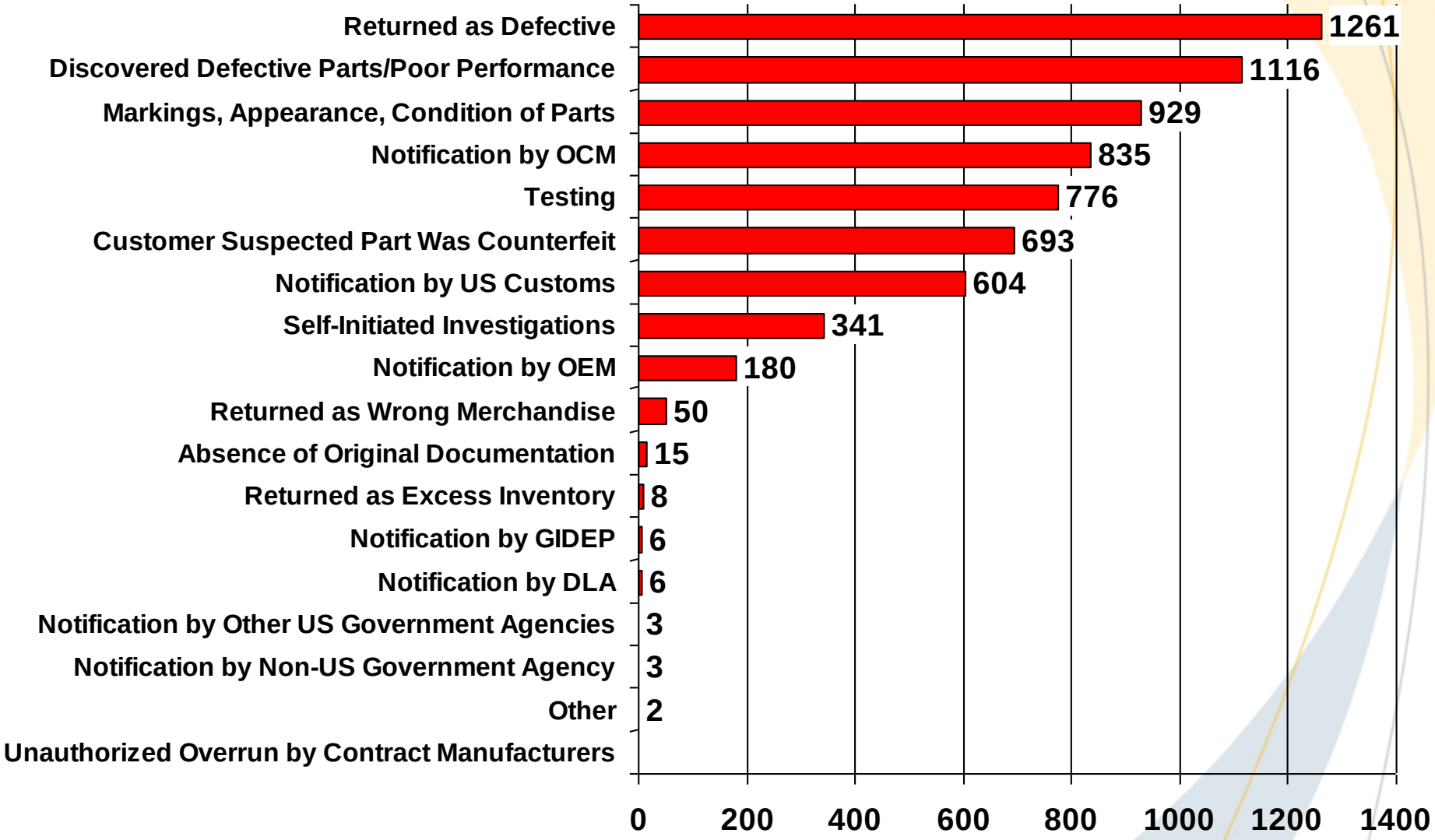
	DLA Organizations	Non-DLA Organizations
No internal actions taken	83%	59%
Performing screening and testing on inventory	17%	24%
Training staff on the negative economic and safety impact of counterfeit products	11%	21%
Revising organization procedures for disposal of “seconds,” defective parts, and production overruns	11%	14%
Revising procurement to more carefully screen/audit/evaluate authorized returns from customers	11%	14%
Adding security markings to existing inventory	6%	10%
Embedding new security measures in existing product lines	6%	0%
Embedding new security measures in product lines	0%	0%

Counterfeits Damaging a Company's Reputation

- **Prime/Sub Contractor Comment: When some businesses report counterfeit parts findings via GIDEP alerts and other companies do not, authorities may think that the reporting companies have more counterfeit issues than non-reporting companies.**
- **Distributor Comment: "The entire brokerage industry has experienced a black eye due to some unethical and/or unknowledgeable brokers. We have lost many contracts from large contract manufacturers simply due to us being a 'broker.'"**

Percent of Companies Indicating Counterfeits Have Negatively Effected Their Image or Reputation	
Discrete Electronic Component Manufacturers	8%
Microcircuit Manufacturers	25%
Authorized Distributors	9%
Independent Distributors	45%
Brokers	44%
Circuit Board Assemblers	6%
Prime/Sub Contractors	7%

How Companies Are Uncovering Counterfeits (2008 est.)



Counterfeit Electronics Study-Themes

- Lack of dialogue between all parties
- Insufficient chain of accountability
- Assumption that others in the supply chain are testing the product
- Record keeping is non-existent
- No one knows who to contact in the Federal government
- There needs to be stricter testing protocols and monitoring
- Most DOD organizations do not have policies in place to prevent counterfeit parts from infiltrating their supply chain
- No type of company or organization has been untouched by counterfeit electronic parts

Everyone must work together to solve the problem.

It's ALL about information

- We provide a product, which performs a valuable function…people want to buy it !!
  - We promote, and sell this product..
    using information (including BRANDING)
- The product's performance generates information…
  - "it works" or "it doesn't"
  - If it doesn't work, in the field, we get information AFTER THE FACT

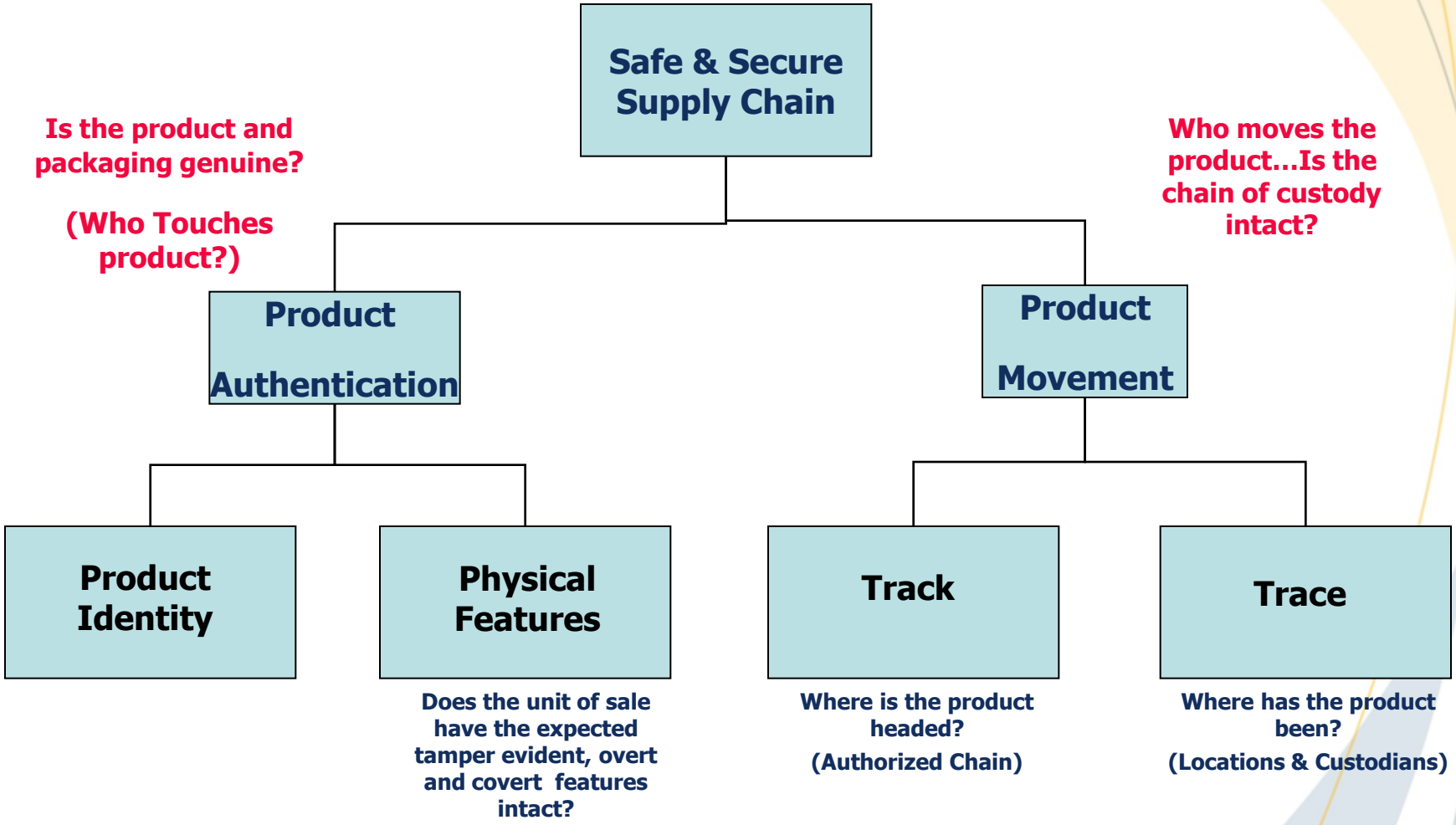
Information !! (2)

- Can we generate information "before the fact"?
  - "Rule of 10's" !!!

Level of completion	Cost to find & repair defect
The part itself	$n
At sub-assembly	10 × $n
At final assembly	100 × $n
At the dealer/distributor	1,000 × $n
At the customer	10,000 × $n

Information (3) Fighting/Preventing

- It's all about information…and what you will do with it, once you have it
  - Your goals dictate the strategies
  - Your strategies dictate choices, including technological choices
  - Technological choices will determine trade-offs you must make

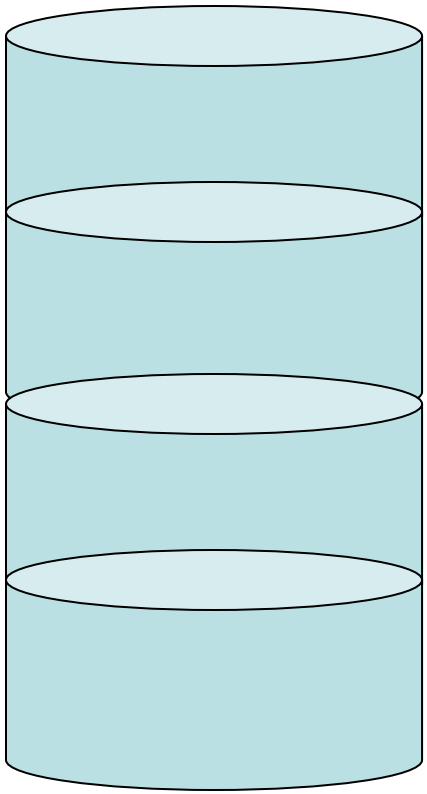

Safe & Secure Supply Chain
Is the product and packaging genuine?
(Who Touches product?)
Who moves the product…Is the chain of custody intact?
Product Authentication
Product Movement
Product Identity
Physical Features
Track
Trace
Does the unit of sale have the expected tamper evident, overt and covert features intact?
Where is the product headed?
(Authorized Chain)
Where has the product been?
(Locations & Custodians)

Types of Strategies

- Defensive
  - PROTECT ourselves..AVOID DANGER
- Offensive
  - ATTACK the opposition
  - Make them REACT to our actions, to avoid us (NEW DANGER)
- Balanced
  - Both offensive and defensive
  - “Holistic”
  - Integrated

Cost of Business

BRAND OWNER



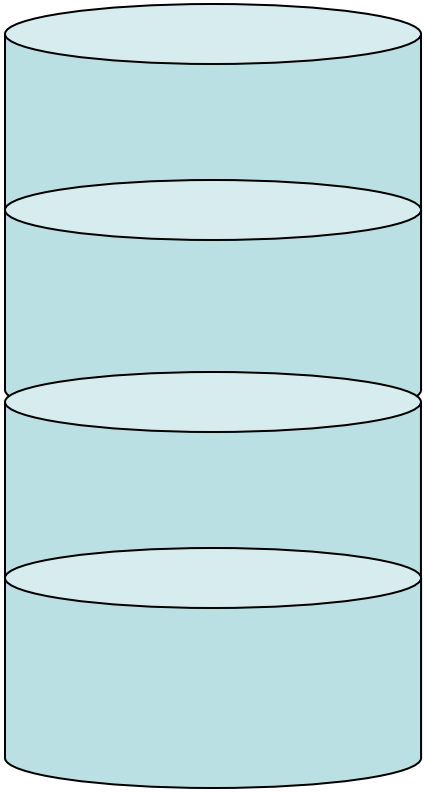
COGS

Warranty

R&D

Marketing

Counterfeiter



COGS

Warranty

R&D

Marketing

- View the counterfeiter as competition
  - Only R&D they do is to “convince you of the appearance, so you’ll pay”
- Accept the fact that the counterfeiter is cynical, clever, smart, well-capitalized and organized
    - ..sociopathic, greedy, and “lazy”…but not “stupid”

The Foundation for Success….YOU!

- A Core Belief
  - It's the same story for all of us
    - Just change a few nouns and verbs
  - This means…learn the lessons from success and failure in other industries
  - Concepts & Synthesis

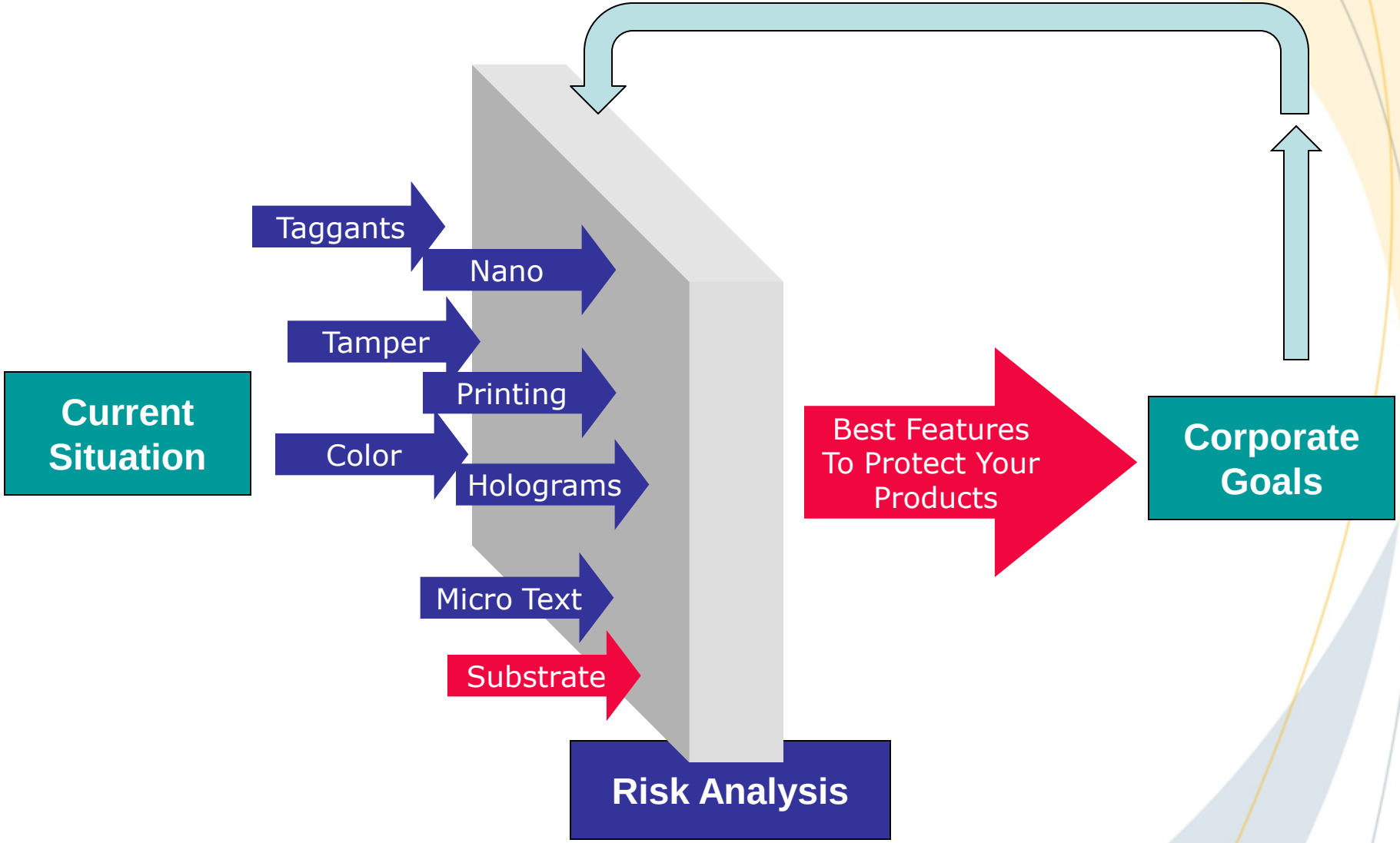
It’s all about information !!!

- Counterfeiter’s goal…convince someone “Well enough”….purchase the product..take the money and run
- What is your Goal ?
- What will you do with the information you generate from your program?
- THIS DICTATES THE TYPE(S) of TECHNOLOGY (TOOLS!)

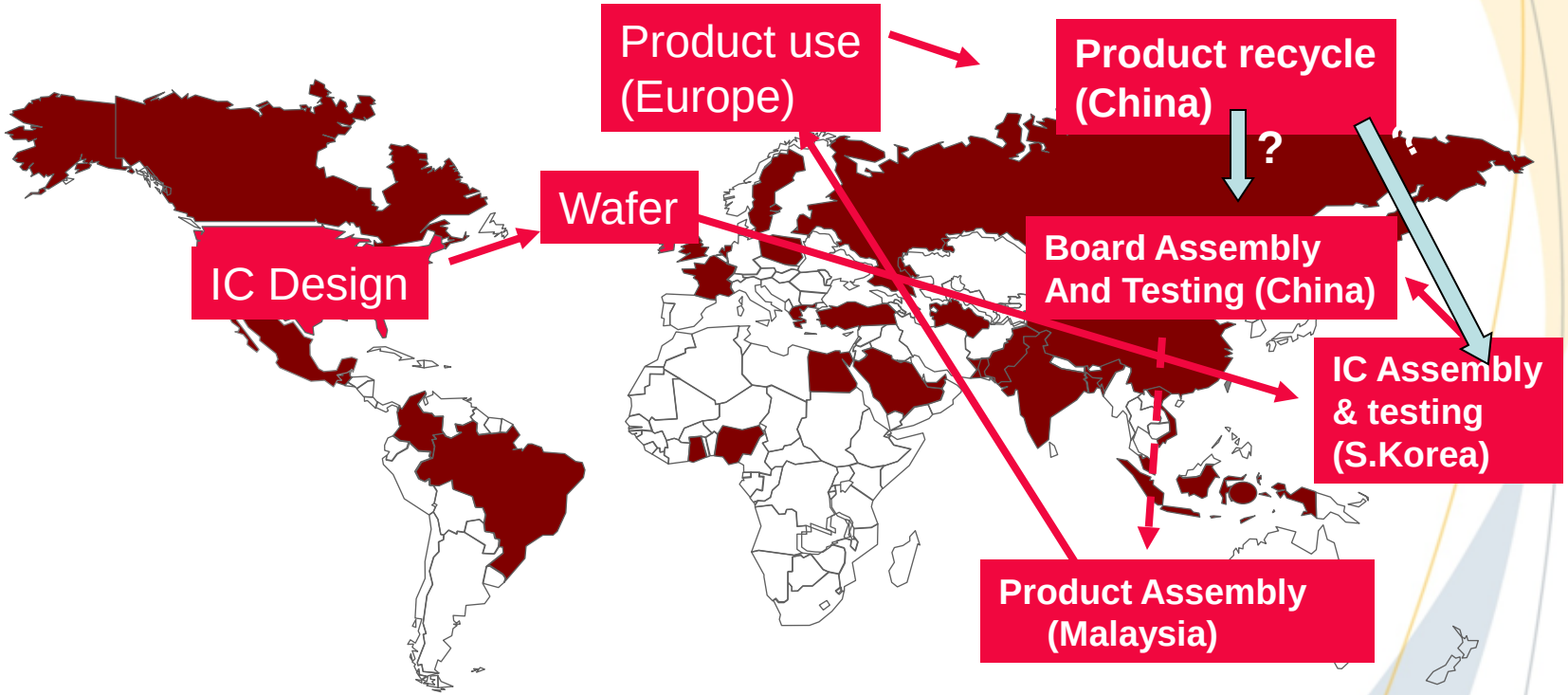
Goals dictate Strategies……. which then dictate Technologies

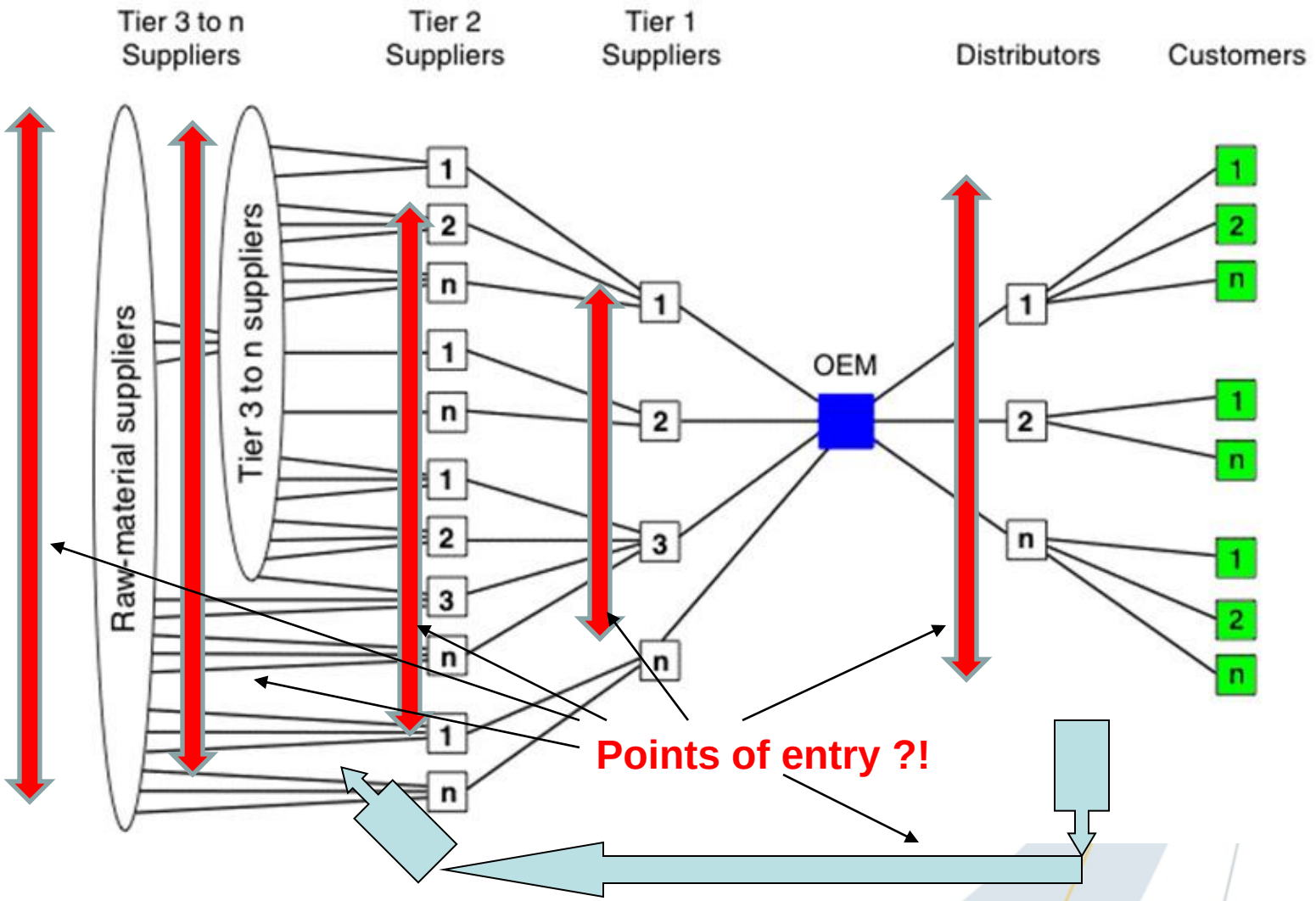
- Continuum from “increase THEIR cost of doing business”, to “let’s put them all in jail”
- AVOID, DETECT, DETER (PREVENT) Different strategies…different technologies
  - Detect..then AVOID…..defensive
  - Detect…then DETER…offensive

Overview of Choices



Global Nature of Electronics




Tier 3 to n Suppliers
Tier 2 Suppliers
Tier 1 Suppliers
Distributors
Customers
Raw-material suppliers
Tier 3 to n suppliers
OEM
Points of entry ?!

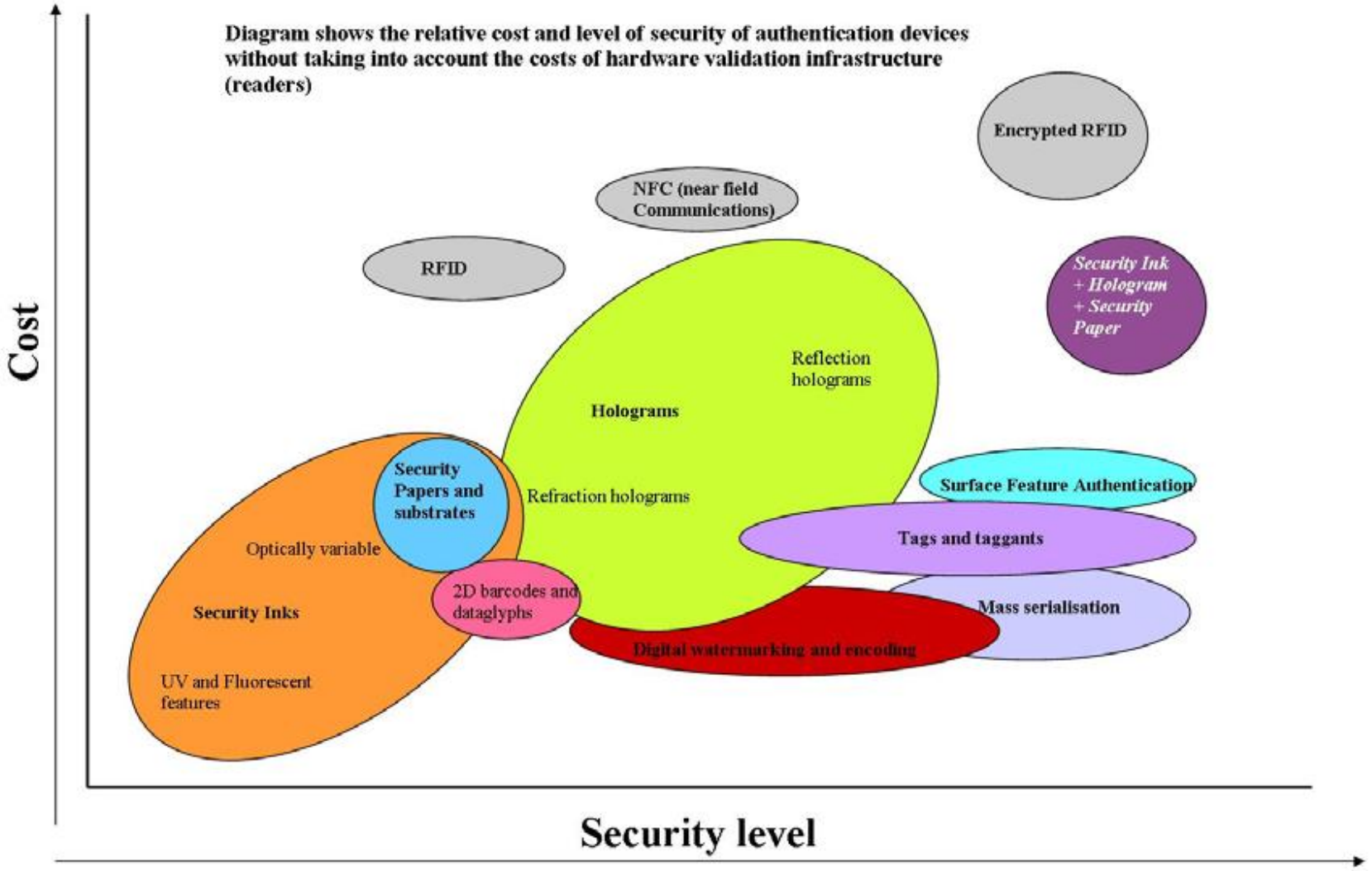
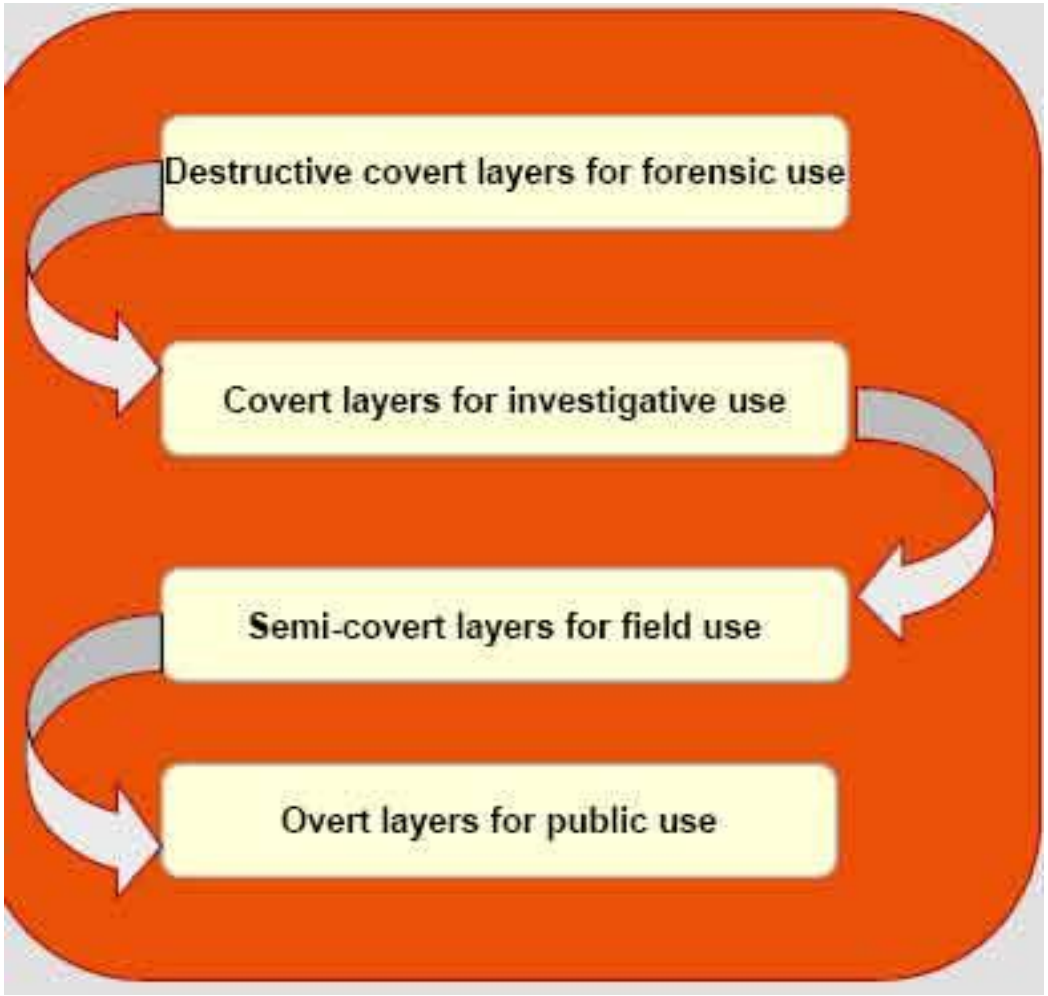


Diagram shows the relative cost and level of security of authentication devices without taking into account the costs of hardware validation infrastructure (readers)
Encrypted RFID
NFC (near field Communications)
RFID
Security Ink + Hologram + Security Paper
Reflection holograms
Holograms
Security Papers and substrates
Refraction holograms
Surface Feature Authentication
Tags and taggants
Optically variable
2D barcodes and dataglyphs
Mass serialisation
Security Inks
Digital watermarking and encoding
UV and Fluorescent features
Cost
Security level

TOOLS !

- First, some “rules”:
  - Mark/identify everything you can
    - Packaging, inserts, caps, lids,..and of course, the product itself, if possible
  - “Layers” of technologies, to match a “layered defense”
  - VARIABILITY of technology is a strong ally

Different Information Needs? Different Tools !!



- There is no one best technology – evolving "NO SILVER BULLET"
  - There are a great many suppliers today – confusing..
- There is no one best way to deploy – strategies are improving

Key Attributes

- Know what problem you are trying to solve.
  - Get as close to the product as you can do so affordably.
- No single technology can assure a product will not be counterfeited.
  - Layers must be utilized
  - Features must be changed…
  - Stay nimble.
- No technology should be deployed without a plan for monitoring it in the field, ever.
- No technology should be deployed that cannot be updated in a moments notice.

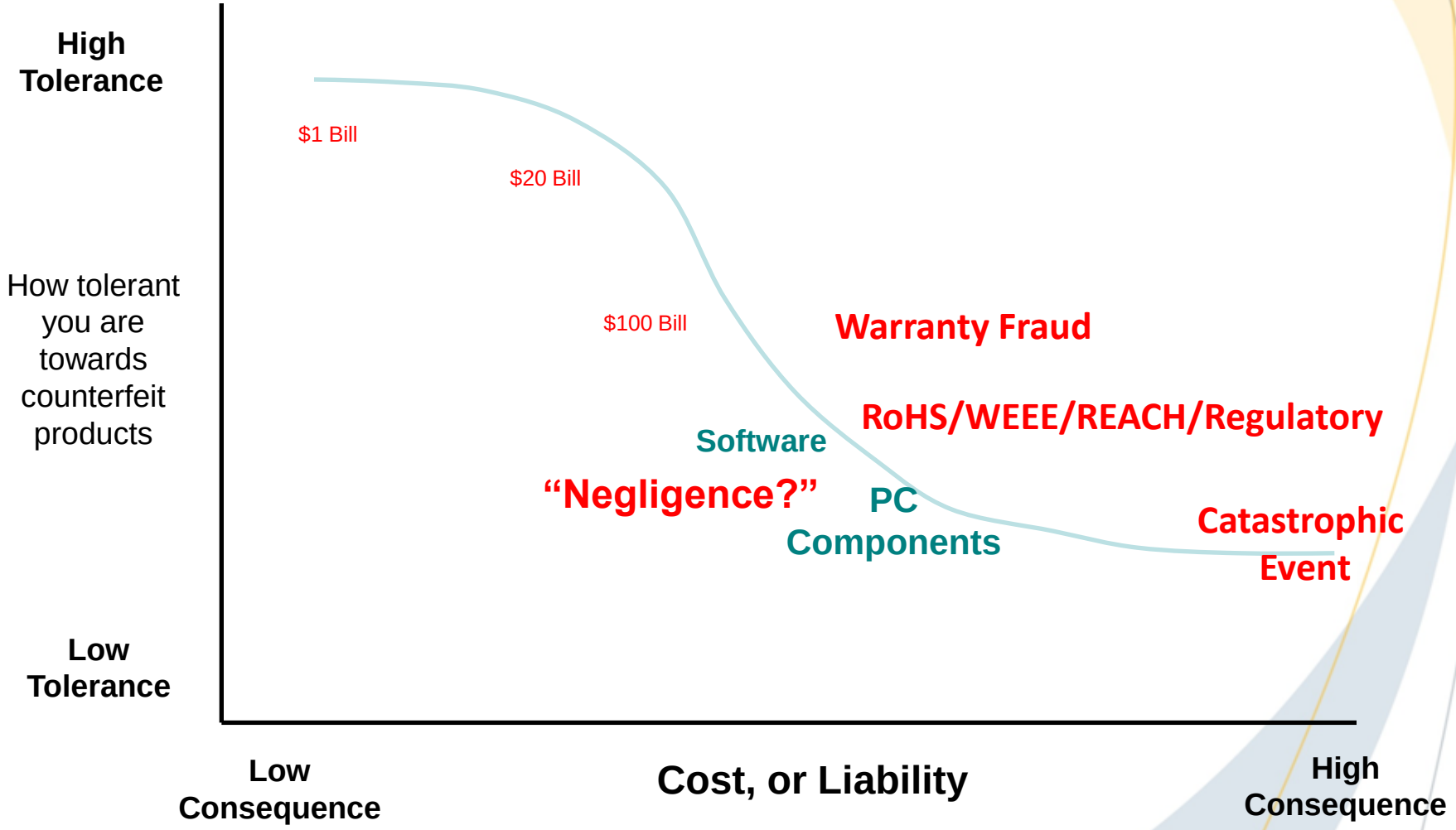
- The dilemma of “Standard Products”
  - You decide fit
  - Security problems?
- The dilemma of “Proprietary for you”
  - R&D time
  - Cost and commercialization

To “Outstrategize”

- Our primary goal….leave my brand alone, vs. “let’s sue the “X@#!%X’s”
  - Don’t hesitate to litigate, but….
  - If primary goal is always litigation, this dictates specific tools/technologies, and procedures
- Combinations of technologies, the so-called “layered defense” (which can also include offense)

Tolerance Curve Concept
(2)

CORPORATE LIABILITY ??



Tactical Factors

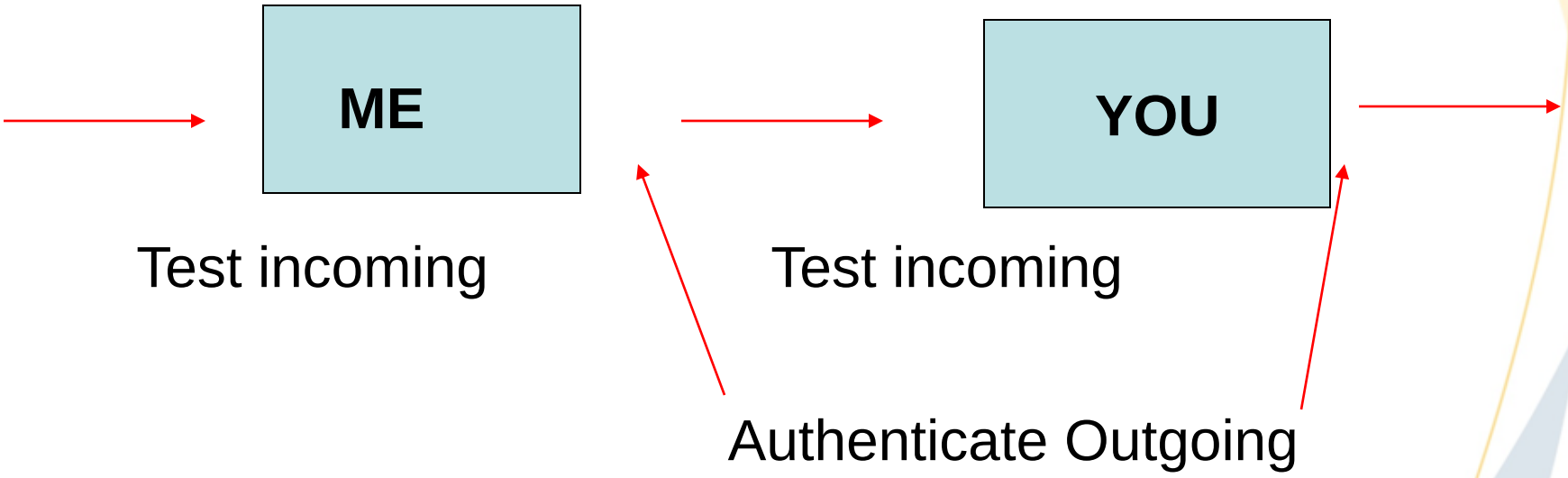
- “Step outside of (your) box”
- Understand the counterfeiters
- Get/stay nimble
- Ask questions to encourage cross-pollination
- Maximize variability in your defenses
  - Variable technologies
  - Layers and change

Levels of Attack

- Forgery of product and its packaging and labeling, including Re-mark to a higher level
- Re-use genuine packs and labels..with counterfeit products
- Re-package out-of-date or reject products in fake containers
- Use unauthorized, look-alike or registered brand names with a counterfeit product
- Hijack the entire brand

From Commerce Report

- Interface, communicate



How ?

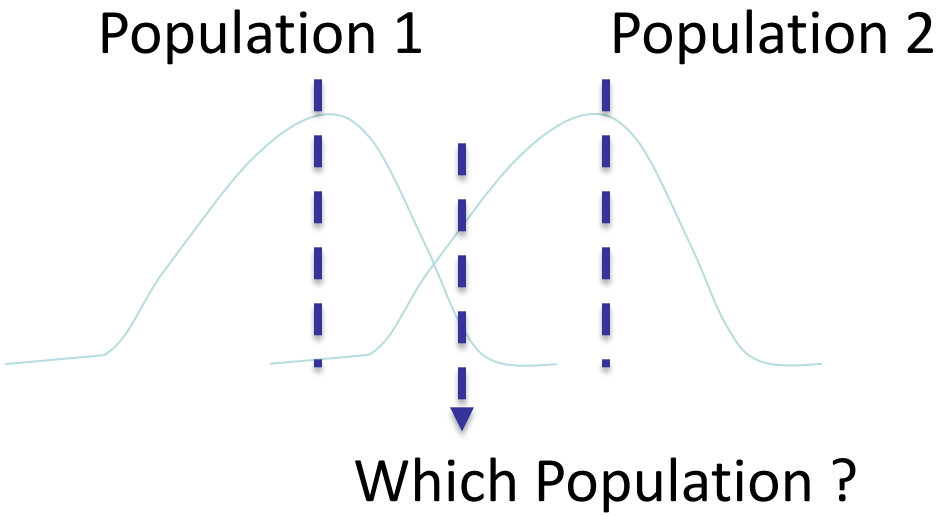
- We all use statistical methods for analysis
  - Compare two populations by using test results of parametric data
  - Critical assumption: both populations are authentic products
    - Still have possibility of type 1 or type 2 errors

- Authentication methods would introduce a new parameter to authenticate BEFORE standard parametric testing

Current Game

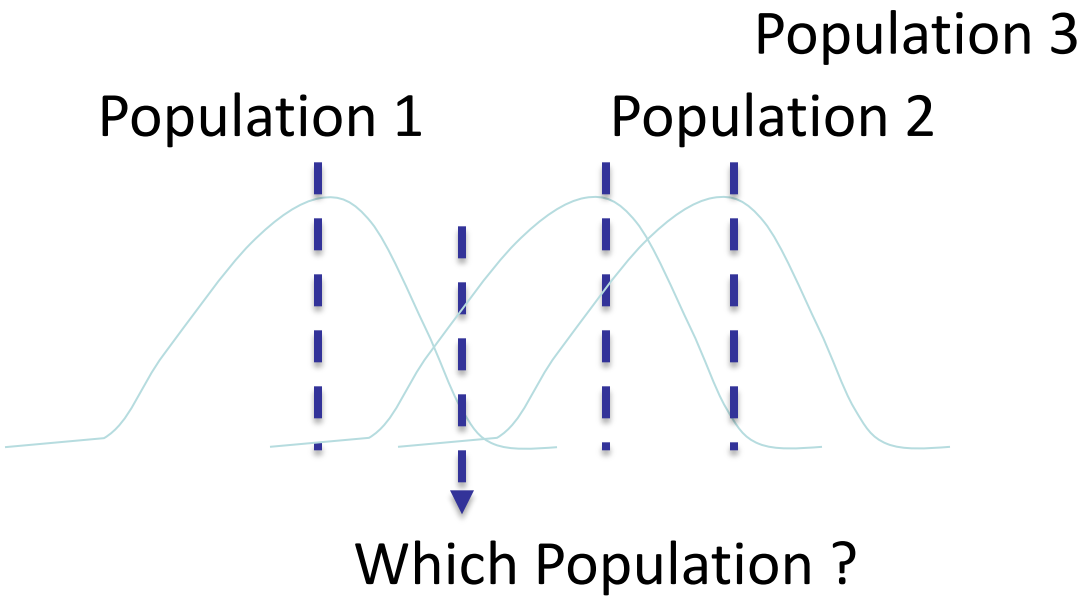
The "Maginot Line Syndrome"?

- SPC.."6 Sigma"…
  - DEFENSIVE STRATEGIES ??



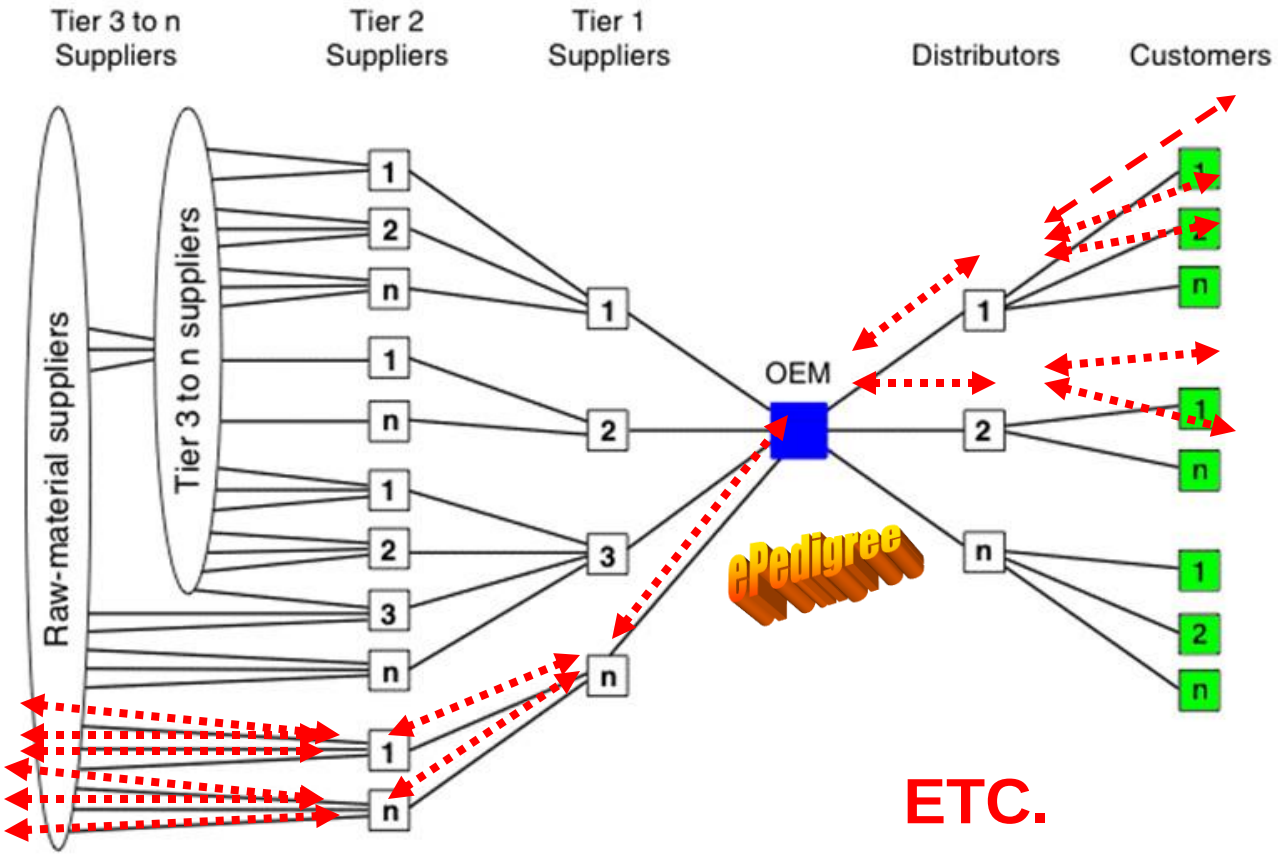
GAME CHANGE !!

- CHANGE THE ATTRIBUTE(S)
  - 1st question: Is it genuine
  - THEN 2nd question: Is it within specifications?
- Is this possible without massive “re-tooling” ?

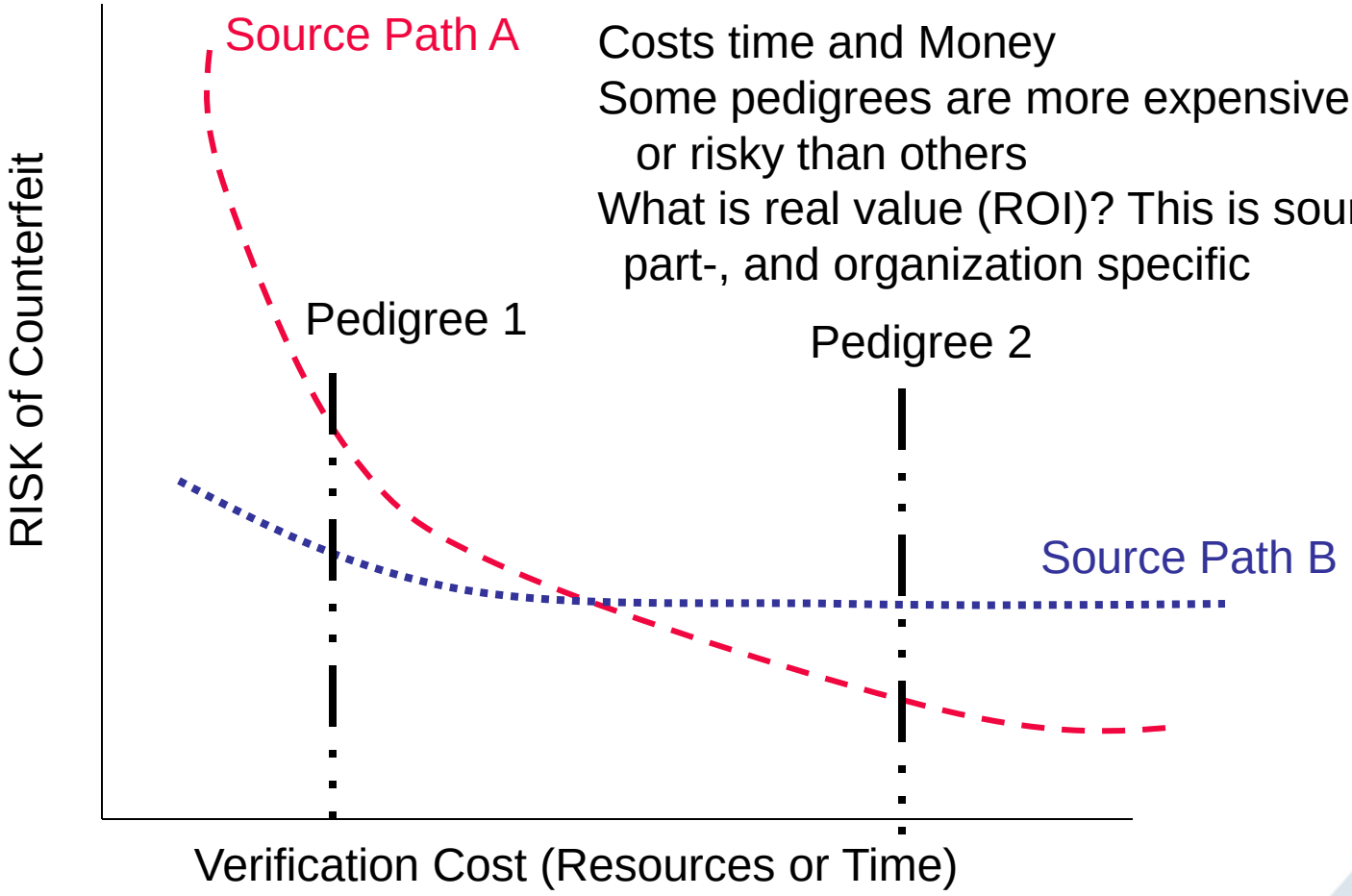


No Feature=FAKE

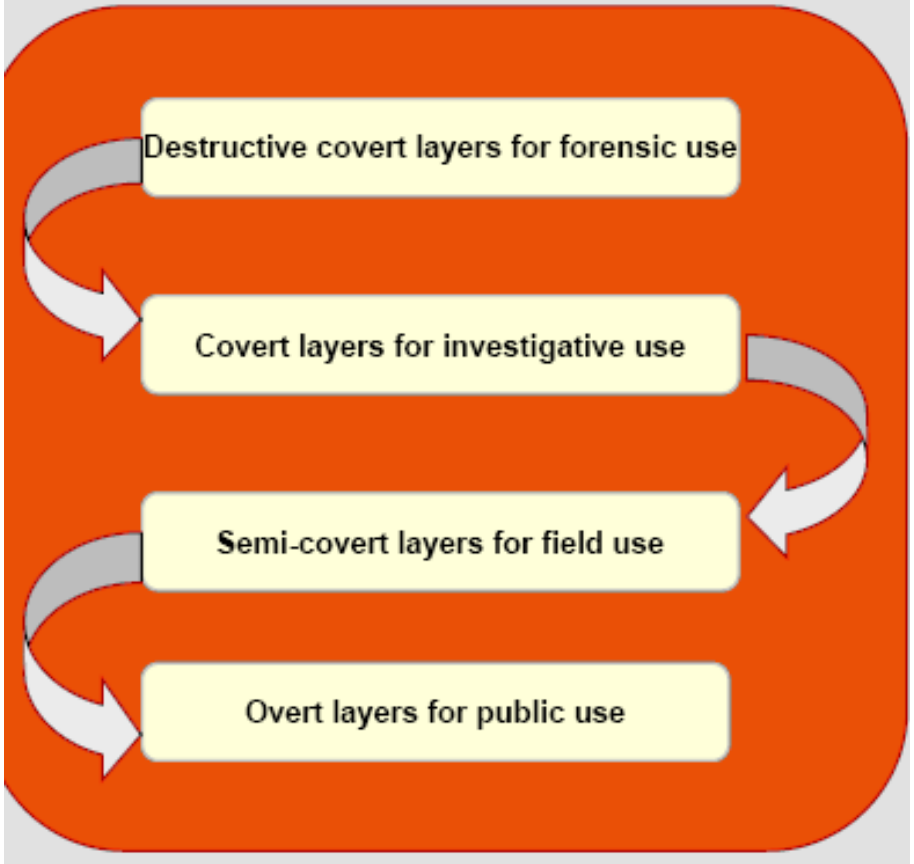
One model of Distribution



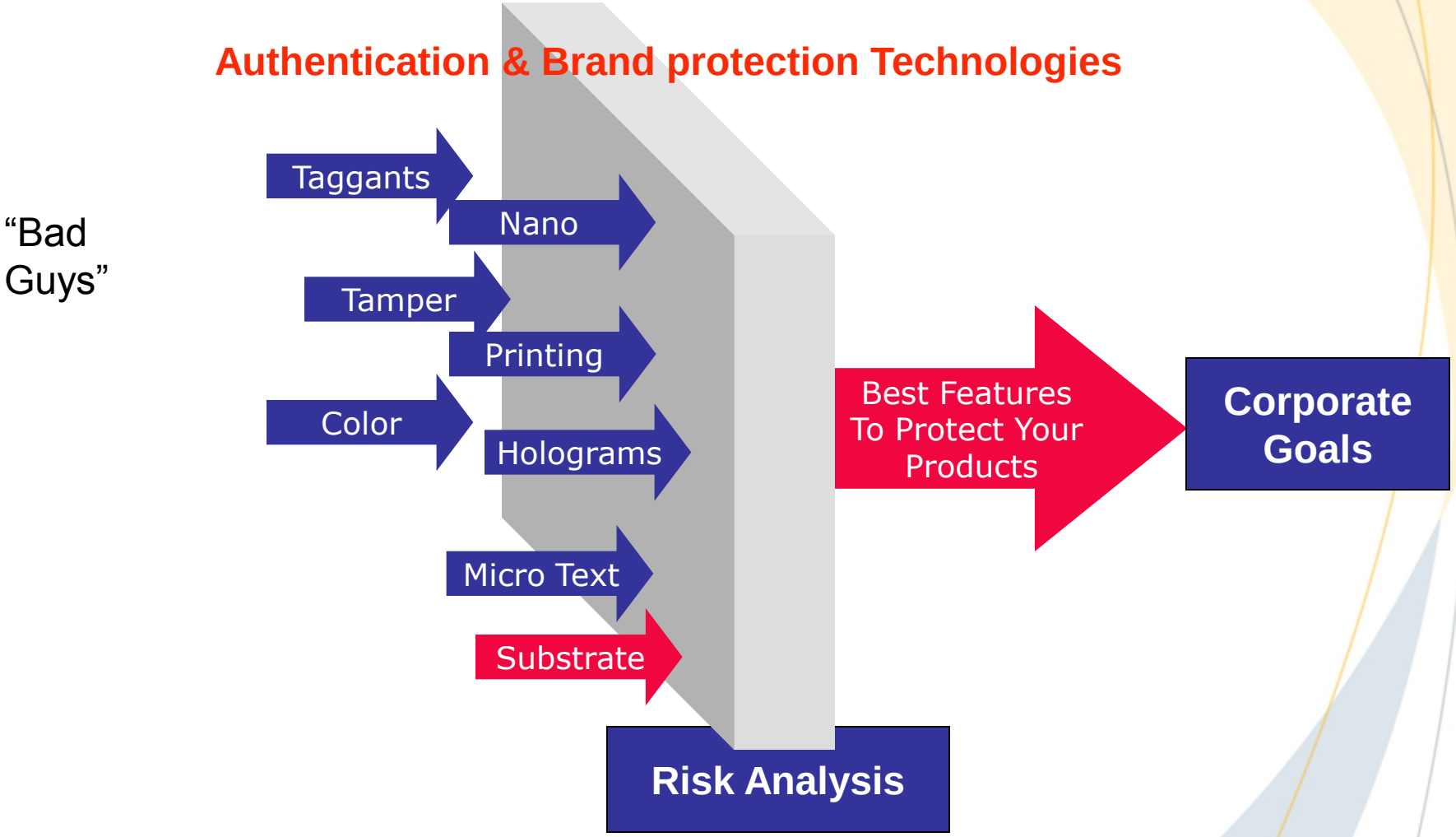
Cost/Risk Assessment (and Know Your Product's Impact)



Layers of protection are successful……



Overview of Choices
Risk Analysis—Corporate Goals



NEMA Matrix

Technology Choices vs Goals

Tecnology Choice vs. GOAL	OVERT	Covert	Forensic	Digital
Pursue legal actions			XX	XX
Investigations/Work with Enforcement		XX	XX	XX
Inform & Educate Public	XX			

Building Blocks

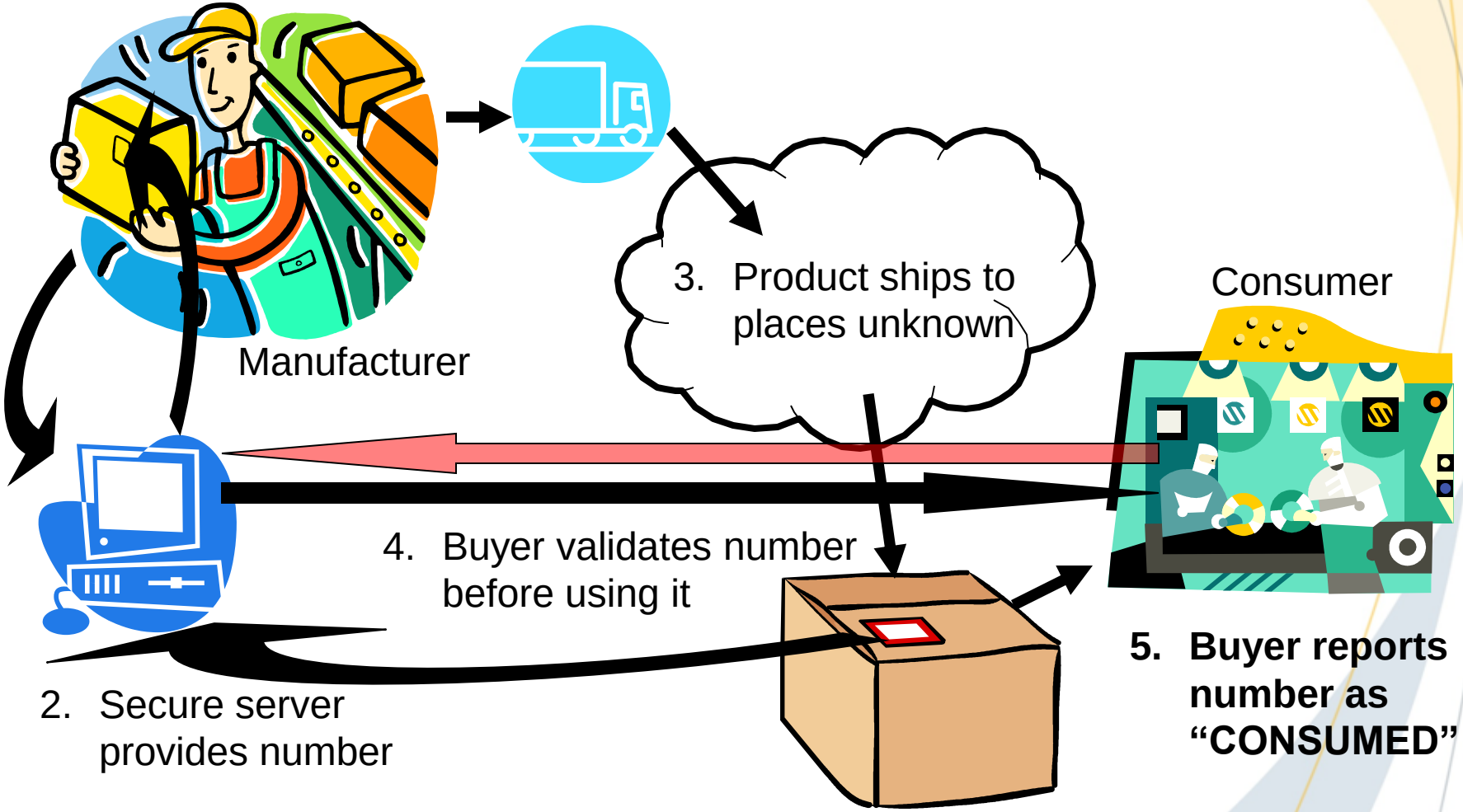
- Technologies are available to help detect, deter, and prosecute
- View counterfeiter as business competitor
  - Increase their cost of doing business…go bother easier victim
  - But..don't hesitate to litigate
- Variability is our friend
- Identify everything you can
  - Especially as far back as possible in the manufacturing process
- Allow for evolution of technologies without disrupting previous work

Consider a Few..

- Information strategy
- Use of a label..I thought it was a sticker?!
- Track and Trace at the WIP level

INFORMATION is the tool

1. Manufacturer asks for encrypted number



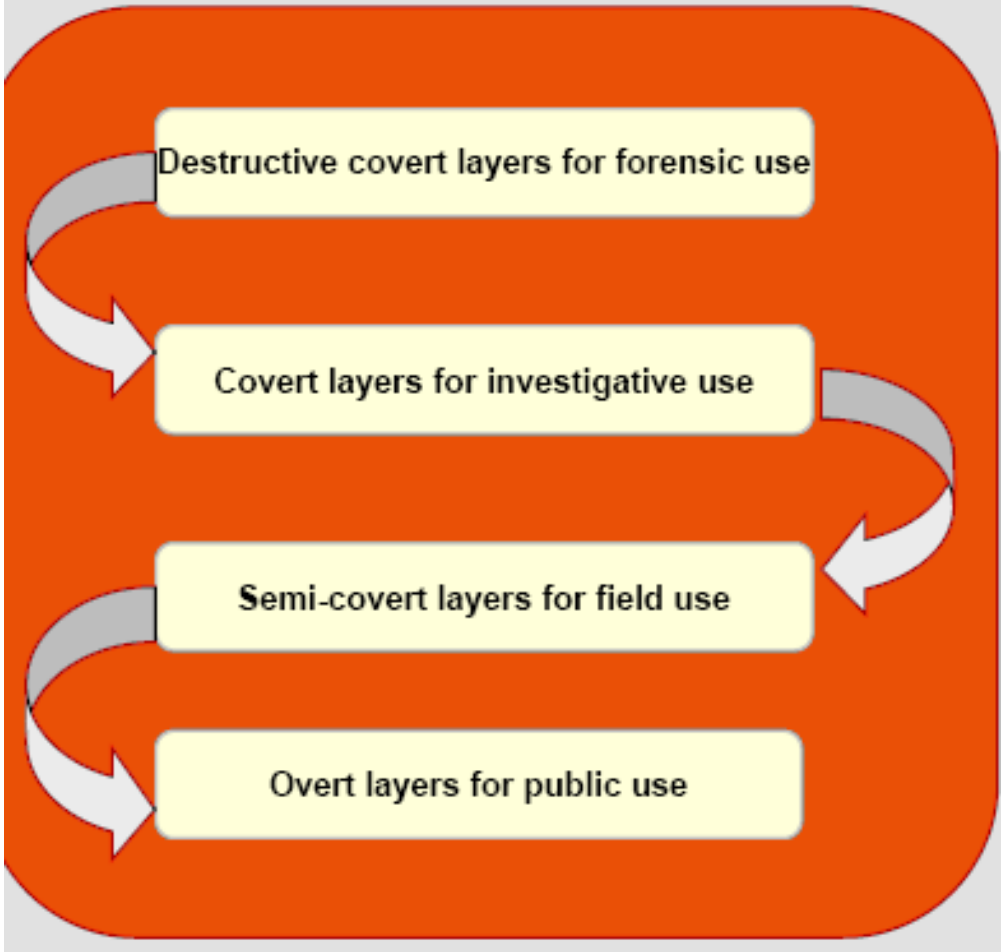
Adds Complexity to Counterfeiter's Business Model….
CHANGES the GAME

- Increases Risk of detection
- Increases his "R&D" costs
- The best defense is a good offense !!
- "Go pick on a different brand..?!"

New Rules for the New Game

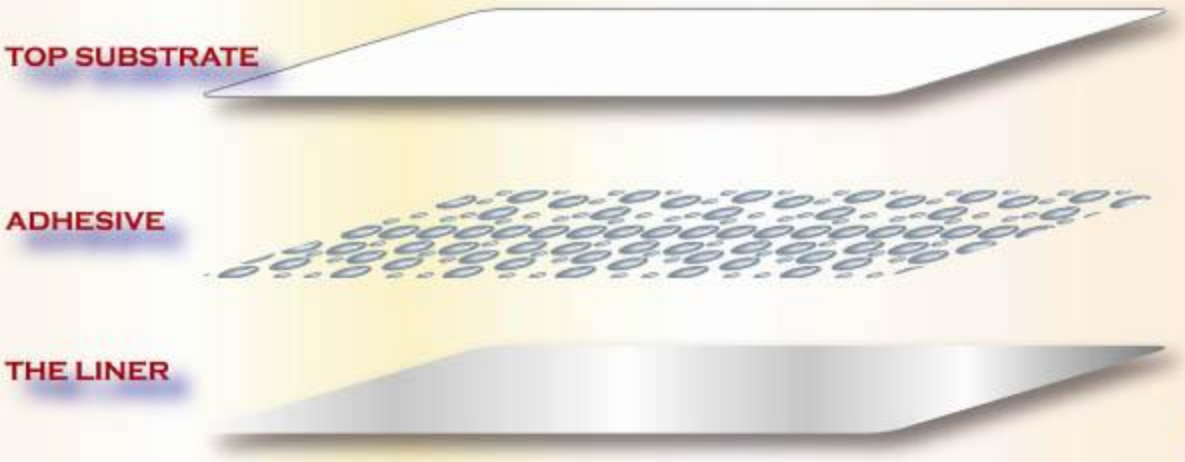
- "No single solution is impossible to imitate.”
- A strong fight against counterfeits combines a number of technologies.“
  - …. with covert technologies … the average [consumer] is unable to determine whether a package is authentic or not.
- "An authentic package does not guarantee an authentic product."
  - A viable solution will combine technologies on the package and in its contents….even in the accompanying leaflets.

LAYERS OF PROTECTION



OVERALL CONSTRUCTION OF A SECURITY LABEL

Standard Label Construction



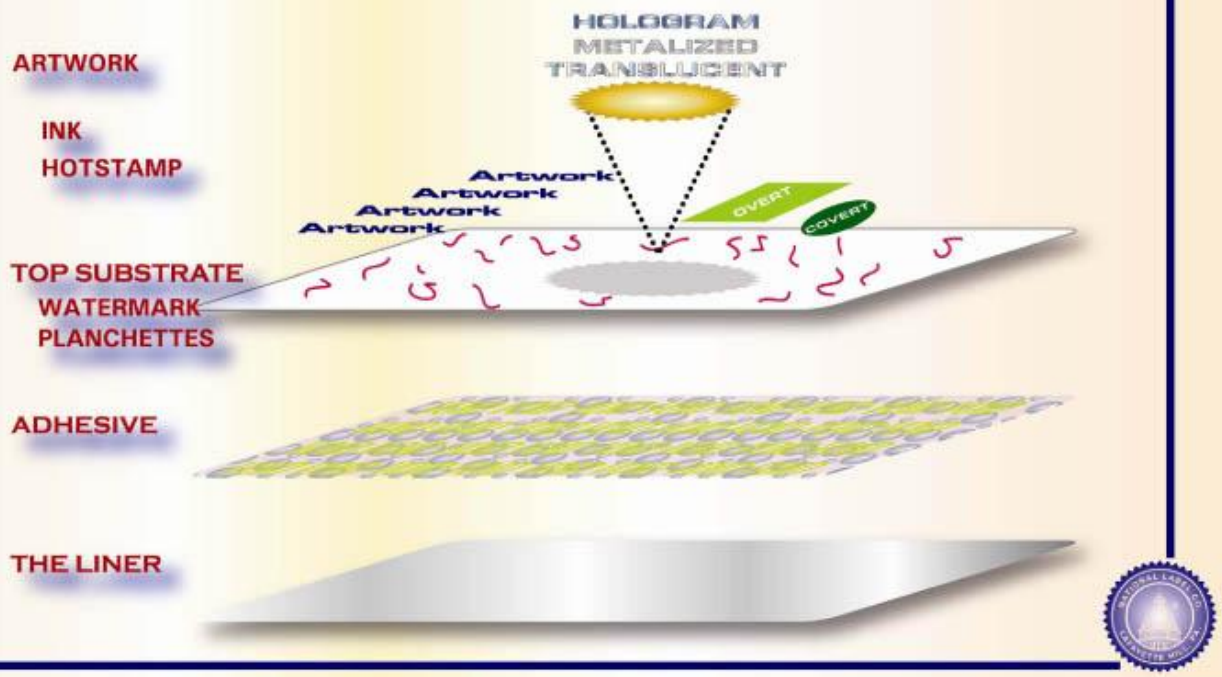
Incorporation of Authentication Features

- Key to definition is the matching of corporate goals with the risk assessment for each product
- If you “think it’s in the ink”….you are limiting your opportunities
- Utilize the “layered construction” of a security label
  - It’s a composite, multi-layered construction..not just a ‘sticker’
  - Each layer is a delivery system for authentication technologies
  - You can begin without additional investment in highly sophisticated digital printing equipment

OVERALL CONSTRUCTION OF A SECURITY LABEL

Holograms

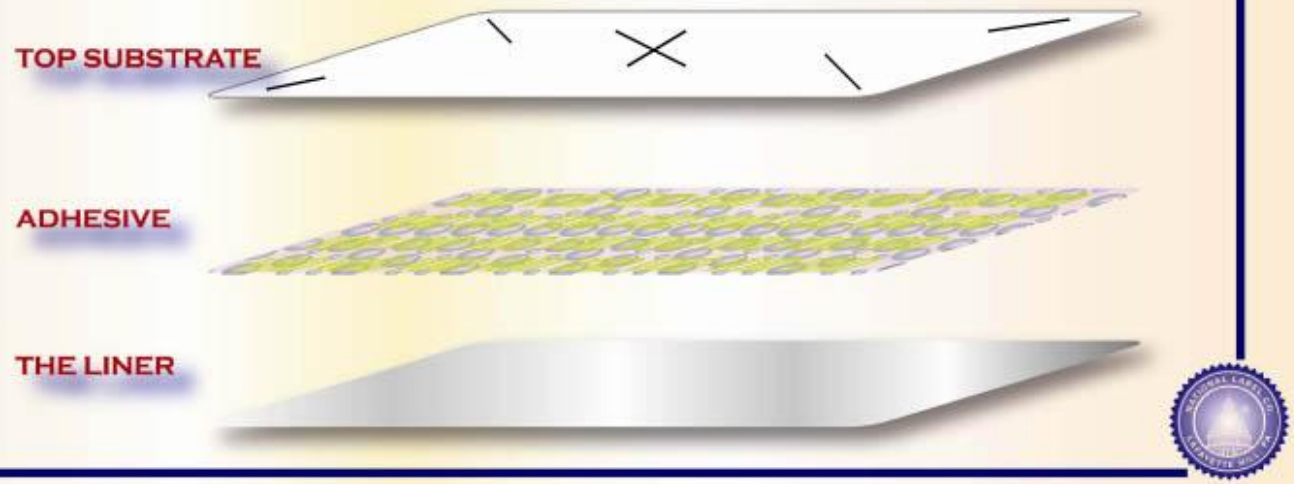
Can be added via Hot Stamping, in the Substrate, or in the Laminate



OVERALL CONSTRUCTION OF A SECURITY LABEL

What about the Die Cut Substrate Layer?

- ***Die Cutting with Internal Die Cut Slits – creates a T/E label and the cost impact is minimal!***



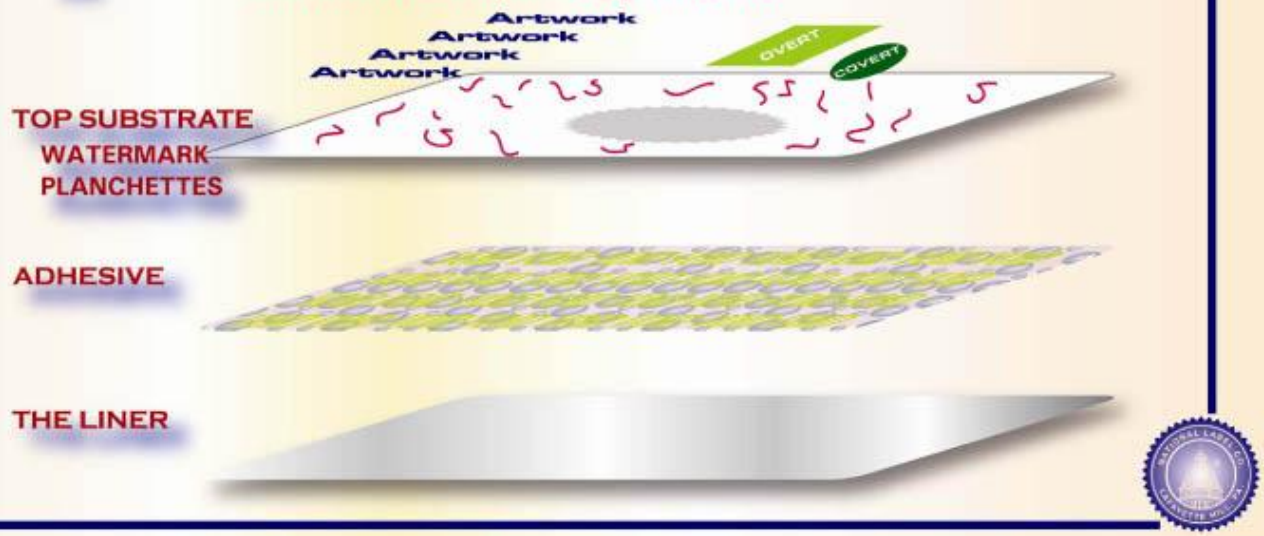
OVERALL CONSTRUCTION OF A SECURITY LABEL

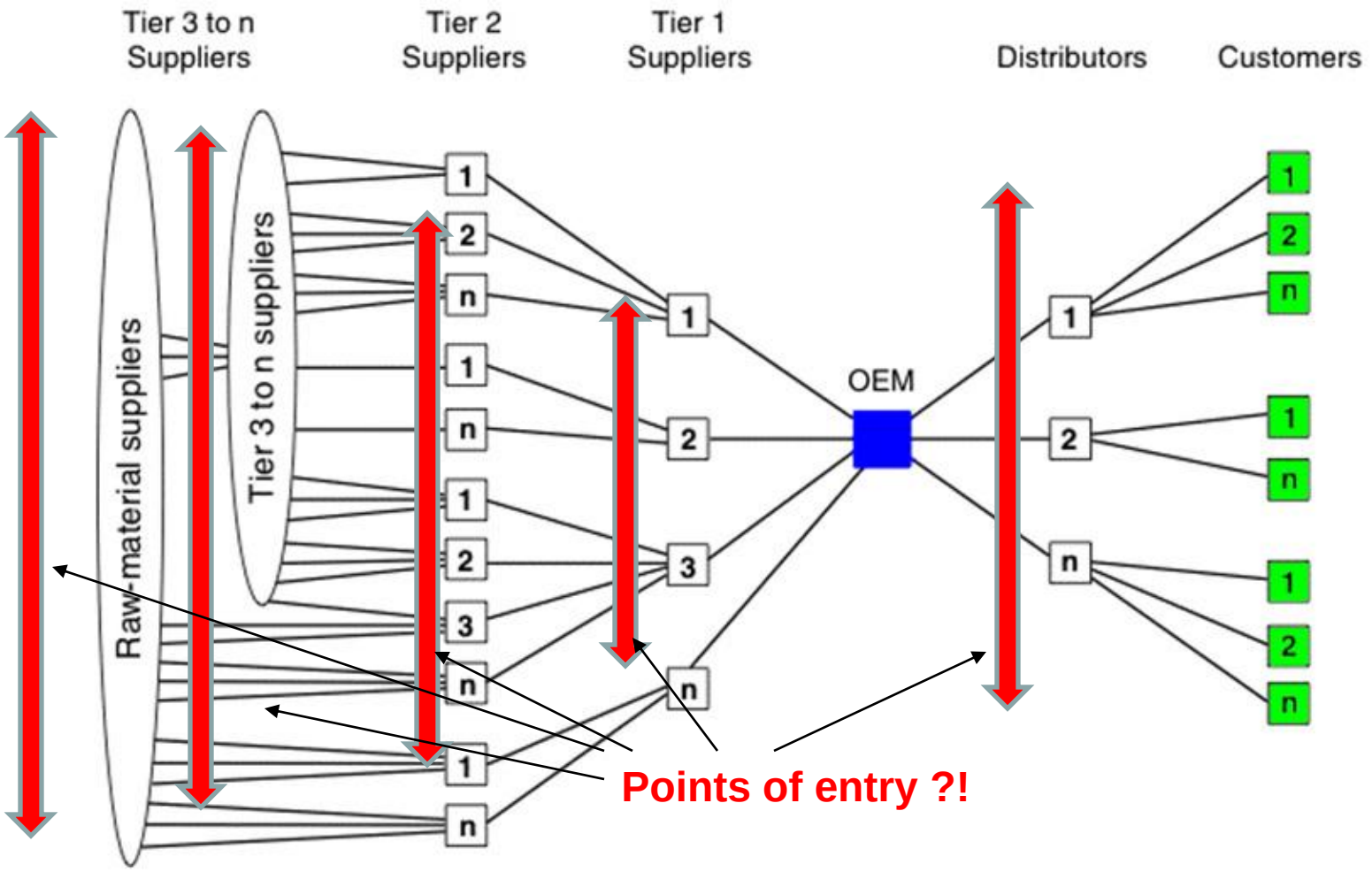
Ink

Various Overt and Covert options are available

Overt – OVI (optically variable / color shifting) Ink, Rainbow Colors, Reflective ink, Metameric Inks, Photochromic Inks, Thermochromic Inks, etc.

Covert – Scratch Off, Heat Sensitive, Microscopic Machine Readable Taggents, etc.



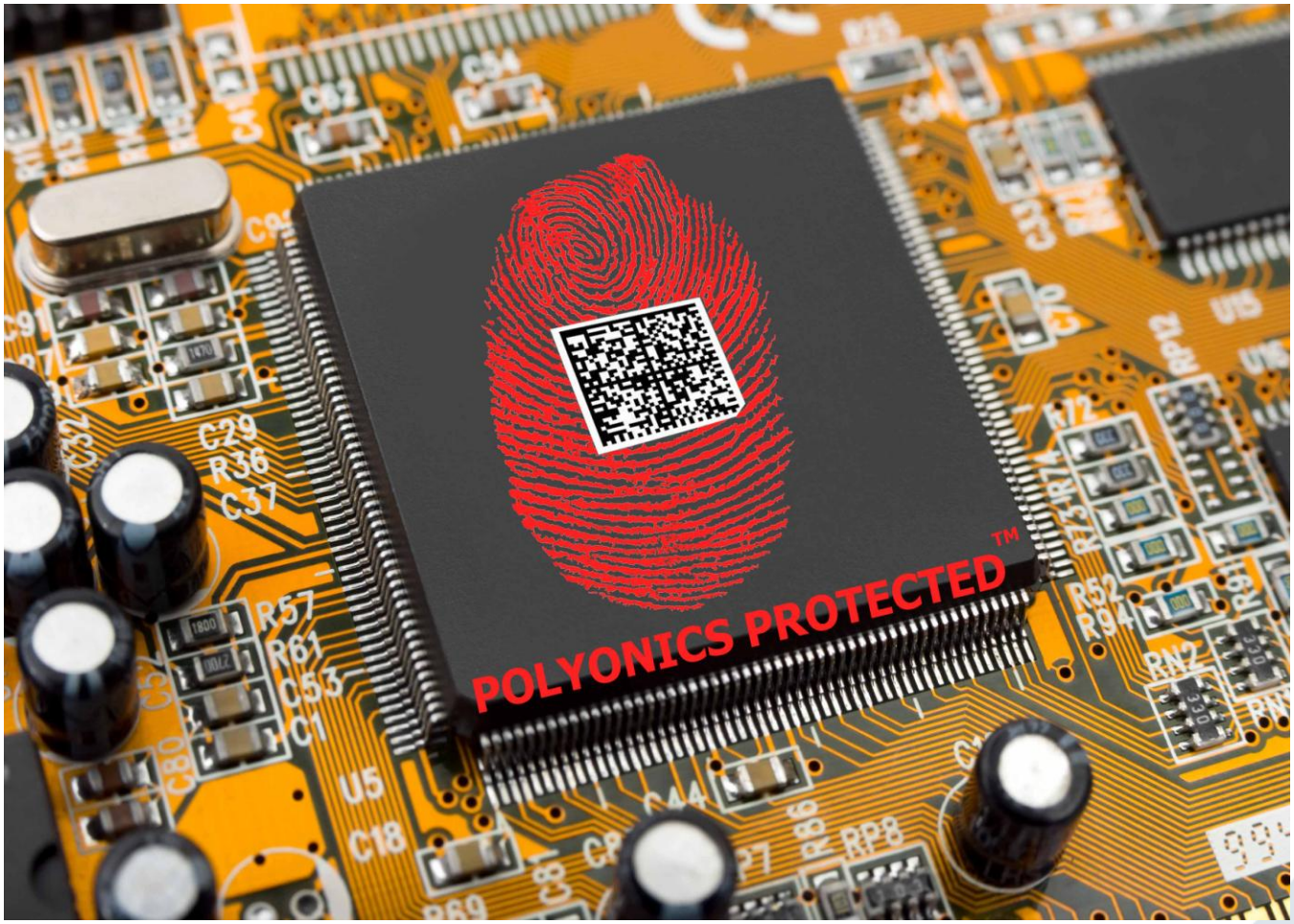

Tier 3 to n Suppliers
Tier 2 Suppliers
Tier 1 Suppliers
Distributors
Customers
Raw-material suppliers
Tier 3 to n suppliers
OEM
1
2
n
Points of entry ?!

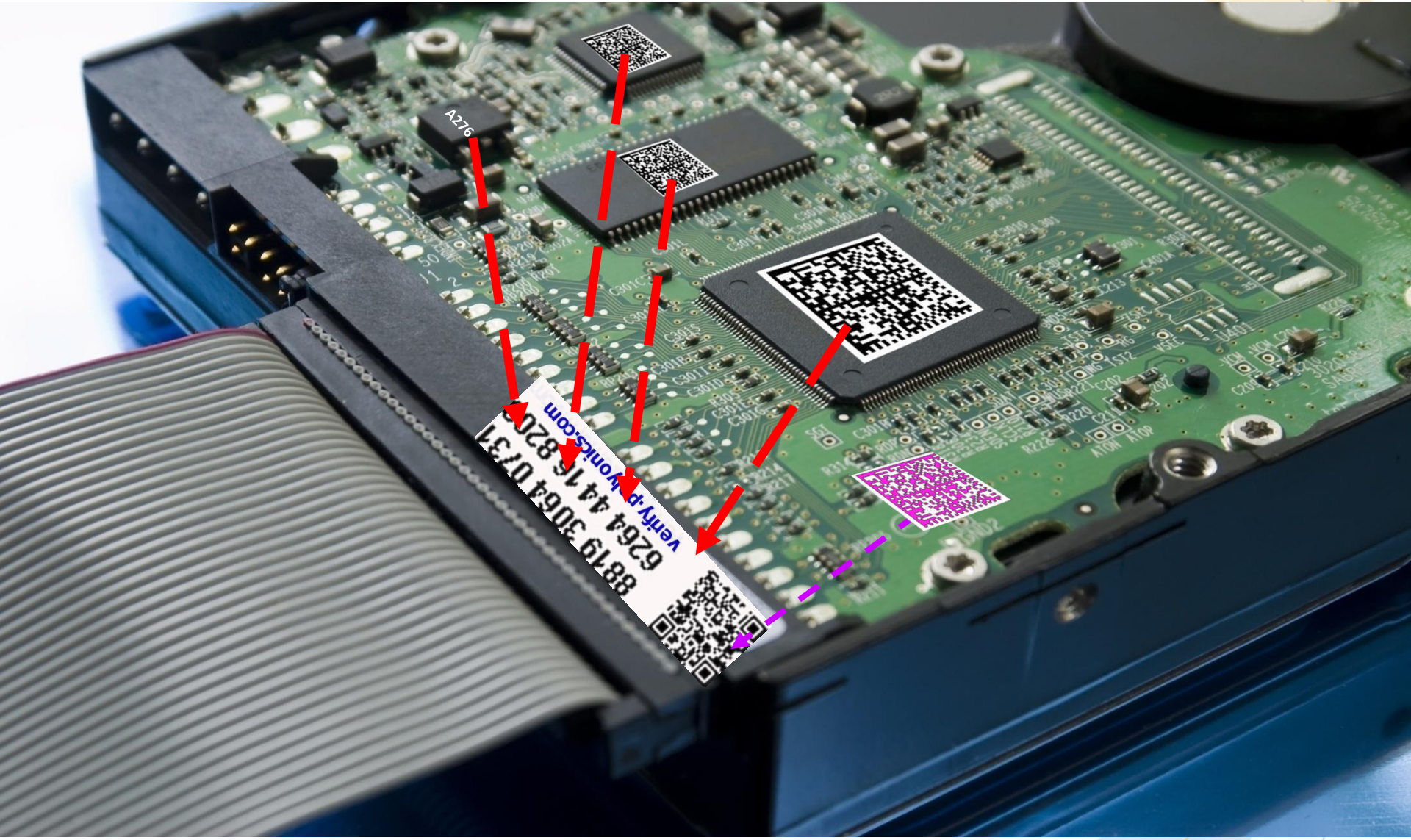
A PROPOSED STRATEGY…. TRACK and TRACE BEGINS WITH WIP !!!

WHY NOT INCORPORATE AUTHENTICATION DATA ?

- Electronics is a barcode intensive industry
- Routine AutoID for product data
  - Intimate use of data interchange between supply chain partners
  - Internal use of PRODUCT/PROCESS information for WIP control, scheduling, etc.

Authentication Begins with WIP




A276
verify.pkyonics.com

Takes Advantage of Strengths

- On the product…during the process
- One-to-one correspondence of product information with AUTHENTICATION
- Matches chain of custody with product function
- Takes advantage of existing AutoID technologies/systems
- Minimal additional costs…incorporate a different scanner..add a field of data….policies, procedures, training

- “Every participant in the supply chain can be a possible source of unauthorized parts and pass it on.

  The responsibility is on each “customer” in the supply chain [including internal customers] to protect themselves..”

  CALCE 9/2008

POLYONICS®

Many thanks to:

- **David Howard, *Johnson & Johnson***
- **David Brown, *Intel*..and others on the *SEMI ACTF***
- **Jim Colby, *HP***
- ***Dr. Steven Simske, HP***
- **Bill Kerns, *Microtrace***
- ***Jeff Strahl, HW Sands***
- **Neil Sellars, *National Label***
- **Gene Panger ..TUV Rheinland**
- **Debra Eggeman, The Independent Distributors of Electronics Association (IDEA)** www.idofea.org
- **CALCE (Center for Advanced Life Cycle Engineering)**
- **Elliott Grant, Yottamark**
- **Dan Harrison, IIMAK**
- **Brad Botwin, US Dept of Commerce, Office of Technology Evaluation**
- **Various people at Inksure, Sun Chemical, and Honeywell Security Products**

- Contact information: Jim Williams, Polyonics, Inc.
  - Phone 603-352-1415
  - Email jim.williams@polyonics.com