Securing The Supply Chain Through e-Pedigree

Security As A Quality Objective

The Shifting Marketplace

The drive to globalize pharma and biotech has created significant challenges in ensuring the integrity and security of the product supply chain

FDA Response

- Mandated that industry move to a solution which would provide traceability throughout the entire supply chain.
- From raw material supplier to the final customer - Industry must drive out risk from the process.

Recent Issues in the News

- Contaminated Heparin-Baxter
- Melamine in Baby Formula
- Medtronic Defibrillator Attack
- What's next ???

FDA Modernization Initiatives- Driving Change

- Critical Path Initiative – To “lean” the drug and medical device development process bringing safer, more effective products to market faster while reducing the candidate failure rate
- Risk Based cGMPs – regulatory oversight based on risk as well as the use of scientific manufacturing tools to reduce risk

FDA Action

- ***FDA News***

FOR IMMEDIATE RELEASE
P06-78
June 9, 2006 **Media Inquiries:**
301-827-6242
Consumer Inquiries:
888-INFO-FDA

FDA Announces New Measures to Protect Americans from Counterfeit Drugs

- The U.S. Food and Drug Administration (FDA) today announced new steps to strengthen existing protections against the growing problem of counterfeit drugs. The measures, which were recommended in a report released today by the agency's Counterfeit Drug Task Force, emphasize certain regulatory actions and the use of new technologies for safeguarding the integrity of the U.S. drug supply.
- "The adoption of the FDA Counterfeit Drug Task Force's recommendations will further reduce the risk that counterfeit products will enter the U.S. drug distribution system and reach patients," said Dr. Andrew C. von Eschenbach, the FDA's Acting Commissioner. "We must remain vigilant in our efforts to ensure our nation's drug supply is protected against an increasingly sophisticated criminal element engaging in a dangerous type of commerce."
- Among other new measures, **FDA will fully implement regulations related to the Prescription Drug Marketing Act of 1987, which requires drug distributors to provide documentation of the chain of custody of drug products -- the so-called "pedigree" -- throughout the distribution system.** FDA had placed on hold certain regulatory provisions because of concerns raised at the time about the impact on small wholesalers.

Industry Response: e-Pedigree

- **Wait And See Attitude** – Some action has been taken with a tactical focus. Strategic focus is lacking
- **FDA** - Has not really begun enforcing the e-pedigree solution – “Details” are still being worked out
- **ICH Q9** - International Baseline for Risk (http://www.ich.org/cache/compo/276-254-1.html)
- **IPEC** - Do a paper audit and create an audit trail for suppliers to demonstrate integrity
- **Industry**- Current technology solutions are too expensive ($1/unit of sale), yet emerging technologies show more promise as time progresses (FDA recently recommended a new technology solution- *Nanoink* which has potential for individual tablet ID).

FDA Response

- Focus on traceability through technology i.e:
  - RFID 
  - 2D Bar-Coding
  - Reliance on the current QMS as foundation for implementation

Pitfalls Of Technology Focus

- We have a tendency to make the project about the technology.
- The challenges in getting technology to work causes us to lose sight of the associated systemic risks.
- Once we have the most challenging technology “assets” working, we declare victory (or at least take a long break).

RFID Passport Case Study

- RFID Passports presented a large technology challenge – Secure RFID Tags
- Current RFID Passport tags have robust security
- Attacker focused on the reader/database and told the database to accept a bogus passport as legitimate (http://arstechnica.com/news.ars/post/20080807-faking-passport-rfid-chips-for-120.html)
- RFID Chip (The Focus) was not attacked. Attacker simply shifts **His Focus** to something else.

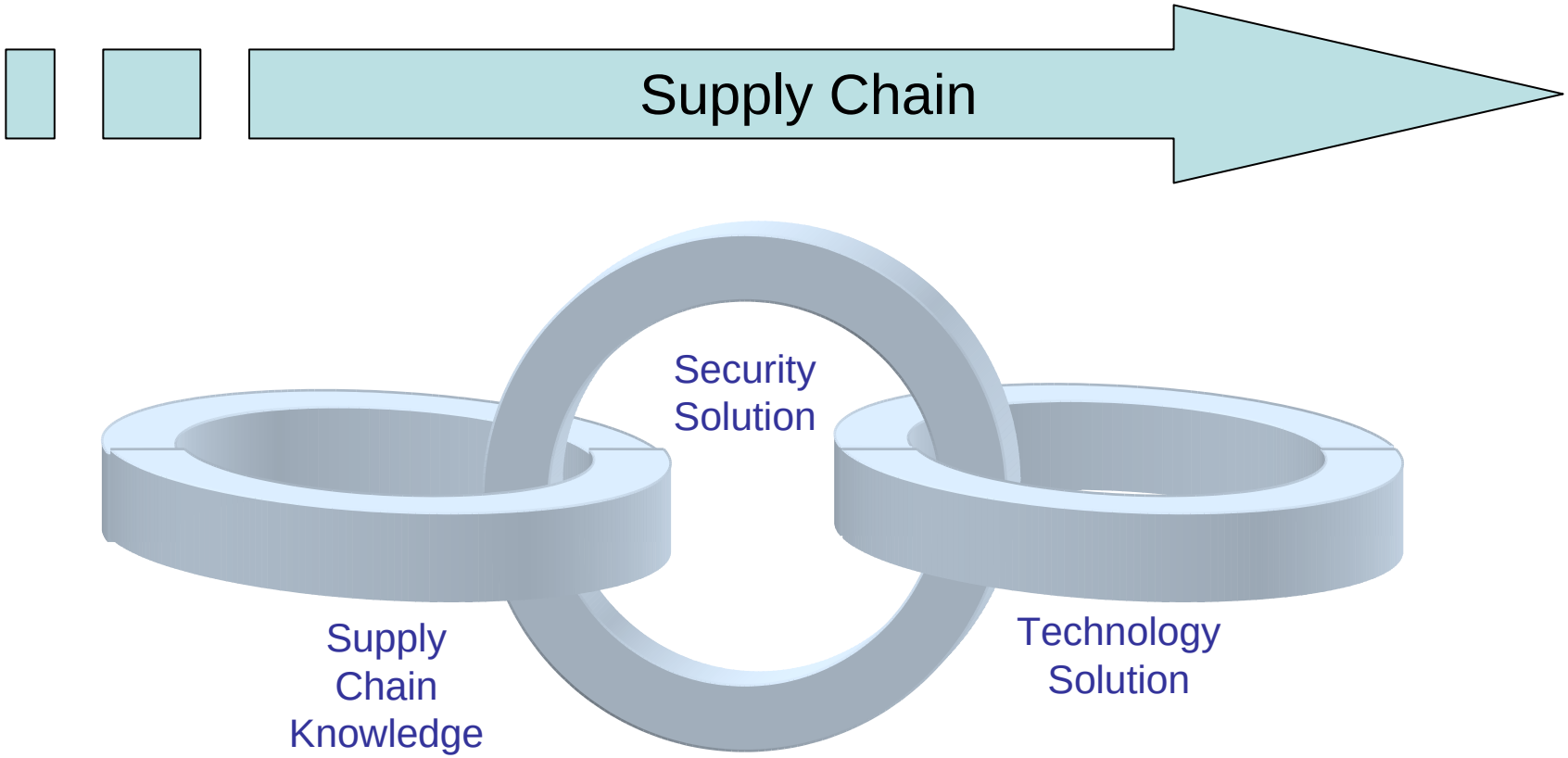
We Can Look At Some Past Examples Of Security Failures And Their Impact

- **Tylenol Cyanide Poisoning: $100 Million Recall !**
- **9/11: We Are Still Dealing With This**
- **Electronic Voting Machines: Hot Topic !**
  - One Manufacturer Believes That They May Never Be Able To Sell Another Electronic Voting Machine Even If They Fix The Security Problems.
  - Diebold Is Trying To Divest Itself Of All Electronic Voting Machine Assets.
  - Media Reports Still Circulate About Electronic Voting Machine Manufacturers Being Part Of A Conspiracy To Defraud The Voting System.

The Challenge

- We are no longer worried about drug diversion as the primary endpoint
- We are worried about the diversion of data.
- This is our Achilles Heel.
- Technology is only part of the answer.

The Key to a Successful E-Pedigree System



Leveraging ICH Q8 and Q9

- Understand the drivers for variation in the process
- Understand the risks in the process
- Mitigate the risks in the process
- Use the right tool to drive down the risk of failure

A Marriage of Equals?

- Is it possible to be successful without giving equal consideration to all three components of e-pedigree (security, technology and supply chain)?

- Ultimately this must be managed like any quality program:
  - Define the process
  - Measure the process
  - Monitor the process

Defending The Subversive Business Model

- **Early Attempts To Control Illegal Drugs (Pre-Internet) Focused On Getting Local Police To Crack Down On Operations (Colombian Drug Lords, Mexican Farms, Opium Fields)**
- **Drug Dealing Cartels Responded With Brute Force (Firepower).**
- **Security For Drug Enforcement Agencies Became An Extremely High Priority As A Result Of This Backlash.**
- **Drug Cartels are still growing and still quite strong despite DEA efforts (http://abcnews.go.com/Nightline/International/story?id=1477964)**

ePedigree Is A Tool To Address The New Drug "CyberWar"

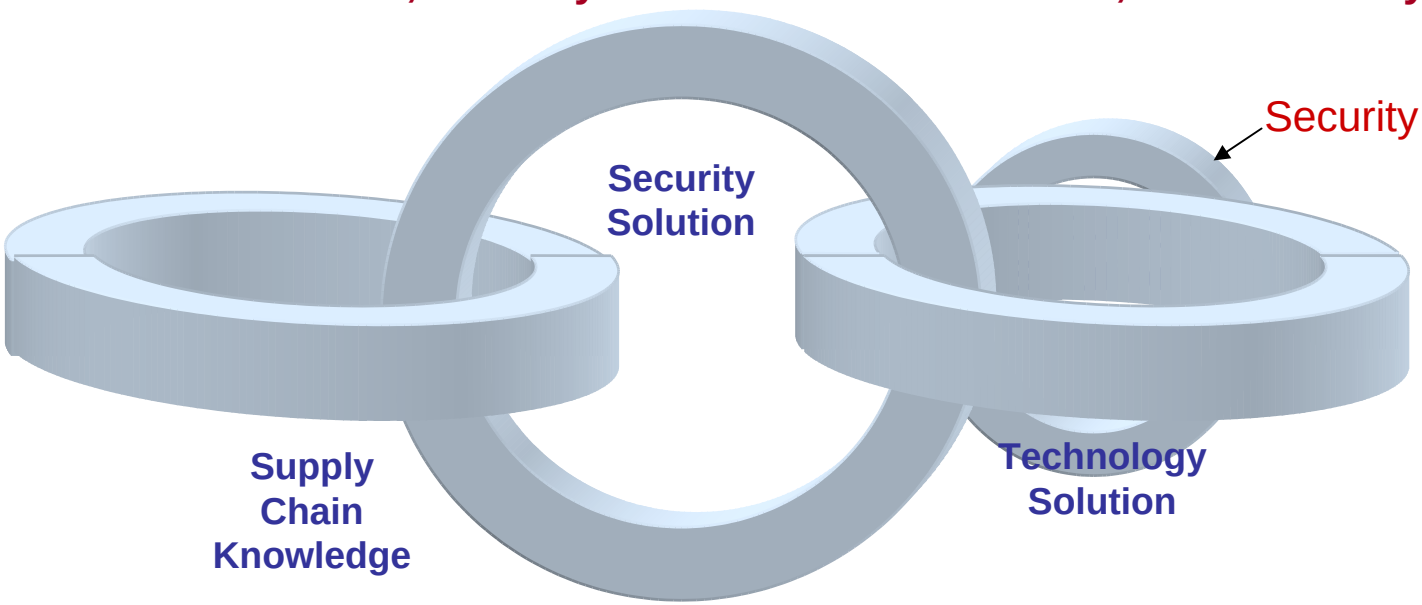
- **Illegal Drug Dealing Has Moved From The Streets To The Desktop.**
- **The World Health Organization estimates global sales of counterfeit medicines at $35 billion to $40 billion a year. (http://www.america.gov/st/washfile-english/2006/November/20061116193712xJatiA0.7200128.html)**
- **Drug Dealers Are Now Arming Themselves With Hackers As "Soldiers" In Their "Armies".**
- **The reality is, the pharma information infrastructure is easy to penetrate.**
- **We must look to our technology infrastructure when assessing the security of our supply chain**

Classical Approach to Security

Security Management Is Grouped Within IT/Engineering (Technolgy).

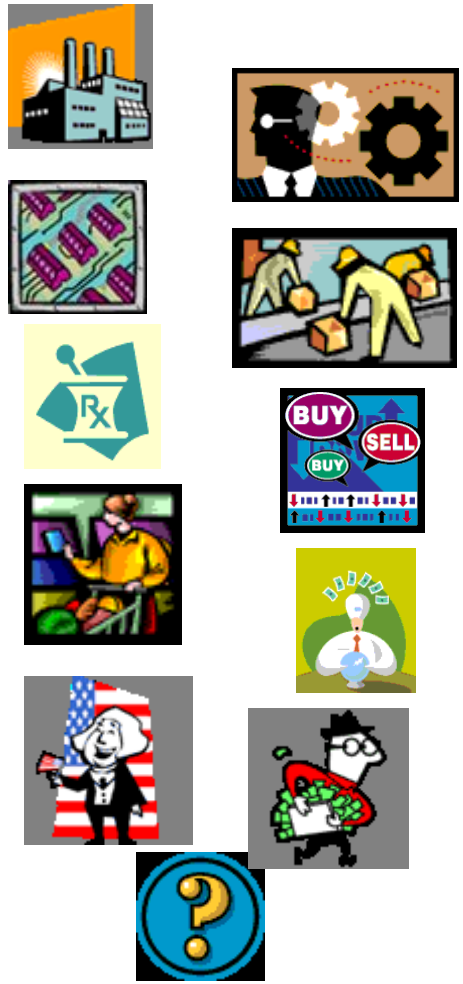
The Result Is Often A Weaker Or "Watered Down" Security Implementation.

As Resources Become Strained, Security Is Watered Down Further, Or Effectively Eliminated.



What Is The Impact Of A Security Failure ?

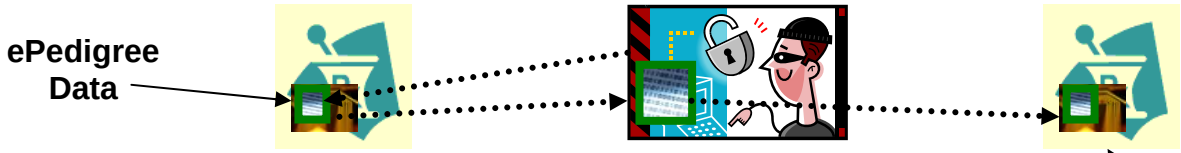
- **Who Are The Stakeholders ?**
  - Manufacturers
  - Integrators/Consultants
  - Technology Providers
  - Distributors
  - Pharmacists/Doctors
  - Stockholders
  - Consumers
  - Taxpayers
  - Government
  - Counterfeiters
  - ?????????



How Is Each Stakeholder Affected ?

A Few Security Threat Examples (RFID)

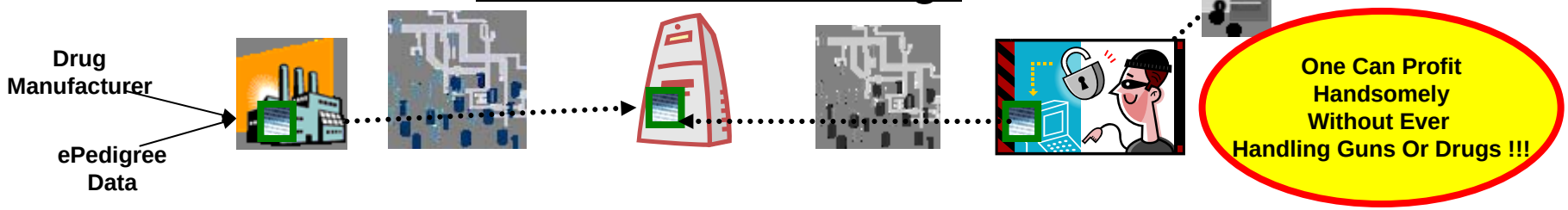
Cloning RFID Tags Or Data



"Snooping" RFID Tags

Data Transmission "Sniffing"

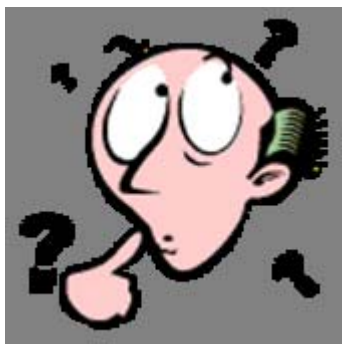
Database "Poisoning"



What Is The Impact Of A Security Failure ?

THE ANSWER IS…

WE DO NOT KNOW THE IMPACT OF A SECURITY FAILURE UNTIL IT HAPPENS

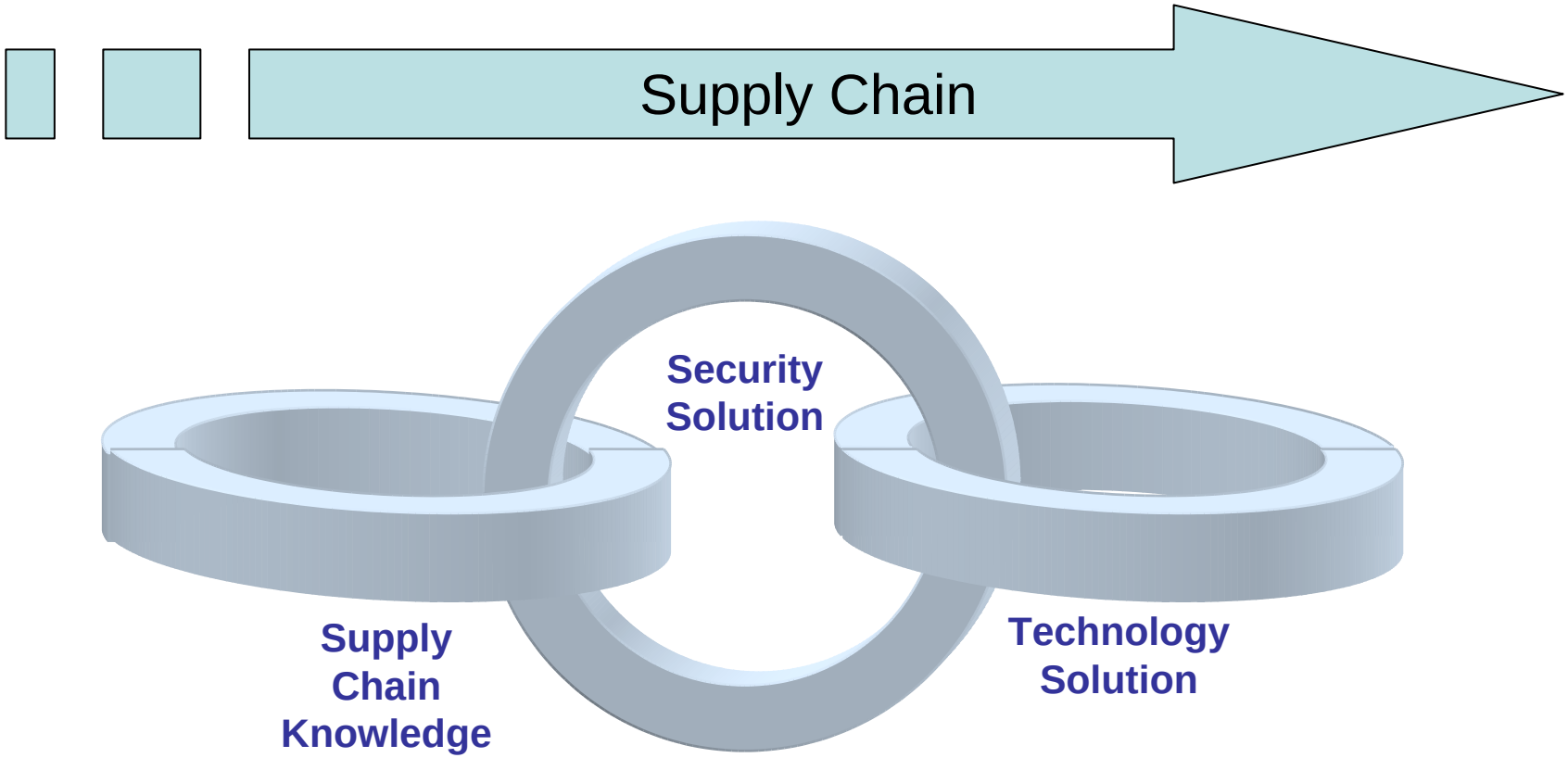


All We Can Do Is Try Our Best To ESTIMATE The Impact Of A Security Failure and Take Steps to Mitigate It

The 7 Deadly Sins Of Security

1. **Not Measuring Risk** – ***What You Don't Know Will Hurt You.***
2. **Thinking Compliance Equals Security** – Compliance = Compliance. Security Is A Process.
3. **Overlooking People –** The human side of things
4. **Too Much Access For Too Many –** User rights
5. **Lax Update/Patching Procedures** – Keeping it up to date
6. **Lax Auditing Procedures** – Making sure it is all doing what it should be doing.
7. **Spurning The K.I.S.S. Principle –** KEEP IT SIMPLE !!!

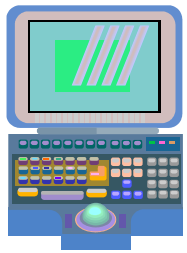
What Is Supply Knowledge?



Understanding the Supply Chain

- Key Components:
  - Procedures/Schedule
  - Personnel
  - Technology
  - Business Drivers
  - Transportation
  - Product Specifics:
    - Product indication
    - Container System
    - Current Traceability Architecture



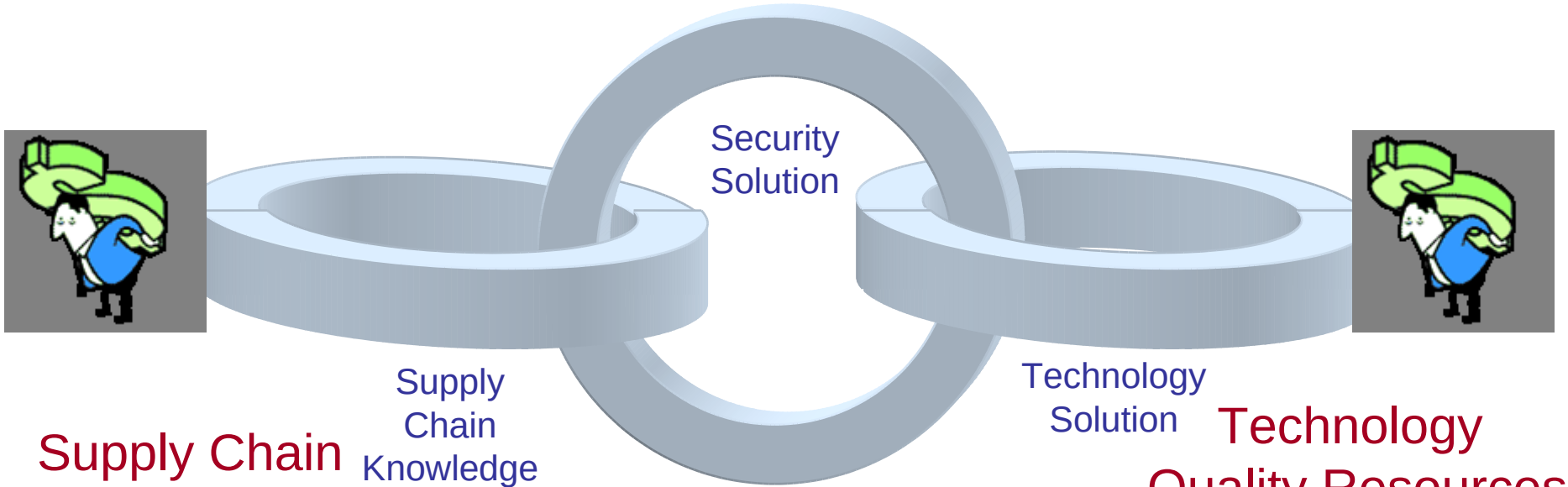


Diagnostic Techniques

- Value Stream Map:
  - Material
  - Information
  - Time
- Harmonization Requirements
- Regulatory, Import/Export Requirements
- Key Stakeholder Analysis

What Do We Do When Security Failures Occur ?

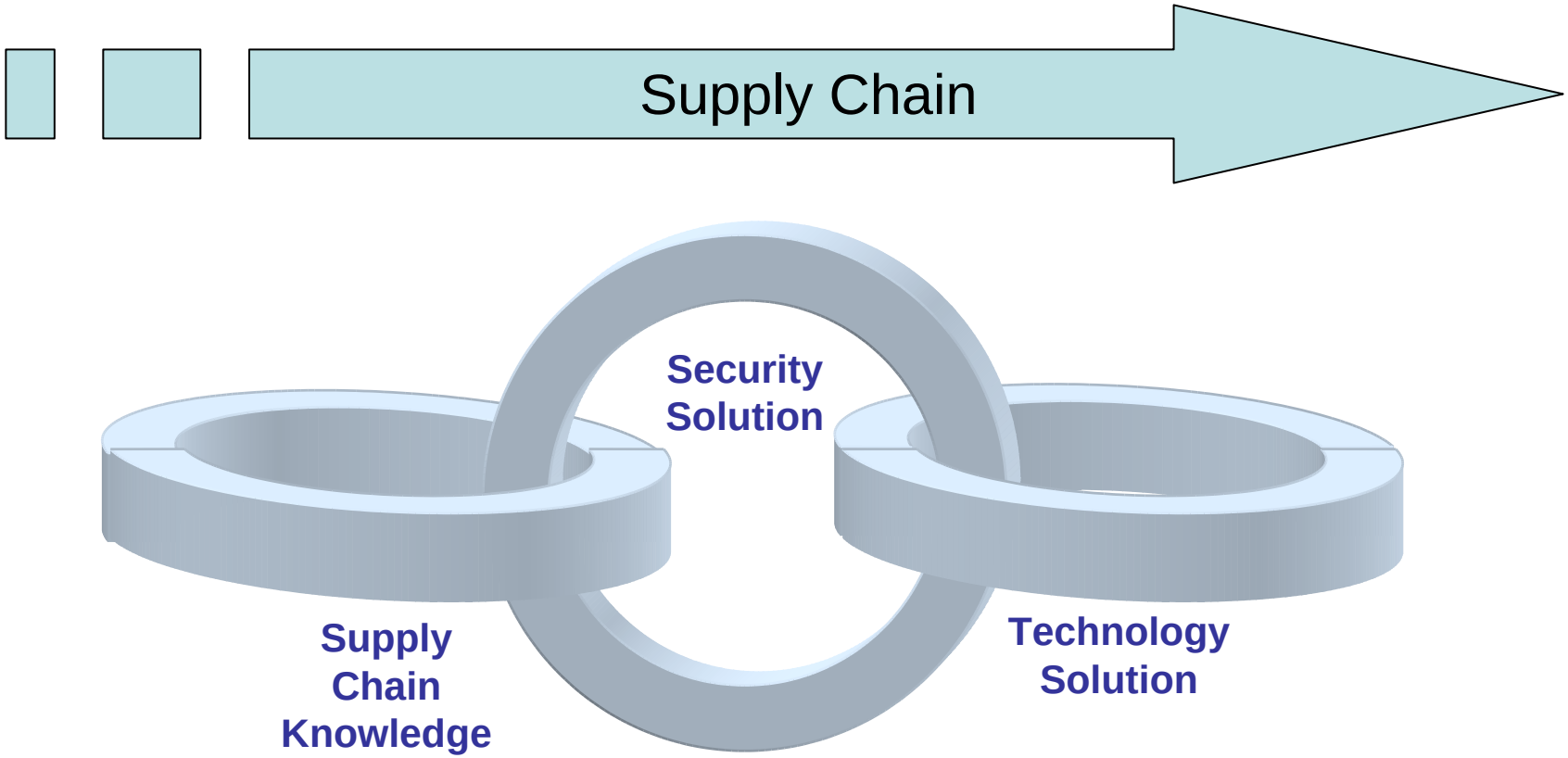
We Allocate A lot of Resources to Security Management



Supply Chain Quality Resources

Technology Quality Resources

What About the Quality of Security?



Risk Management

- In order to assess the quality of our security solution we must assess its capability to address the threats to the Supply Chain

- We must clearly understand the challenges EVERY stakeholder brings to the risk profile

Adopt Risk Management Tools

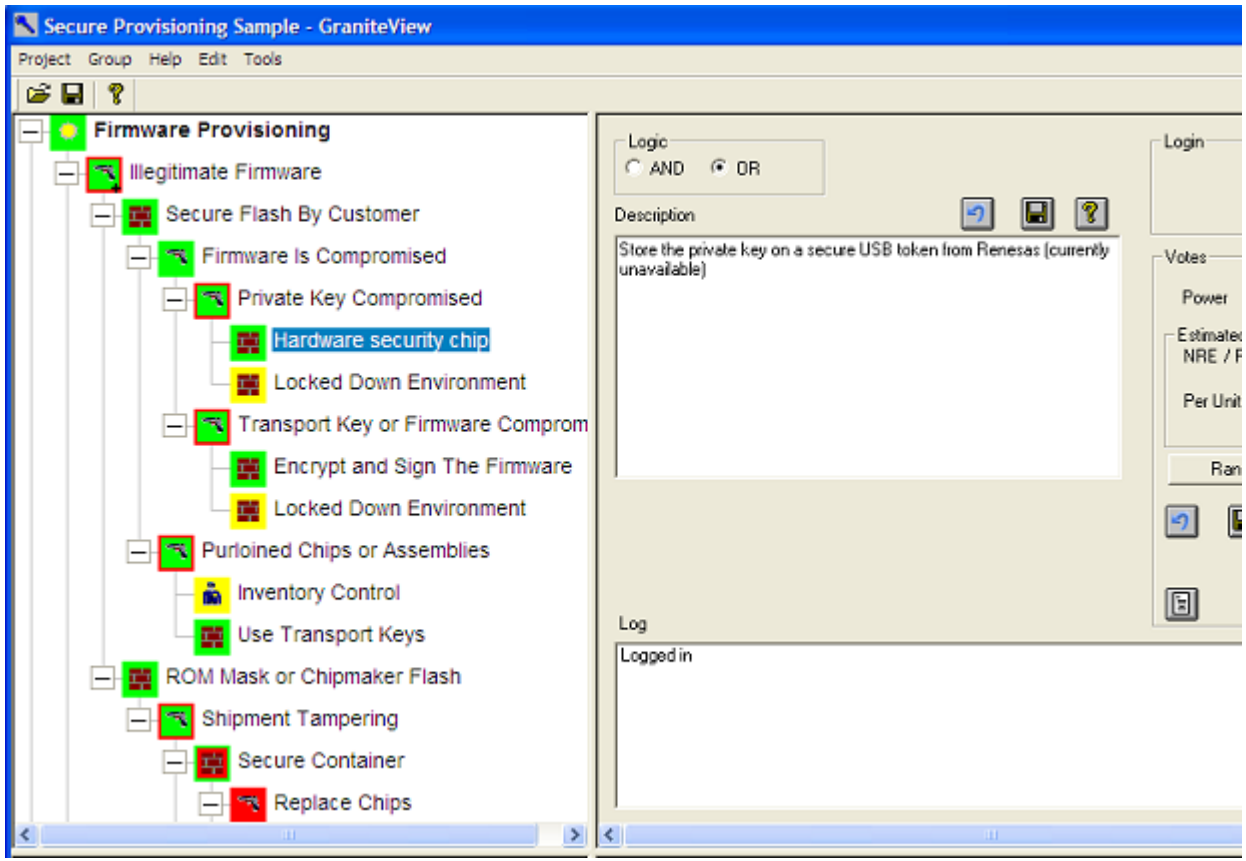
- Auxiliary Tools
- Fault Tree Analysis (FTA)
- Hazard Analysis and Critical Control Points (HACCP)
- Hazard Operability Analysis (HAZOP)
- Failure Modes and Effects Analysis (FMEA)

Failure Modes And Effects Analysis (FMEA)

- Failure modes and effects analysis (FMEA) is a step-by-step approach for identifying all possible failures in a design, a manufacturing or assembly process, or a product or service.
- “Failure modes” means the ways, or modes, in which something might fail. Failures are any errors or defects, especially ones that affect the customer, and can be potential or actual.
- “Effects analysis” refers to studying the consequences of those failures.
- Failures are prioritized according to how serious their consequences are, how frequently they occur and how easily they can be detected. The purpose of the FMEA is to take actions to eliminate or reduce failures, starting with the highest-priority ones.
- Failure modes and effects analysis also documents current knowledge and actions about the risks of failures, for use in continuous improvement. FMEA is used during design to prevent failures. Later it’s used for control, before and during ongoing operation of the process. Ideally, FMEA begins during the earliest conceptual stages of design and continues throughout the life of the product or service.

Description Taken From http://www.asq.org/learn-about-quality/process-analysis-tools/overview/fmea.html

Threat Modeling: The Security World Equivalent Of The FMEA



- Collaborative Visual Representations of Threats, Countermeasures, and Business Processes
- Determine Objectives Before Technological Choices
- Scenarios Around Security/Cost Tradeoffs
- Build a Security Roadmap

Conclusions

- Despite industry ambivalence e-pedigree is a looming issue for Quality professionals
- We must look beyond the technology solutions and rely upon a systems approach in order to identify and mitigate weaknesses in our supply chain
- As Quality professionals we can leverage our existing QMS system to press the issue:
  - Deviations, NC, CAPA programs are just a few that can dictate, within the framework of a objective risk based system, a path to identification and mitigation

Thank You For Your Attention!

Bikash Chatterjee
bchatterjee@pharmatechassociates.com
(510) 732-0177 x302

Mike Ahmadi
mike.ahmadi@granitekey.com
(925) 413-4365