THE IIA



The Rise of Economic Espionage
&
Breaking the NYNEX Case

Dallas, Texas, May 14, 2008

Presented on behalf of The Institute of Internal Auditors

by
MacDonnell Ulsch
Jefferson Wells

Biography: MacDonnell Ulsch

- Director, Technology Risk Management, Jefferson Wells.
- Privacy and economic espionage specialist for the firm.
- Author of “Threat! Managing Risk in a Hostile World,” published mid-2008 by The Institute of Internal Auditor Research Foundation.
- Served on the United States Secrecy Commission under Sen. Daniel Patrick Moynihan and Senator Jesse Helms.
- Worked with U.S. Sen. Sam Nunn on information security policy.
- Worked at the National Security Institute and advised counter-intelligence office of a U.S. President. Serves on Advisory Board.
- Former Director of Global Risk at PricewaterhouseCoopers.
- Interviewed frequently by major national media, including *The New York Times.*
- Advised “DaVinci Code” author Dan Brown on his national security novel, “Digital Fortress.”

It Began in Lowell, Massachusetts

- In 1811 Francis Cabot Lowell traveled to Doncaster, England, to see firsthand the Cartwright Loom.
- The Cartwright Loom was the backbone of the industrial economy in England.
- The factory chiefs gave Lowell a tour of the factory and also showed him the blueprints of the very sophisticated Cartwright Loom.
- For the Brits, arrogance and false sense of security proved fatal.
- Lowell was underestimated: he had a photographic memory and captured the intricacies of the loom design. The colonies a threat?
- By 1813 the first American power loom, based on the British design, was built, led by a group of Boston merchants. The rest is history.

Trade Secrets: What Are They?

- **Trade secrets** are all forms and types of financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically or in writing, which the owner has taken reasonable measures to protect; and has an independent economic value.

Economic Espionage Defined

- Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly:
  - Steals, or without authorization … obtains a trade secret;
  - … copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;
  - Receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization …

Foreign Instrumentality Required

"Foreign instrumentality" means any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government.

A National Security Issue

"The protection of trade secret information, critical technologies, and proprietary information is an integral part of US economic security. Do to the importance of maintaining US economic competition, current policy is to treat foreign threats to the economic well-being of the US as a national security issue. As a result, economic security is directly linked to, and inseparable from, national security."

Protected Secret

- The original 121-year-old formula is locked in a SunTrust bank vault in Atlanta.
- Authorization to access the formula is by a resolution of the Board of Directors.
- Only two Coca-Cola employees at any given time know the formula. Each knows the full formula.
- Their identities are never disclosed.
- They never fly on the same aircraft.
- Strict non-disclosure agreements are enforced.
- July 2006 attempt to sell new Coke product formula for $1.5M: sentenced to 8 years.

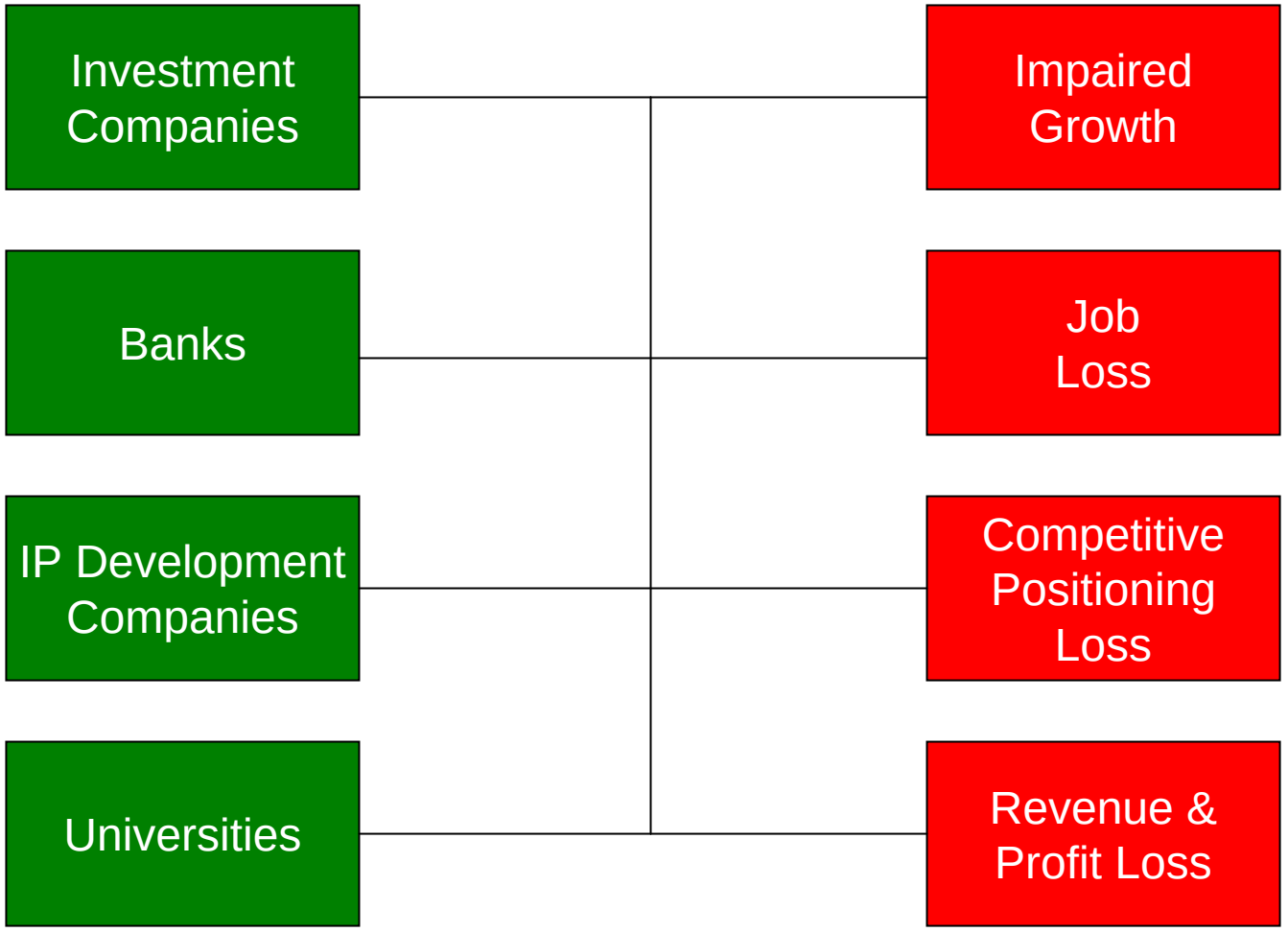
IP Theft is Wide-Ranging

- Increasing investments from venture capital firms, private equity firms, strategic partner investments.
- Post-Soviet global enterprise investment range differentiates from earlier investment cycles:
  - China
  - India
  - Ukraine
  - Russia
  - Bulgaria
  - Estonia
  - Romania
- Strong drivers:
  - Rise of global organized crime
    - US v. Russia comparison
  - Increase in demand for money laundering of drug money
  - Increase in terrorist faction availability
  - Increase in child pornography
    - Drives theft of Internet payment system IP

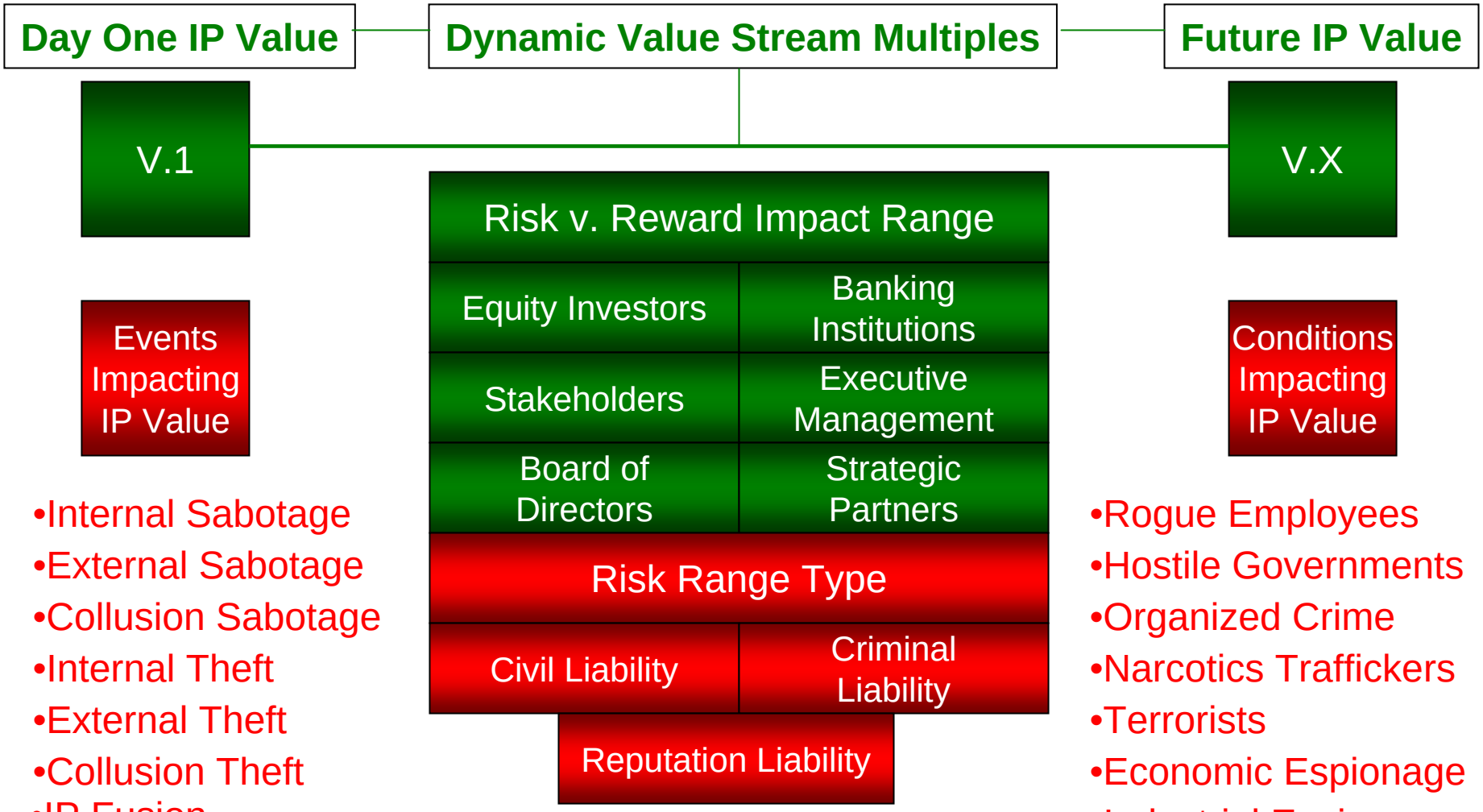
IP Investment Range

- Internet applications
  - Payment systems
  - Mobile
  - Web development
- Transportation
  - Automotive
  - Aeronautical
  - Space
- Pharmaceutical/Medical
  - Diabetes
  - Obesity
  - Diagnostics
  - Non-invasive surgical procedures
- Green Energy Government & Industry Global Warming Initiatives
  - Solar
  - Wind
  - Petroleum
  - Other

IP Espionage Direct Victim Impact



What is the Value of Your IP? And Risk?



Who Steals Trade Secrets?

- Employees.
- Foreign or multinational corporations.
- Foreign government-sponsored educational and scientific institutions.
- Free-lance agents (some of whom are unemployed former intelligence officers).
- Computer hackers.
- Terrorist organizations.
- Revolutionary groups.
- Extremist ethnic or religious organizations.
- Drug syndicates.
- Organized crime.

ORGANIZED CRIME LINK

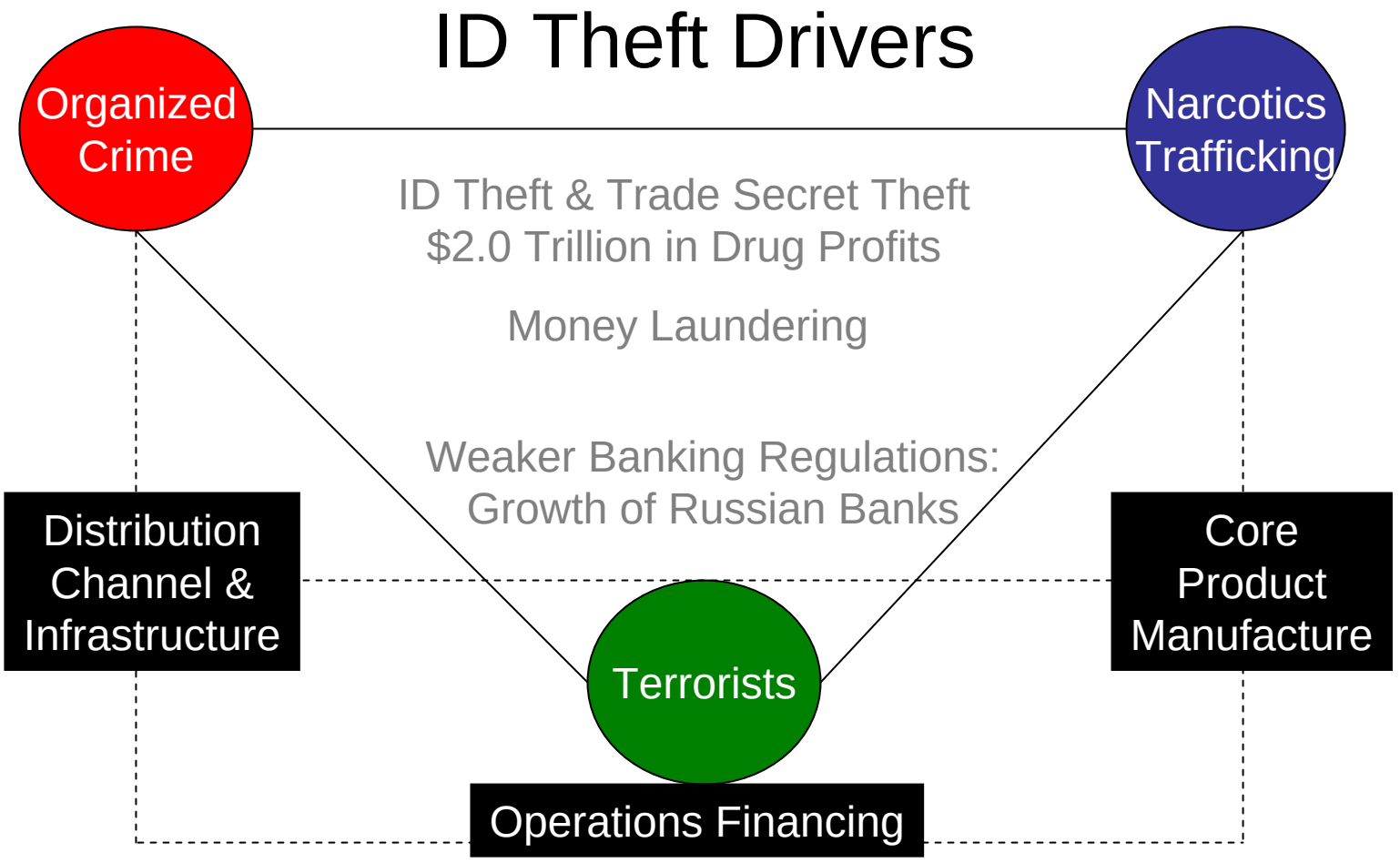
Organized Crime Proliferation

- Organized crime is involved in trade secret theft and economic espionage.
- Russia has emerged as a major international influence in organized crime.
- Compare organized crime in the U.S. and Russia:
  - US:
    - 24 crime families
    - 2,000 active members
  - Russia
    - 5,000 – 8,000 groups
    - 100,000 active members

Russian Organized Crime & IP Theft

- The theft of intellectual property by organized crime is escalating in the following states, in particular:
  - New York
  - California
  - Pennsylvania
  - Massachusetts
- According to a report from Michigan State University School of Criminal Justice:
  - Russian activity is accelerating as a result of the dismantling of the Soviet Union.
  - Federal authorities are currently investigating and infiltrating these criminal enterprises.
  - “The threat from … economic crimes (such as the theft of intellectual property, industrial espionage … and computer-related crime) is increasingly recognized as a matter of national security.”
- Use of IT and communications professions by organized crime is growing.

Behind the Veil of Identity and IP Theft



IP Linkage to Terrorists?

- Terrorist attack on June 30, 2007 Glasgow International Airport.
- Jeep Cherokee loaded with propane as canisters driven into airport pedestrian entrance.
- Attack occurred three days after appointment of Glasgow-born Gordon Brown as Prime Minister.
- Two terrorists in the Jeep:
  - Bilal Abdullah, a medical doctor with ties to the ultra-violent Sunni Wahabists. Iraqi descent.
  - Kafel (or Khalid) Ahmed, en aeronautical engineer working on his doctorate in computational fluid dynamics in Cambridge, England. Born in Bangalore, India.
    - Sympathetic to plight of Muslims in Iraq, Afghanistan, and Chechnya

Linkage to Terrorists, continued

- Worked for an Indian outsourcing company
- The Company was under contract with clients including Boeing and Airbus and worked on highly sensitive aerodynamic projects such as specialty component wing design
  - May have had access to sensitive, proprietary information:
    - » Safety concerns
    - » Sabotage
    - » IP theft

– Both terrorists are believed to have been behind other terrorist attacks in the UK.

Trade Secret Theft Drivers

- After the demise of the Soviet Union, the U.S. became the world's only superpower, powered significantly by the investment and development of sophisticated technology. The illicit acquisition of technology by other governments and commercial entities is orders of magnitude less expensive, and it reduces the time to market.

Trade Secret Theft Drivers, continued

- The principal drivers of economic espionage and trade secret theft are:
  - Military force modernization by other nations, many of them hostile to US interests.
  - Economic competition.
  - Commercial modernization.
  - Money laundering.

A Matter of Coincidence?

<u>Question:</u> Did each government arrive independently at each design at the same time?

United States

Russian

Linkage to Child Pornography

- The majority of child pornographic images and videos seized are produced primarily in:
  - The former Soviet states.
  - Southeast Asia (including Japan).
  - South America (increasingly).
- The proliferation of commercial pay-per-view technology and Internet payment systems technology that provide anonymity are in demand.

China: Pursing Global IP

- The People's Republic of China developed the 863 program to acquire dual use technology—commercial and military application.
- 863 program targets six key areas:
  - Information Technology
  - Advanced Materials
  - Biotechnology & Advanced Agricultural Technology
  - Advanced Manufacturing and Automation Technology
  - Energy Technology
  - Resource & Environment Technology

863 Program Targets, continued

- Information Technology:
  - Computer Software & Hardware Technology
  - Communication Technology
  - Information Acquisition & Processing Technology
  - Information Security Technology
- Advanced Materials:
  - Photo-Electronic Materials & Devices Technology
  - Special Functional Materials Technology
  - High-Performance Structural Materials Technology

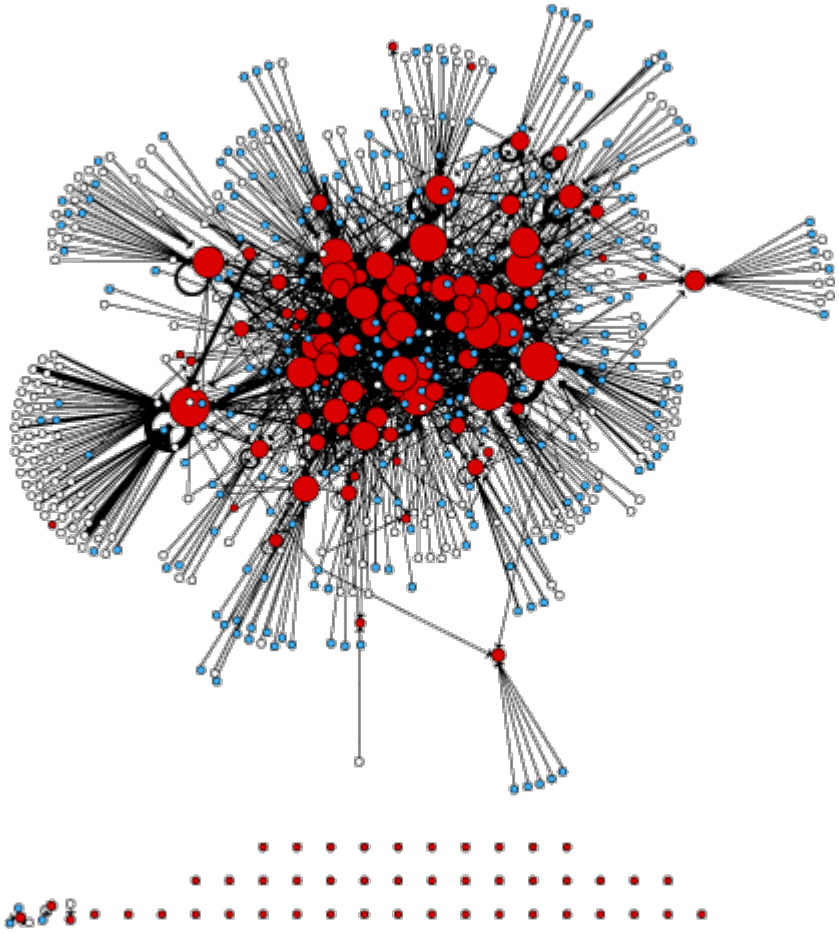
863 Program, continued

- Biotechnology & Advanced Agricultural Technology:
  - Bioengineering Technology
  - Gene Manipulation Technology
  - Bio-information Technology
  - Advanced Agriculture Technology
- Advanced Manufacturing & Automation Technology:
  - Contemporary Integrated Manufacturing Systems (CIMS)
  - Robotics Technologies

863 Program, continued

- Energy Technology:
  - Sustainable Energy Technology
  - Clean Coal Technology
- Resource & Environment Technology:
  - Marine Resources Exploitation Technology
  - Marine Biotechnology
  - Ocean Monitoring Technology
  - Technologies for the Prevention of Environmental Pollution

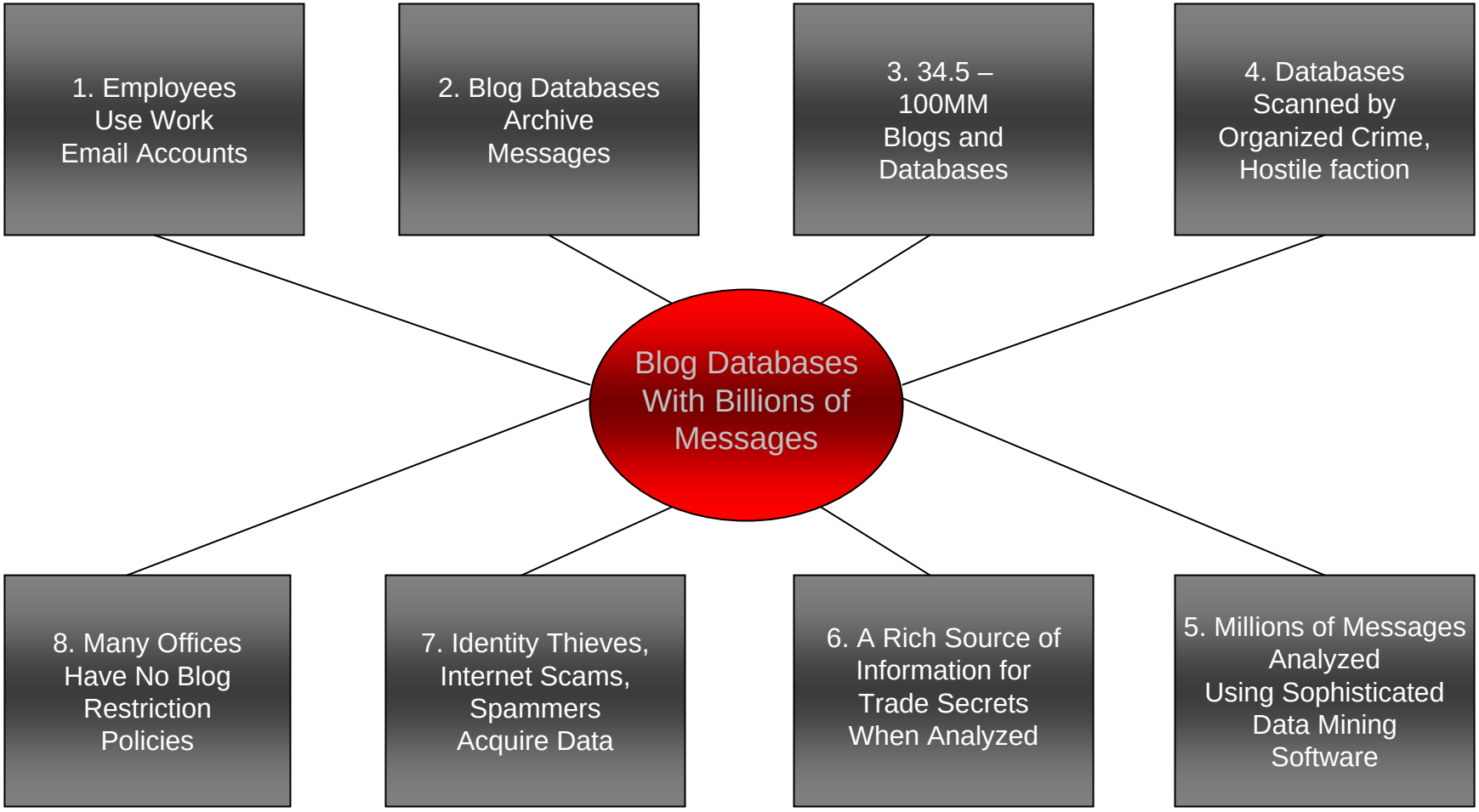
TECHNOLOGY FUELS RISK



Blogging: A Growing Example

- Rapid growth: 34.5MM to over 100MM blogs worldwide.
- Rapid growth: blog audience: 20 percent the size of total newspaper reading audience.
- 9 percent of computer users have created blogs.
- Blogging from laptops and Internet-enabled PDAs.
- In an organization of 100,000 employees:
  - 25 percent blog or 25,000.
  - Blogging an average of twice per week is 50,000 messages a week or 2.4MM annually.
  - Many blog from work.
  - Others blog from mobile platforms.
- Organized crime is believed to be behind or influence a number of gambling and pornography blogs.

Here's the Problem With Blogs



A Mobile Society

- Mobile workforce
  - Work from home
  - Work from remote office locations
  - Work from hotels
- Mobile enablers
  - Cell phones (Internet enabled)
  - Personal Digital Assistants
  - Flash drives
  - Removable media
  - Laptops

Mobile Device Theft

- More than two million a year reported stolen worldwide.
- 1,600 a day reported stolen in the U.S.
- A laptop is stolen every 53 seconds.
- Chances of a laptop being stolen are one in ten.
- 97% are never recovered.
- Most common crime after identity theft.
- Contains the most sensitive data, including social security numbers, as well as intellectual property, and trade secrets.
- Six of one hundred government and defense workers in the United Kingdom are said to have lost or had stolen a laptop computer.
- Many stolen laptops have passwords written on paper and taped to the underside of the laptop.

Are trade secrets on your laptops?

What policies do you have in place to prevent mobile device theft?

Mobility: A Risk Force Multiplier

- Mobile technology contributes to the dimension of risk:
  - Greater distribution of target information.
  - Less institutional monitoring.
  - Fewer employee observations about risky behavior.
  - Less attention to security policies and procedures.
  - Greater likelihood of losing a mobile device.
  - Greater likelihood of mobile device theft.
  - Greater likelihood of a breach.

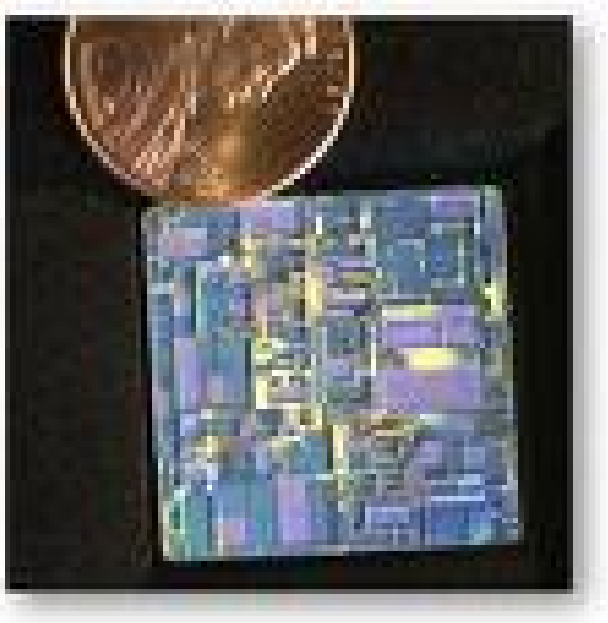
Where Is Your IP?

- Electronic information seldom resides in one place.
- Information structures are designed for redundancy.
- Then behavior reinforces the principle of redundancy.
- Where does data exist and where is it at risk:
  - Desktop computer
  - Laptops
  - Handhelds
  - Cell phones
  - Flash drives
  - Portable backup drives
  - Data centers: domestic and foreign
  - Home computers
  - Data management third-parties
  - Internet Service Providers
  - Spouse's and children's computers
  - Hotels & resorts & conferences
  - Neighbors homes
  - Restaurants
  - Taxis
  - Office
  - Subway
  - Rental & personal cars
  - Email servers
  - In escrow

So, IP is Mobile

- IP may transported by or to:
  - PDAs
  - Internet-enabled cell phones
  - Laptops
  - Home computers
    - Spouse
    - Children
  - Workplace computers
  - Hard copy files
  - Spiral notebooks
  - Waste bins
  - Discarded or recycled computers
  - Flash drives
  - Portable drives
  - CDs

STEALING TRADE SECRETS



Find the Trade Secret

"Just a quick note to say hi. Thought this was a cool picture. Call me when you can: I've got a business question for you."

Laptops

Blogs

Internet-Enabled Cell Phones

CDs

Portable Drives

Flash Drives

PDAs

Case History I

DuPont and Chemist Gary Min

- Former Chinese national.
- Former DuPont chemist stole secrets worth $400MM.
- Recently pleaded guilty to corporate espionage.
- In the crosshairs: KEVLAR, TEFLON, NOMEX, LUCITE and other products protected under trade secret.
- May have intended to sell secrets to government of China or to Chinese companies.
- An employee for 10 years.
- Had developed significant products. He had access to a high-security electronic database at DuPont.
- This enabled him, but it was also his downfall.

Tripping the Wire

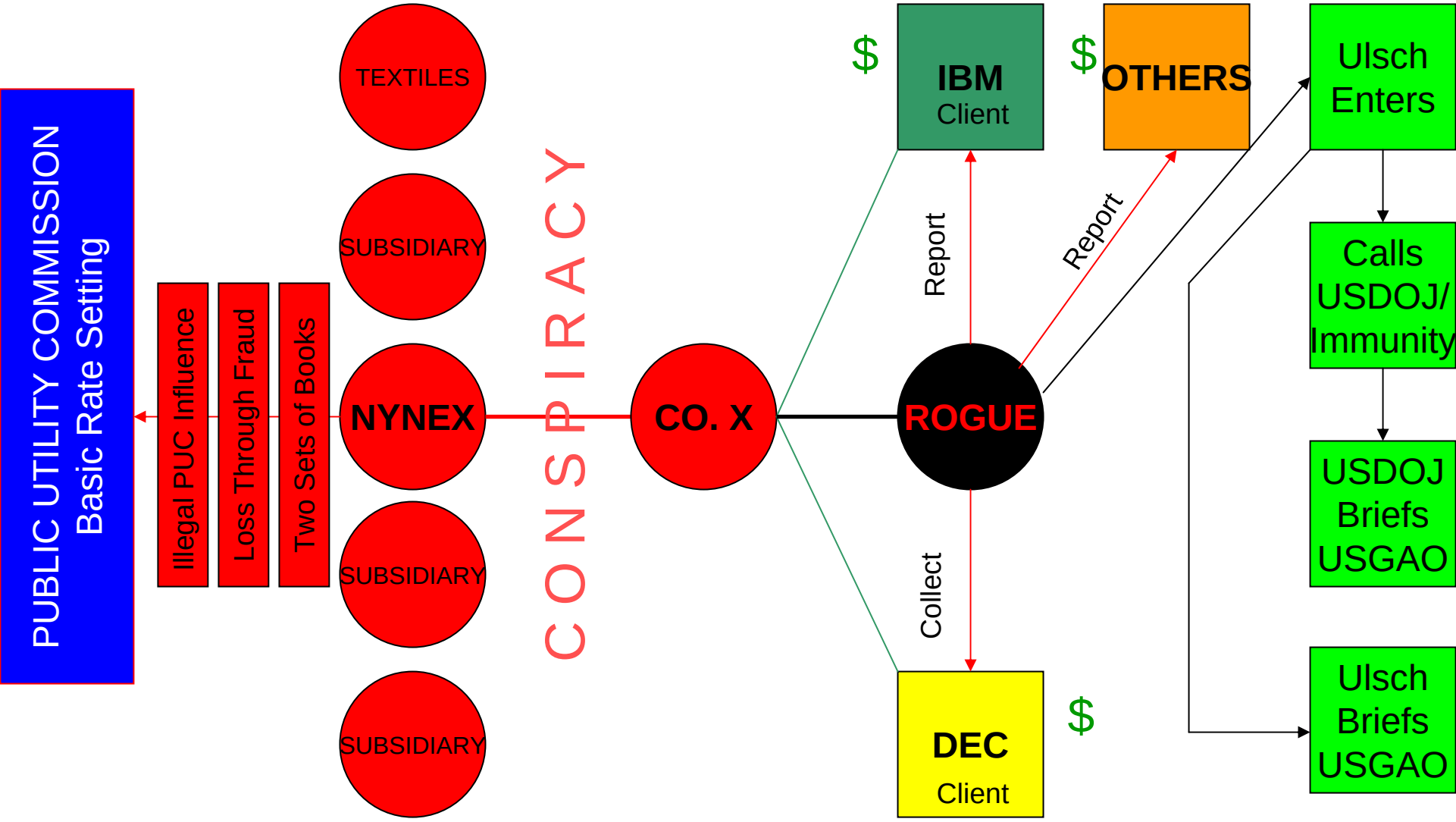
- His biggest mistake was elevating his profile to security:
  - Over a short period of time he downloaded 22,000 abstracts and documents from the secure DuPont database.
  - 15-20 hours at a time.
  - This level of activity represented 15 times more use than the next highest user at DuPont.
  - Federal authorities were contacted at this time.
- Min leaves DuPont and goes to work for Victrex PLC. He transferred 180 documents to his Victrex computer.
- Min was in China when a DuPont investigator found documents at Min's home and in an apartment he had rented. Other documents were found on his home PC.

Case History II

The NYNEX Case

- Certain elements of this case were tried in federal court and were reported in the *Wall Street Journal*.
- Other aspects of this case have never been made public.
- I am making certain elements of the case public today.
- No individuals will be mentioned by name.
- Principal companies will be named.
- Several companies will not be named. Such disclosure would enable the identification of the individuals involved.

Industrial Espionage Case History II



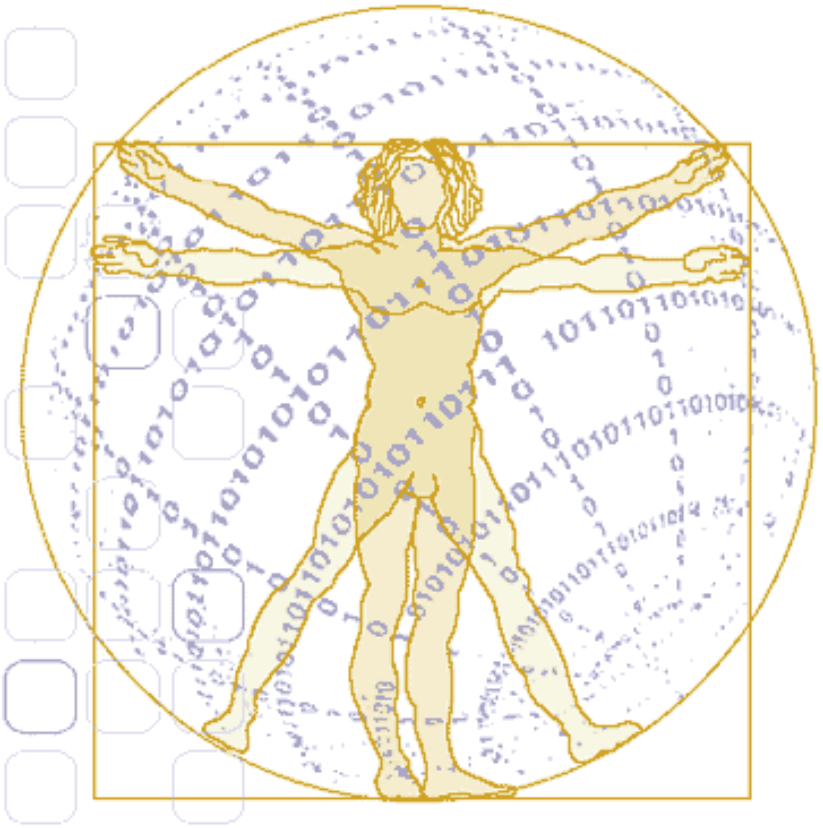
Aftermath

- NYNEX exited the information products and services business at a loss estimated to be in the hundreds of millions of dollars.
- NYNEX discharged senior executives over the incidents.
- A number of Co. X executives were terminated.
  - A senior executive was restricted from serving on any public board for several years.
  - His employment was terminated.
  - He was fined but avoided imprisonment.
  - He was recently honored for his industry contributions.
  - He is currently the CEO of a privately held, successful company.

Aftermath, continued

- The rogue consultant was granted full federal and state immunity from prosecution:
  - He was not fined and faced no prison term.
  - He runs a very successful research and consulting firm.
  - He is financially secure.
- Another senior executive formed a company afterwards and then sold it, making about $100MM.
  - He was never charged in the case.

Defending Against Espionage & Theft

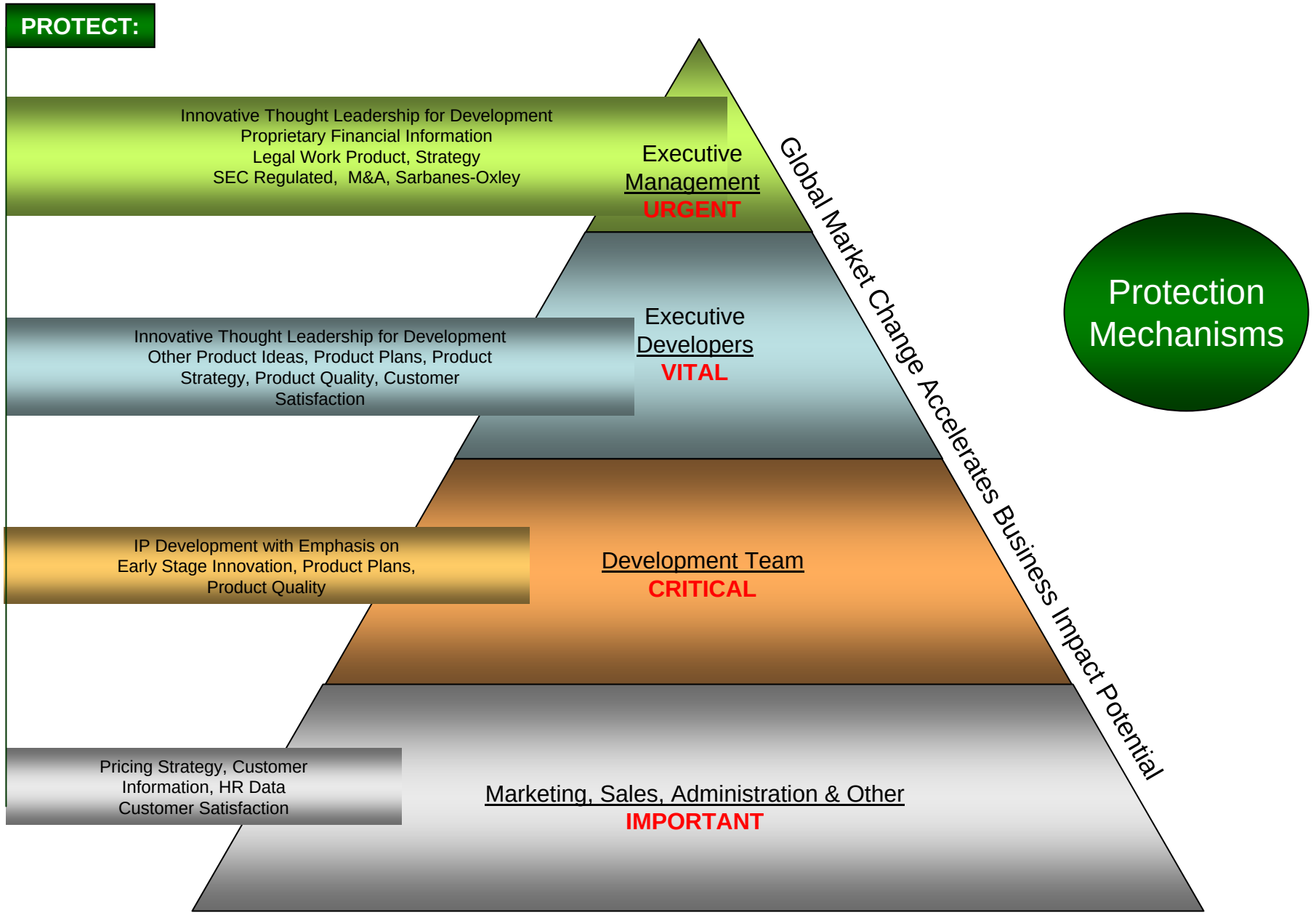


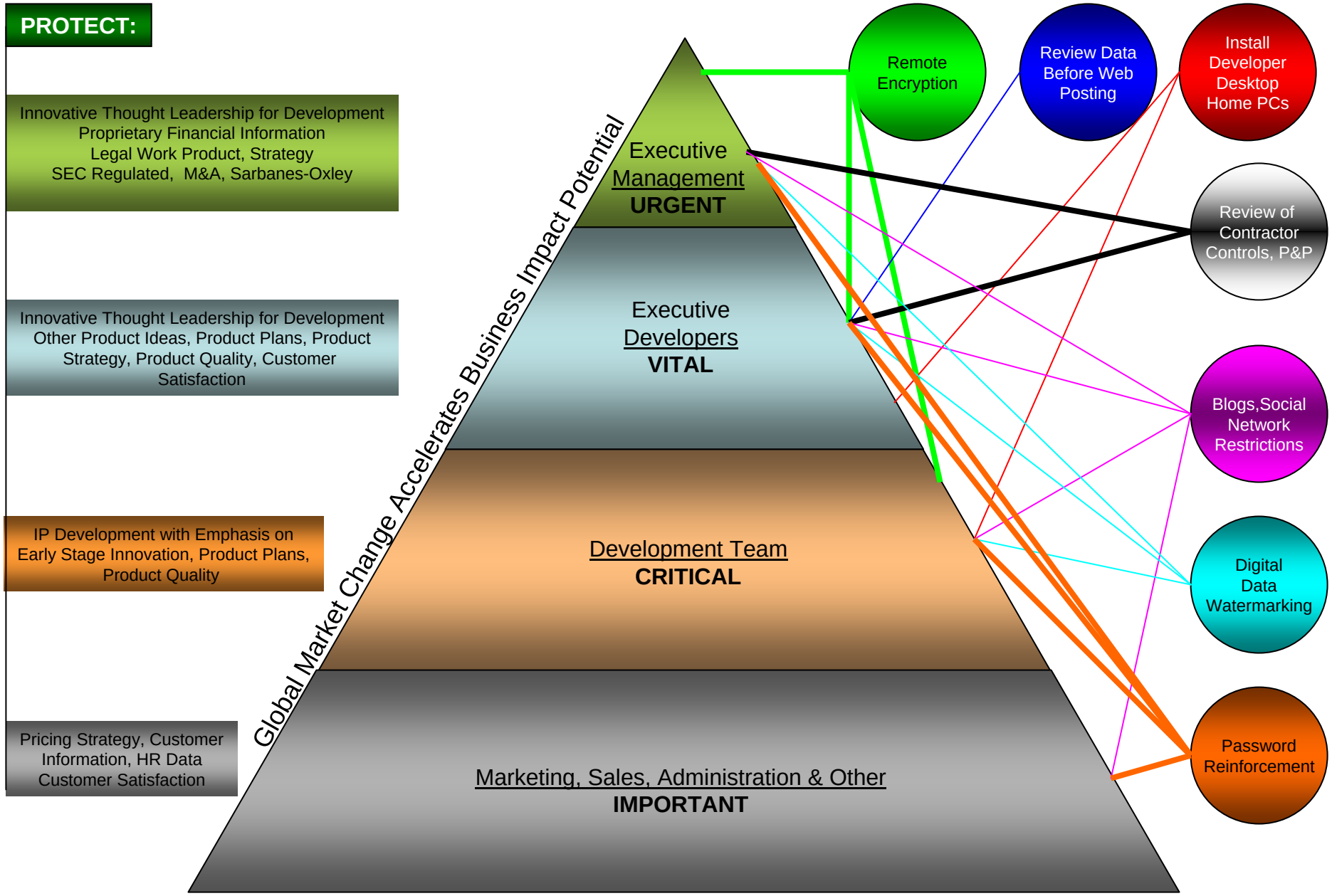
Securing Against the Threat

- Recognize that the threat is real (FBI).
  - *Many remain in denial. "It won't happen to me."*
- Identify and valuate trade secrets (FBI).
  - *This can be a major undertaking for many organizations. In today's complex data structures (including offshore information management), information assets seldom reside in one physical or logical location. Where is your information?*
  - *Comply with Electronic Discovery requirements.*
- Implement a definable program for safeguarding trade secrets (FBI).
  - *Many companies have not even defined a security program targeting trade secret espionage.*
  - *Be sure to include technology socialization initiatives.*

Securing Against the Threat …

- Secure physical trade secrets and limit access to trade secrets (FBI).
  - *Easier in the physical world than in the logical world. Mobile technology makes this increasingly difficult.*
  - Do your policies include clean desk policies and locking file cabinets?
- Confine intellectual knowledge (FBI).
  - *Mobile technology makes this increasingly difficult.*
  - *Define who needs access, when access is needed, and for how long access is needed.*
  - *Restrict the movement of data.*
- Provide ongoing security training to employees (FBI).
  - *Mobile technology proliferation exceeds the ability to defend against its applications and awareness of its risks.*
  - *Lack of awareness remains the greatest deficiency.*


PROTECT:
Innovative Thought Leadership for Development
Proprietary Financial Information
Legal Work Product, Strategy
SEC Regulated, M&A, Sarbanes-Oxley
Executive
Management
URGENT
Innovative Thought Leadership for Development
Other Product Ideas, Product Plans, Product
Strategy, Product Quality, Customer
Satisfaction
Executive
Developers
VITAL
IP Development with Emphasis on
Early Stage Innovation, Product Plans,
Product Quality
Development Team
CRITICAL
Pricing Strategy, Customer
Information, HR Data
Customer Satisfaction
Marketing, Sales, Administration & Other
IMPORTANT
Global Market Change Accelerates Business Impact Potential
Protection
Mechanisms


PROTECT:
Innovative Thought Leadership for Development
Proprietary Financial Information
Legal Work Product, Strategy
SEC Regulated, M&A, Sarbanes-Oxley
Innovative Thought Leadership for Development
Other Product Ideas, Product Plans, Product Strategy, Product Quality, Customer Satisfaction
IP Development with Emphasis on Early Stage Innovation, Product Plans, Product Quality
Pricing Strategy, Customer Information, HR Data
Customer Satisfaction
Global Market Change Accelerates Business Impact Potential
Executive
Management
URGENT
Executive
Developers
VITAL
Development Team
CRITICAL
Marketing, Sales, Administration & Other
IMPORTANT
Remote Encryption
Review Data Before Web Posting
Install Developer Desktop Home PCs
Review of Contractor Controls, P&P
Blogs,Social Network Restrictions
Digital Data Watermarking
Password Reinforcement

12 C.F.R. 30: Safety and Soundness Standards

Interagency Guidelines Establishing Standards for Safeguarding Customer Information

Set forth standards pursuant to section 39 of the Federal Deposit Insurance Act (section 39, codified at 12 U.S.C. 1831p-1), and sections 501 and 505(b), codified at 15 U.S.C. 6801 and 6805(b), of the
Gramm-Leach-Bliley Act. These Guidelines address standards for developing and implementing administrative, technical, and physical
safeguards to protect the security, confidentiality, and integrity of customer information.

TREND: Security Convergence!

Reducing Trade Secret Theft

- Information classification
  - Do you know where data is?
  - Is all data treated the same?
  - Is trade secret data managed differently.
- Mark data
  - Paper
  - Electronic
- Monitor restricted access
  - Create strong awareness
  - Establish access violation response
- Manage access to trade secrets
  - Does everyone with access really need access.
  - What are the backgrounds of those with access—who can be trusted?
  - Local court of jurisdiction v. federal checks
  - Major life event reinvestigation

Reducing Trade Secret Theft, continued

  - Periodic reinvestigation
- Non-Disclosure Agreements:
  - Keep current
  - Update as conditions change
- Have a crisis management plan:
  - What is said to the press will influence:
    - Customers
    - Partners
    - Employees
    - Stock value and volatility
- Team approach to protecting restricted information:
  - Physical security/Technical security/Administrative security
  - CISO/CSO
  - Chief Risk Officer
  - Legal
  - Human Resources
  - Executive Management

Tightening Controls Over IP

- Master Services Agreement: Domestic and Foreign, including Third-Party Data Management
  - Require the right to audit on demand
  - Define the depth and scope of the audit or define as an unlimited audit
  - Set vendor expectation regarding audit:
    - Tone at the top
    - Security officer training and certifications
    - Staff awareness and training
    - Security reporting structure requirements
    - Best practice expectations
    - Policies and procedures disclosure
    - Turnover rate
    - Employee incentives to remain with company

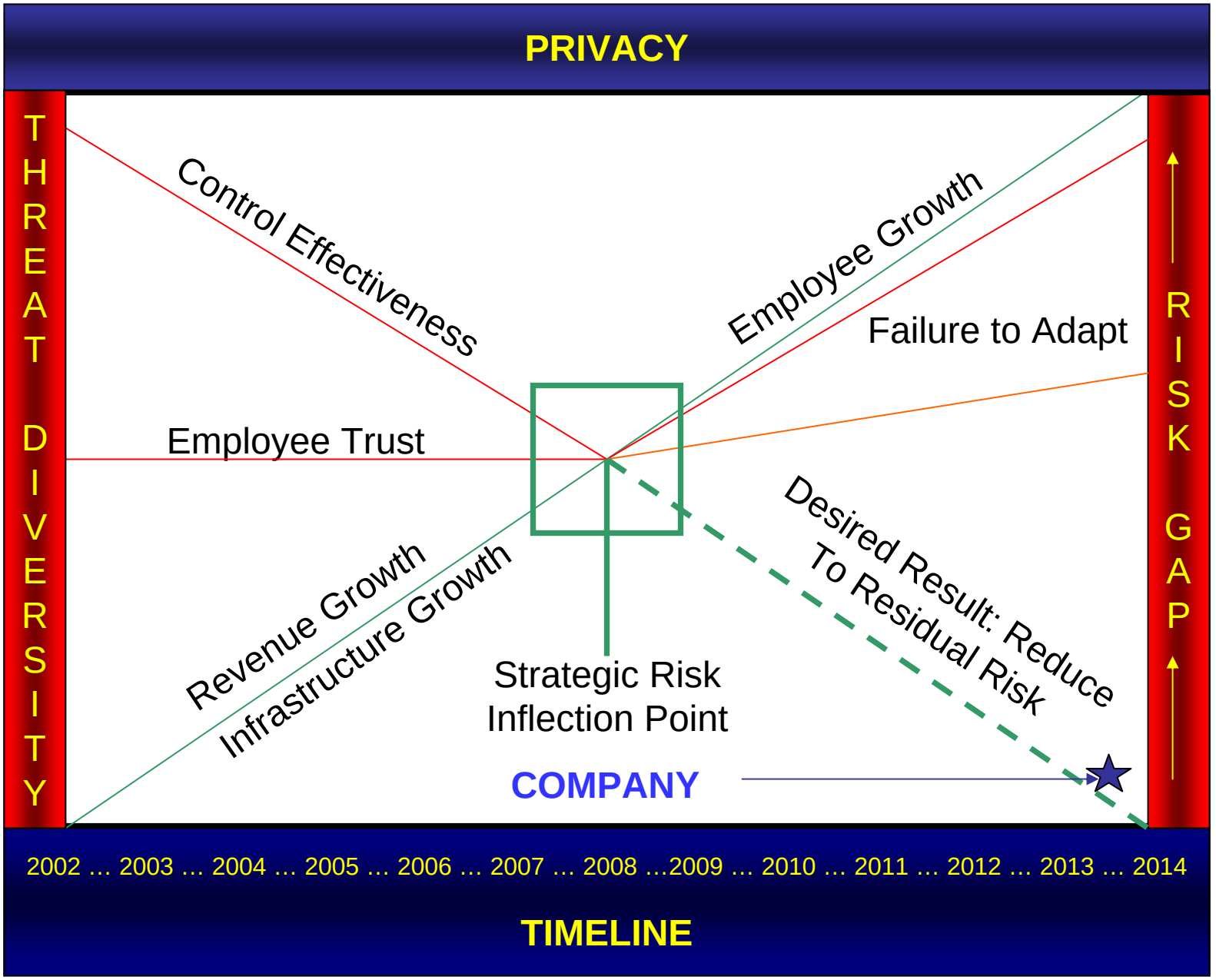
Tightening Controls, continued

- Compliance with all regulatory and specialized requirements such as PCI
- Disclosure of critical and material events
- Hiring practices:
  - Recruitment
  - Background investigations
- Facility site selection criteria:
  - Weather resistance and resiliency
  - Traffic: transient, static
  - Single company site
- 79 key security concerns

Trade Secret Thefts and Banks

- Historically, Russian agents have used financial institutions as sources of recruitment.
- Banks in high technology and defense markets targeted.
- Look for vulnerable employees:
  - Romantic involvements
  - Financial difficulties
  - In recent Boston case, Police recruited a bank employee to participate in identity theft.
- Bank employees can identify technology and defense company employees that may be experiencing financial difficulty due to major life event changes such divorce, illness, excessive spending, educational expense burdens, etc.
  - Once identified by the bank employee, the technology or defense employee can be targeted for bribery.

Strategic Risk Inflection Point



Jefferson Wells

Don Ulsch
Director, Technology Risk Management
Global SME IT Governance
Don.Ulsch@JeffersonWells.com
Telephone (212) 823-8600
Mobile (978) 808-6526