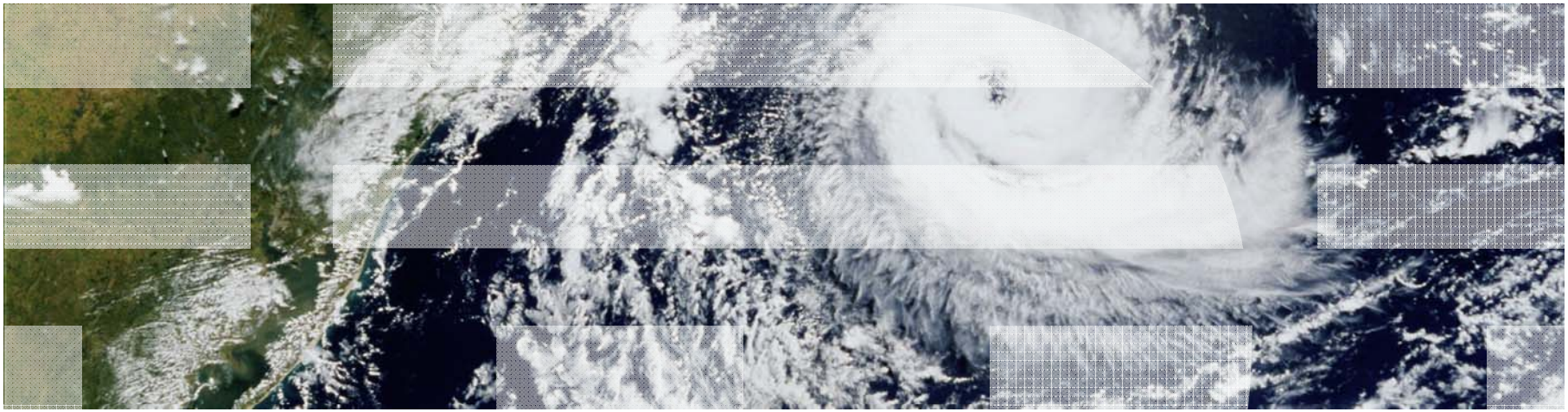
Dr. Tilak Agerwala, VP, Systems
Dr. Chung-Sheng Li, Director, Commercial Systems
Dr. J.R. Rao, Senior Manager, Security Department
IBM Research Division

Fine-Grained Cybersecurity for Continuous Assurance of Intellectual Property Integrity



Cybersecurity in the Headlines

TECHNOLOGY | APRIL 8, 2009

Electricity Grid in U.S. Penetrated By Spies

Article | Video | Comments (140)

Email | Print | Save This | Like 1K | + More | Text

WSJ.com Expand your access to WSJ.com - FOR FREE CLICK HERE

By SIOBHAN GORMAN

Vast Spy System Loots Computers in 103 Countries

By JOHN MARKOFF
Published: March 28, 2009

TORONTO — A vast electronic spying operation has infiltrated computers and has stolen documents from hundreds of government and private offices around the world, including those of the Dalai Lama, Canadian researchers have concluded.

TWITTER | COMMENTS (76) | E-MAIL | PRINT | SINGLE PAGE | REPRINTS | SHARE

Enlarge This Image

Tim Leyes for The New York Times

The Toronto academic researchers who are reporting on the spying operation dubbed GhostNet include, from left, Ronald J. Deibert, Greg Walton, Nart Villeneuve and Rafal A. Rohozinski.

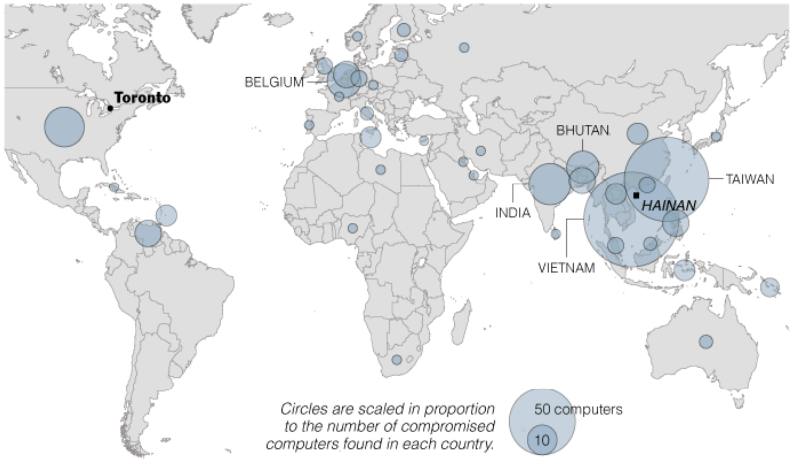
Multimedia

In a report to be issued this weekend, the researchers said that the system was being controlled from computers based almost exclusively in China, but that they could not say conclusively that the Chinese government was involved.

The researchers, who are based at the Munk Center for International Studies at the University of Toronto, had been asked by the office of the Dalai Lama, the exiled Tibetan leader whom China regularly denounces, to examine its computers for signs of malicious software, or malware.

The Vast Reach of 'GhostNet'

Researchers have detected an intelligence gathering operation involving at least 1,295 compromised computers. Below, the locations of 347 of the compromised machines, many of which were tracked to diplomatic and economic government offices of South and Southeast Asian countries.



Source: Information Warfare Monitor

THE NEW YORK TIMES

TECHNOLOGY | FEBRUARY 4, 2010, 11:32 P.M. ET

Google Working With NSA to Investigate Cyber Attack

Article | Stock Quotes | Comments (17)

Email | Print | Save This | Like | + More | Text

By SIOBHAN GORMAN and JESSICA E. VASCELLARO

Officials at the National Security Agency have been working with Google Inc. to investigate the cyber attacks that Google announced publicly last month, according to people familiar with the investigation.

We've fou
a way to h
reach for
new heigh

TECHNOLOGY | FEBRUARY 18, 2010

Broad New Hacking Attack Detected

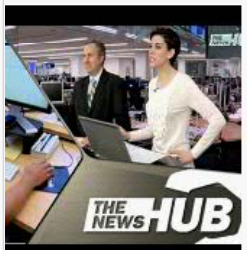
Global Offensive Snagged Corporate, Personal Data at nearly 2,500 Companies; Is Still Running

Article | Video | Stock Quotes | Comments (51)

Save This | Like 121 | + More | Text

MAN

and China successfully broke into computers at nearly 2,500 companies and
es over the last 18 months in a coordinated global attack that exposed vast
al and corporate secrets to theft, according to a computer-security company
breach.



The damage from the latest cyberattack is still being assessed, and affected companies are still being notified. But data compiled by NetWitness, the closely held firm that discovered the breaches, showed that hackers gained access to a wide array of data at 2,411 companies, from credit-card transactions to intellectual property.

TECHNOLOGY | FEBRUARY 5, 2011

Hackers Penetrate Nasdaq Computers

Article | Stock Quotes | Comments (69)

Email | Print | Save This | Like 1K | + More | Text

WSJ.com Expand your access to WSJ.com - FOR FREE CLICK HERE

By DEVLIN BARRETT

Hackers have repeatedly penetrated the computer network of the company that runs the Nasdaq Stock Market during the past year, and federal investigators are trying to identify the perpetrators and their purpose, according to people familiar with the matter.

The exchange's trading platform—the part of the system that executes trades—wasn't compromised, these people said. However, it couldn't be determined which other parts of Nasdaq's computer network were accessed.

Investigators are considering a range of possible motives, including unlawful financial gain, theft of trade secrets and a national-security threat designed to damage the exchange.

The Nasdaq situation has set off alarms within the government because of the exchange's critical role, which officials put right up with power companies and air-traffic-control operations, all part of the nation's basic infrastructure. Other infrastructure components have been compromised in the past, including a case in which hackers planted potentially disruptive software programs in the U.S. electrical grid, according to current and former national-security officials.

How the Stuxnet Digital Warheads Attacked Iran's Nuclear Installations

By Alex Williams / November 20, 2010 6:22 PM / 17 Comments

Tweet 286 | Like 49 | Hacker News | submit | Share 11

ReadWriteEnterprise channel is a resource and guide for IT managers and technologists in the Enterprise. The channel is sponsored by Qwest Business.

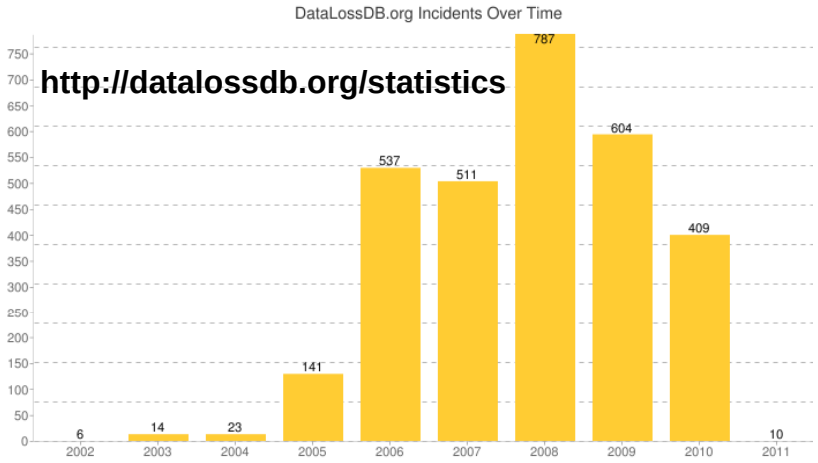
Stuxnet is a computer worm that can do as much damage as a bomb could in destroying an industrial plant or military installation. The Wikipedia entry about Stuxnet says it is the first discovered worm that spies on and reprograms industrial systems.

Stuxnet's capabilities are clear following its use to attack Iran's nuclear installations. The implications are considerable. Any enterprise that uses industrial control systems could be attacked by the worm, potentially causing as much damage as any sort of explosion.

Iran states the attack did not affect its nuclear program. But experts say it's possible that the worm is the reason why Iran delayed the start of its uranium enrichment program.

Malicious cybersecurity incidents resulting from both insider and external vulnerabilities are on the rise

- Traditional **perimeter defense** has become less effective due to the rapid growth of information volume, fast adoption of new technologies and the need to flexibly collaborate across enterprise boundaries.
- Security policies and technologies will become more **fine-grained**. They will be complemented by a **multi-tier containment** security solution that spans across platform, cloud computing/data center, middleware and service oriented architecture, collaboration & community to protect individual business objects
- **Security breaches & fraud are a *continuum*. Far field fraud detection** technologies which provide early warnings about major security breaches and fraudulent transactions before such incidents will emerge to complement existing near field techniques.



- Malicious attacks have surpassed human error for the first time in 2009 (ITRC)
- 48 percent of data breaches across all industries were caused by insiders. (Verizon 2010 Data Breach Investigations Report)
- Cybersecurity incidents in industrial control systems on the rise (HSNW 04/16/10)

Economic Impacts Landscape due to Cybersecurity vulnerabilities

Source: Robert Gibran

Different Types of Loss:
- Cash
- Data
- Intellectual Property
- Trust

Actual Loss:

- **$105 billion** a year (McAfee, 2007)
- **$67 billion** a year (FBI, 2006)
  - **$50** billion a year in identity fraud
- **$202** per compromised record, with an average **$6.6 million** per attack (Ponemon, 2009)
- **$559 million** in Intellectual Property loss, **$4.6 million** per firm (McAfee, 2008)

Potential Loss:

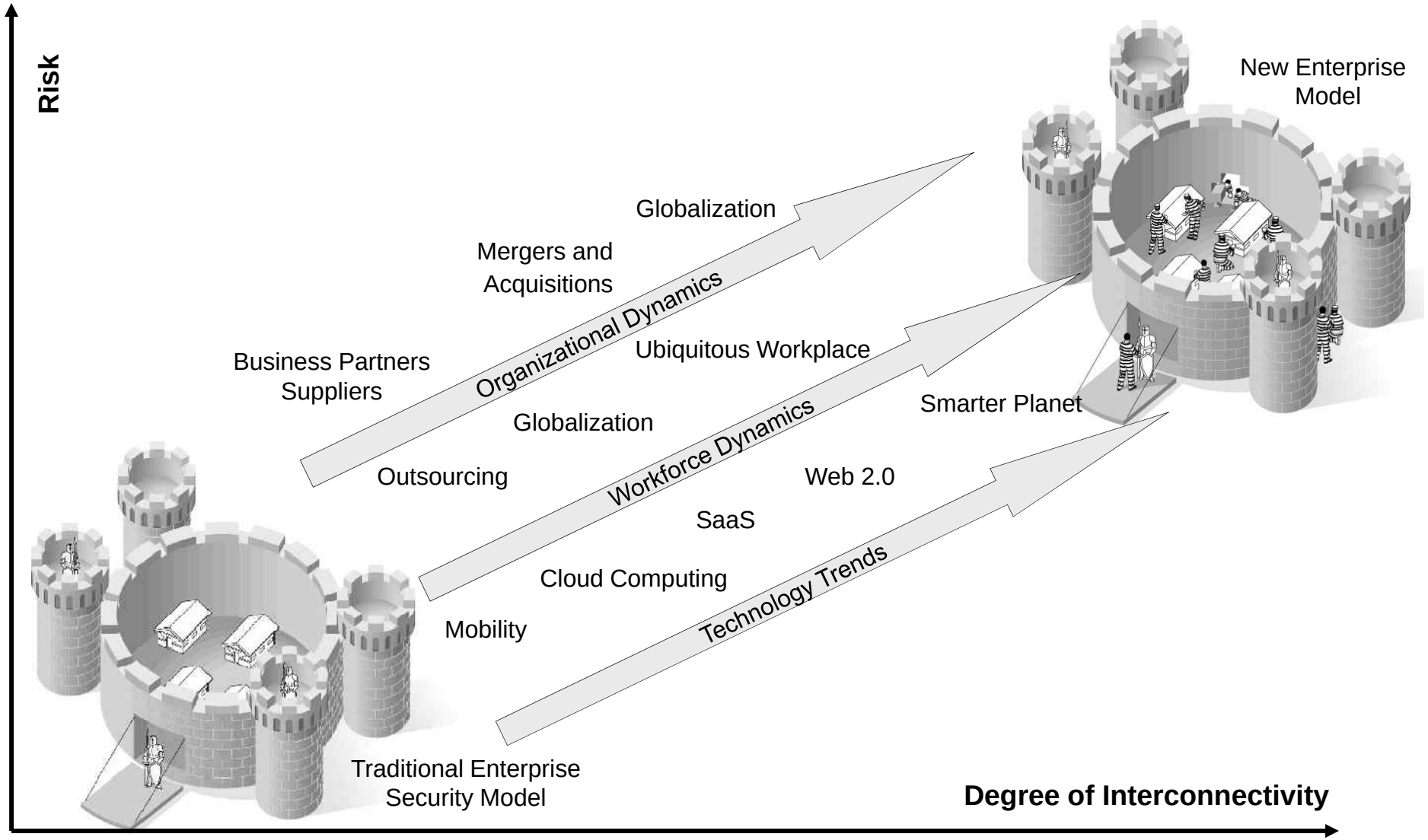
- Estimated at **$700 billion** for a major attack on critical infrastructures (U.S. Cyber Consequences Unit)

Multiple Sources of Profit from the loss:
- Cash
- Data
- Intellectual Property
- Bot Armies

On May 29, 2009, the Federal government issued a report that stated that, between 2008 and 2009 American business losses due to cyber attacks had grown to more than **$1 trillion** worth of intellectual property

Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure, May 2009.

Changing Assumptions of Enterprise Security



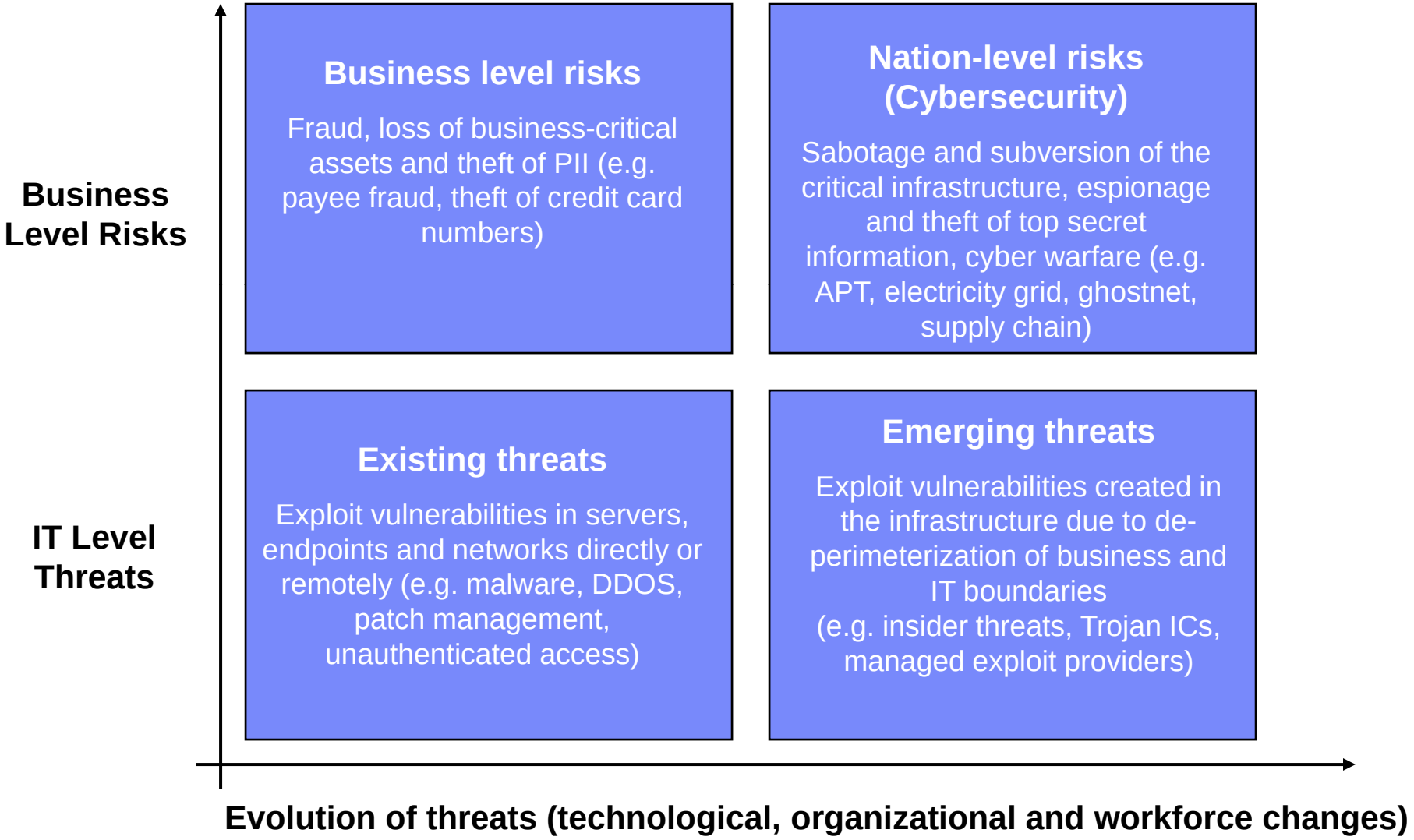
* Gifs from https://www.opengroup.org/jericho/Respondingtodp_implementation_080929.pdf

Traditional Security Controls are ineffective against advanced persistence threat

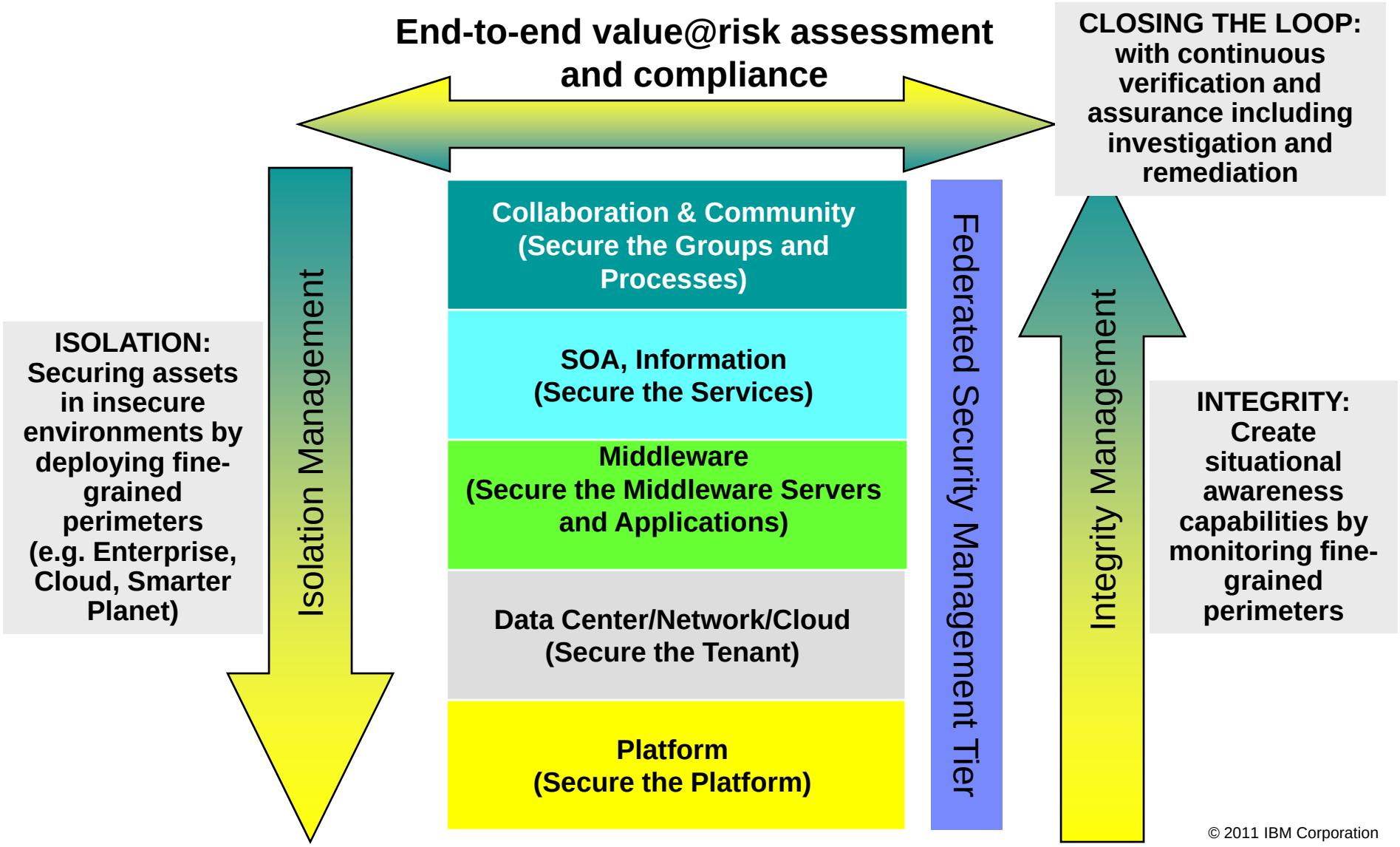
Traditional Malware	Advanced Persistent Threat
▪ **Opportunistic infection (non specific target), uncontrolled distribution**	▪ **Targeted at specific individuals and organizations, controlled distribution**
▪ **Motives: theft of personal info, disruption (DoS)**	▪ **Motives: theft of sensitive, high value information**
▪ **Static code, broadly deployed & once deployed, does not change**	▪ **Dynamic code, customized for each target & altered after infection**
▪ **One shot attack; once detected & remediated, attack essentially over**	▪ **Persistent attack. If detected or defeated, alternate methods employed**
▪ **Operational objective: broad distribution scope**	▪ **Operational objective: remaining undetected**

***From Eric J. Meyers, Du Pont**

Evolution of Threats, Escalation of Risks

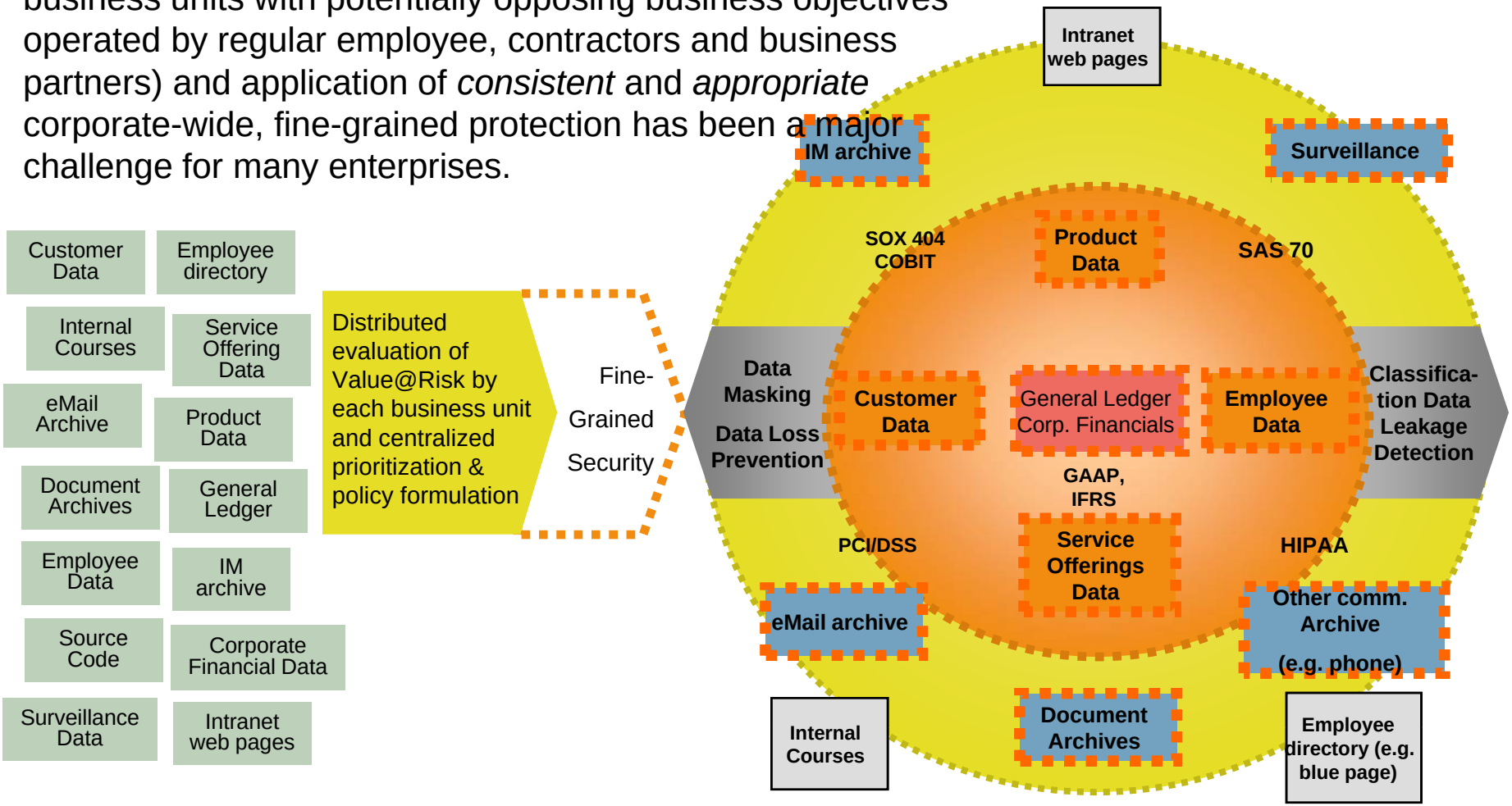


Our Proposition: Fine-grained, multi-tier containment approach to secure the critical infrastructure, IP resources and sensitive information



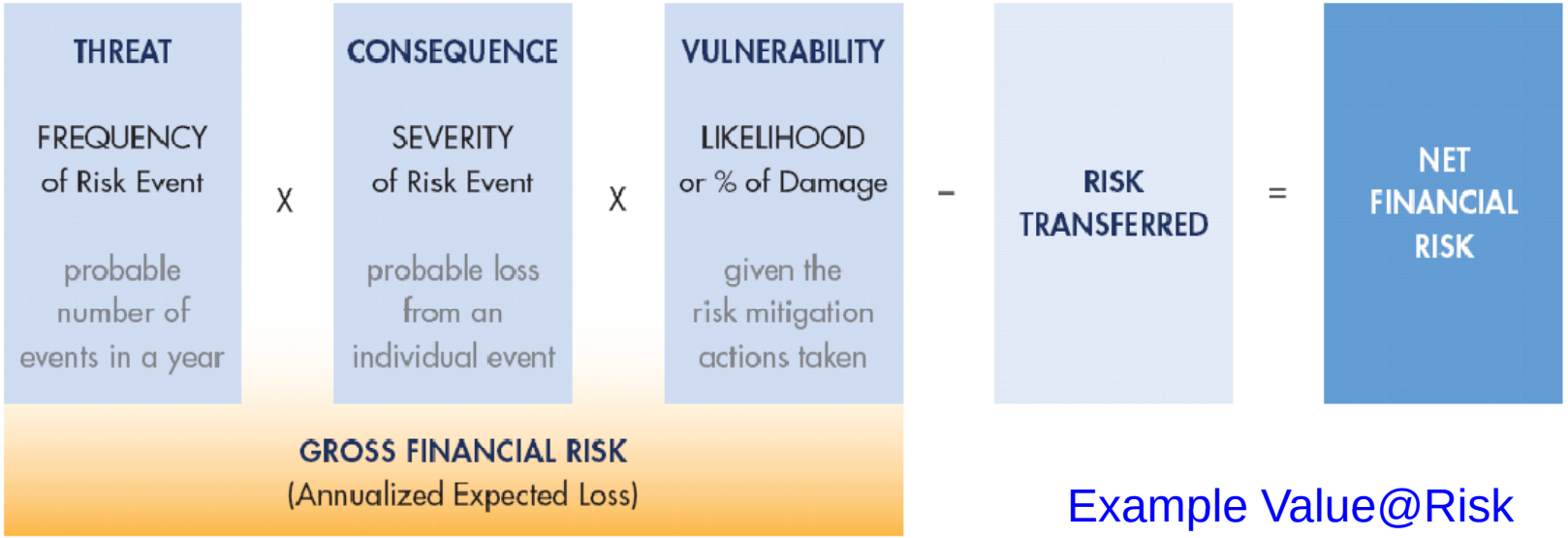
1. Fine-grained security can complement perimeter-based protection in enterprises today

Systematic identification of IP assets (from loosely-coupled business units with potentially opposing business objectives operated by regular employee, contractors and business partners) and application of *consistent* and *appropriate* corporate-wide, fine-grained protection has been a major challenge for many enterprises.

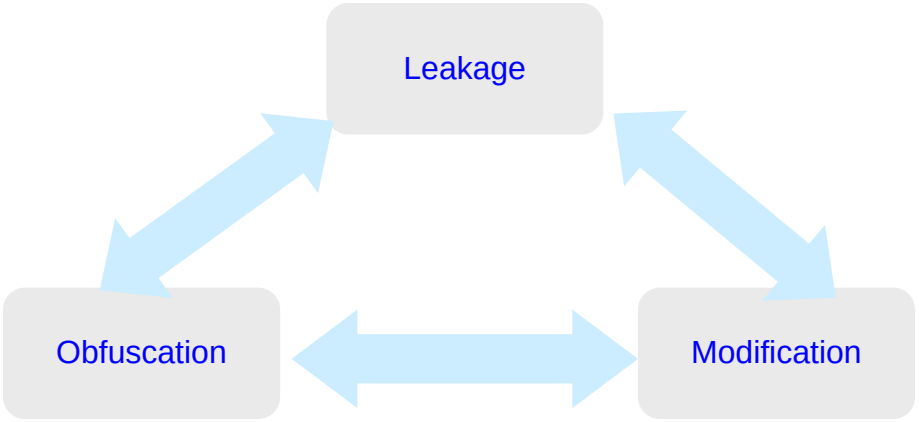


1. Value@Risk Model: often required to rationalize the required investment in cybersecurity for protecting enterprise intellectual properties

source: the financial management of cyber risk, internet security alliance



Insider & external Threats

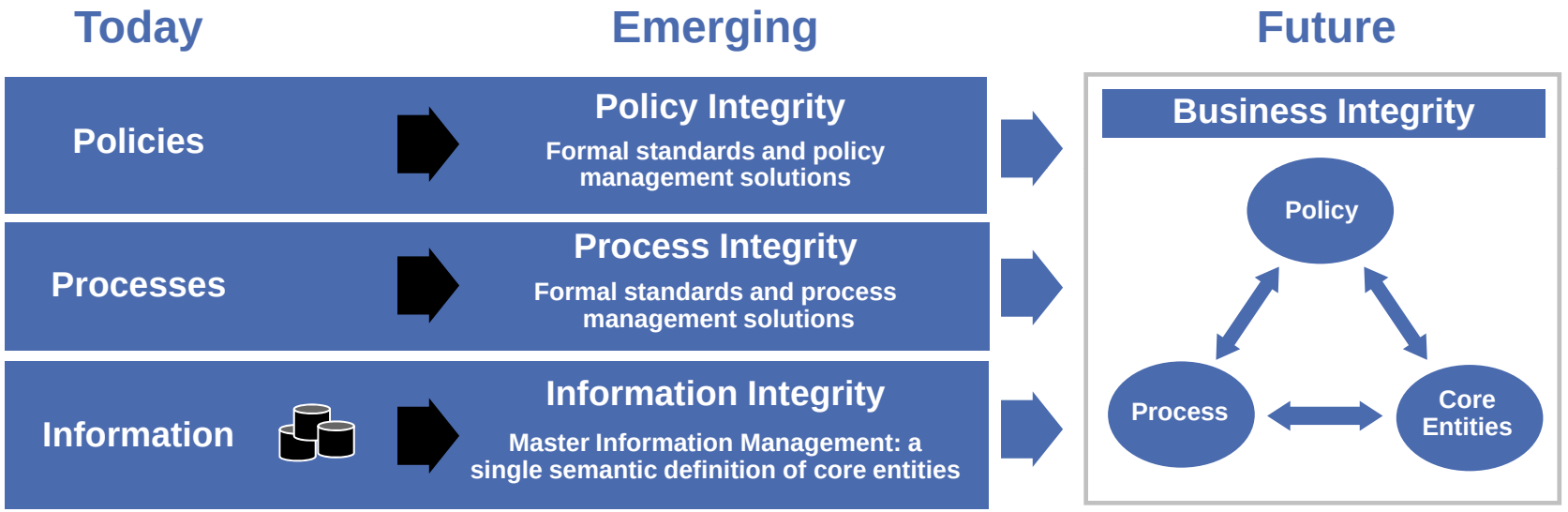


Example Value@Risk

	Leakage	Obfuscation	Modification
Threat	10/year	2/year	1/year
Consequence	$1M/ event	$0.5M/ event	$10M/event
Vulnerability	80%	25%	50%
Net Financial Risk/year	8M	0.25M	$5M

2. Continuous assurance of IP integrity requires simultaneous integrity management across policy, process, and information

We are in the embryonic stages of a new epoch in IP integrity management as businesses evolve to develop a consistent and interdependent view of their policies, processes, and core entities



- Today information, processes and policies are typically inconsistent and incomplete
- Emerging solutions address consistencies and management of policies, processes and core entities independently
- An integrated and automated approach to policy, process and core entity management will emerge to ensure business integrity is maintained at all levels of the enterprise

2. Continuous Assurance often relies on continuously capturing and cross validating provenance among policies, process, and information of IP

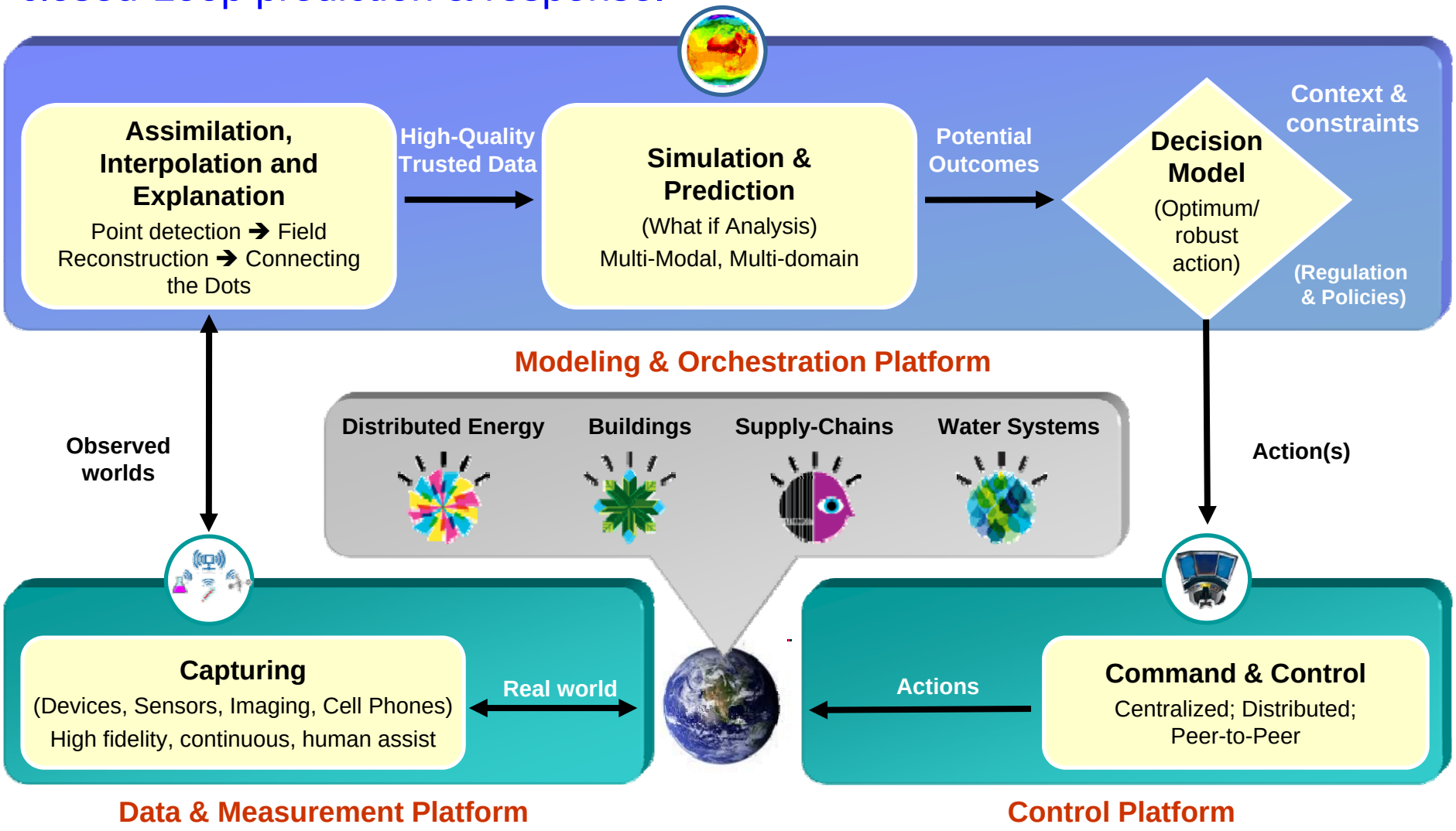
- Traditionally, provenance provides ownership history of a valued work of art or literature and is used to determine its authenticity
- Authenticity of provenance information is critical to ensure the integrity of the corresponding object
- For example, the provenance of the Mona Lisa is incomplete as it was stolen in 1911 and its whereabouts was unknown for two years
- Information provenance will capture the history of data objects and the processes that act on them

Provenance:
Acquired by François I, either directly from Leonardo da Vinci, during his stay in France, or upon his death from his heirs, the painting remained in the royal collections from the beginning of the sixteenth century to the creation of the Central Arts Museum at the Louvre in 1793. We know that it was kept at Versailles under the reign of Louis XIV and that it was in the Tuileries during the First Empire. Since the Restoration, the Mona Lisa has always remained in the Louvre Museum, a key piece of the national collections.

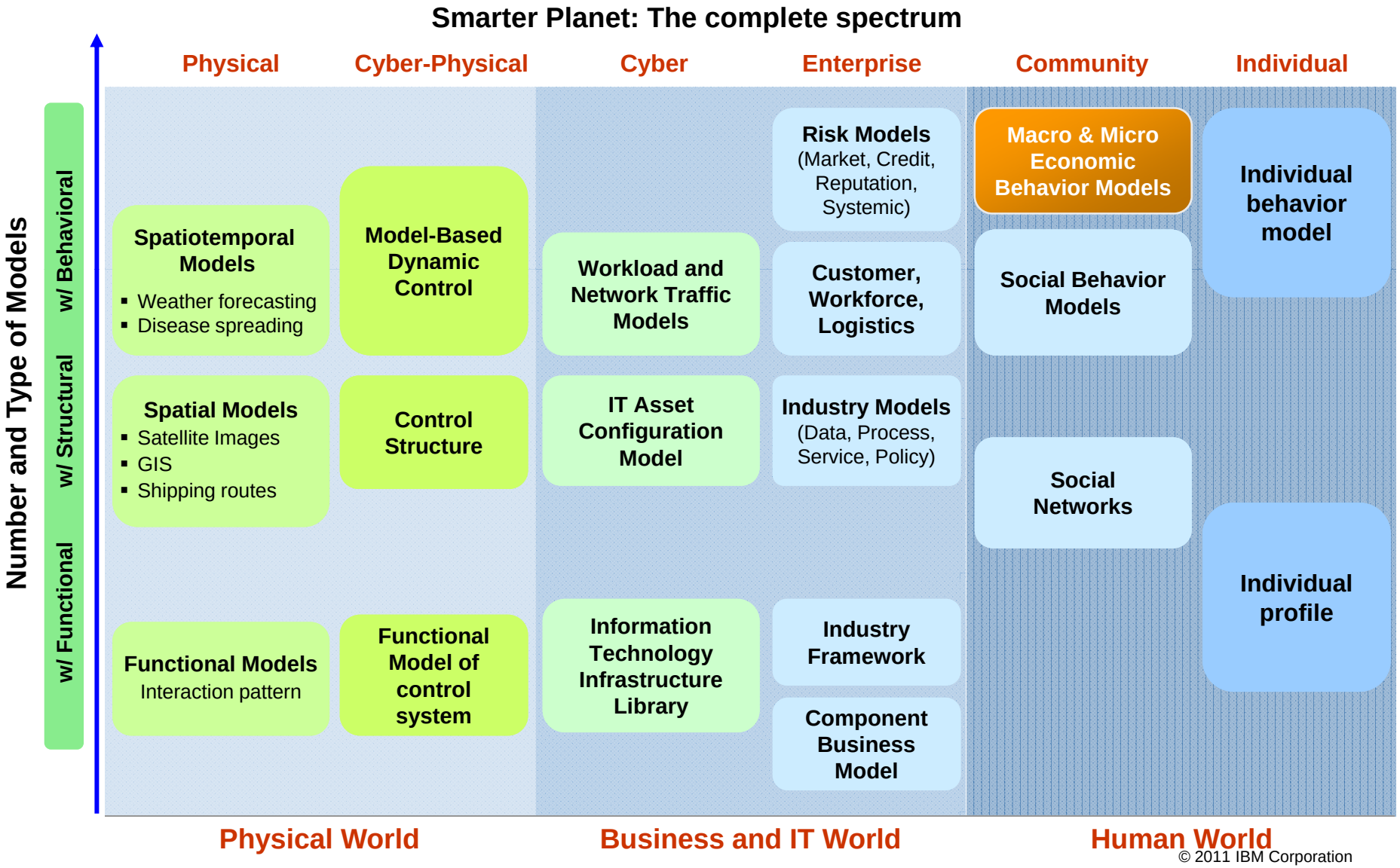
Source: http://www.hepguru.com/monalisa/main_intro.php

Provenance provides a documented history of an object

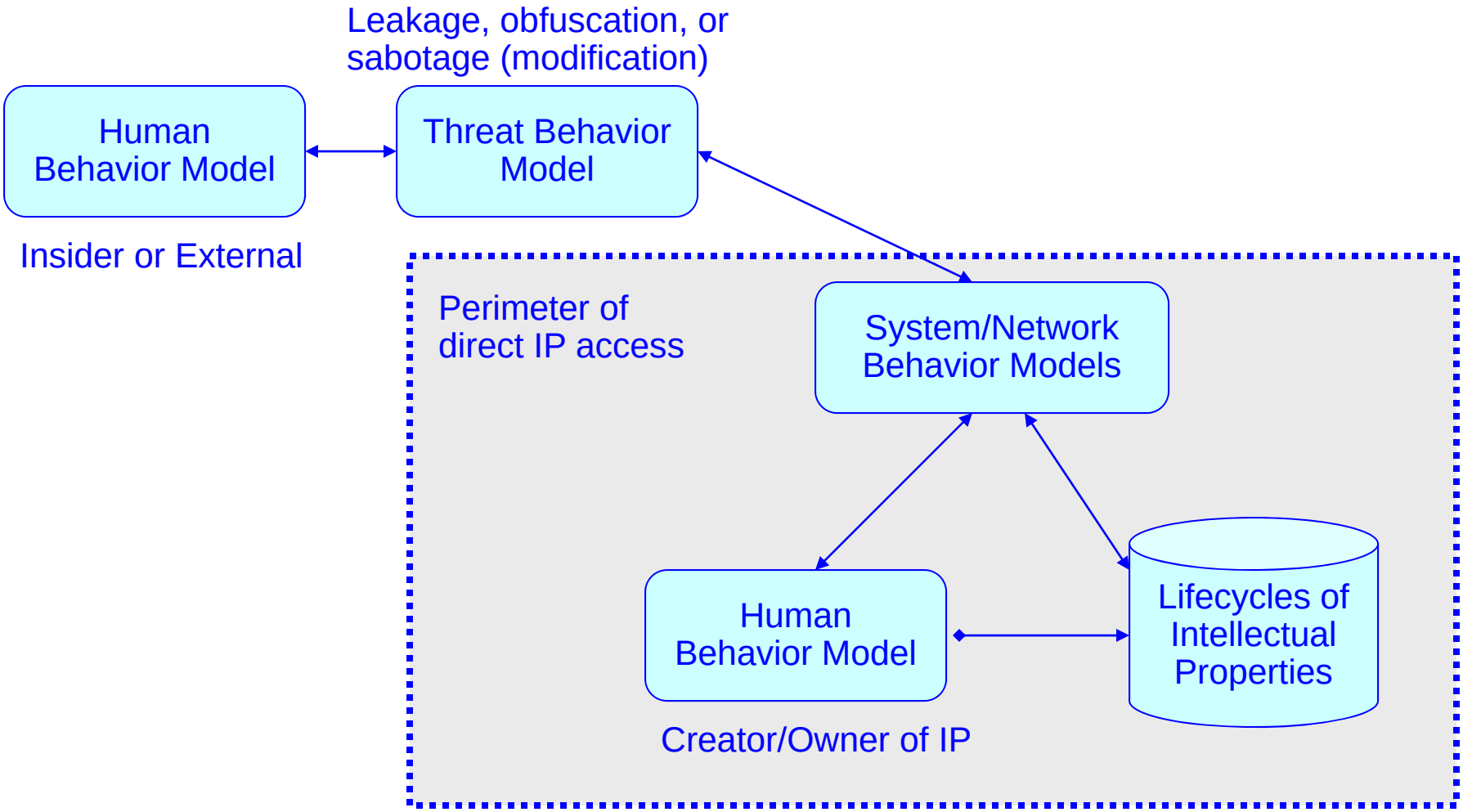
3. Integrity Management: Interconnected platforms provide dynamic capture & assimilation of data, the orchestration of behavioral models, and control for closed-Loop prediction & response.



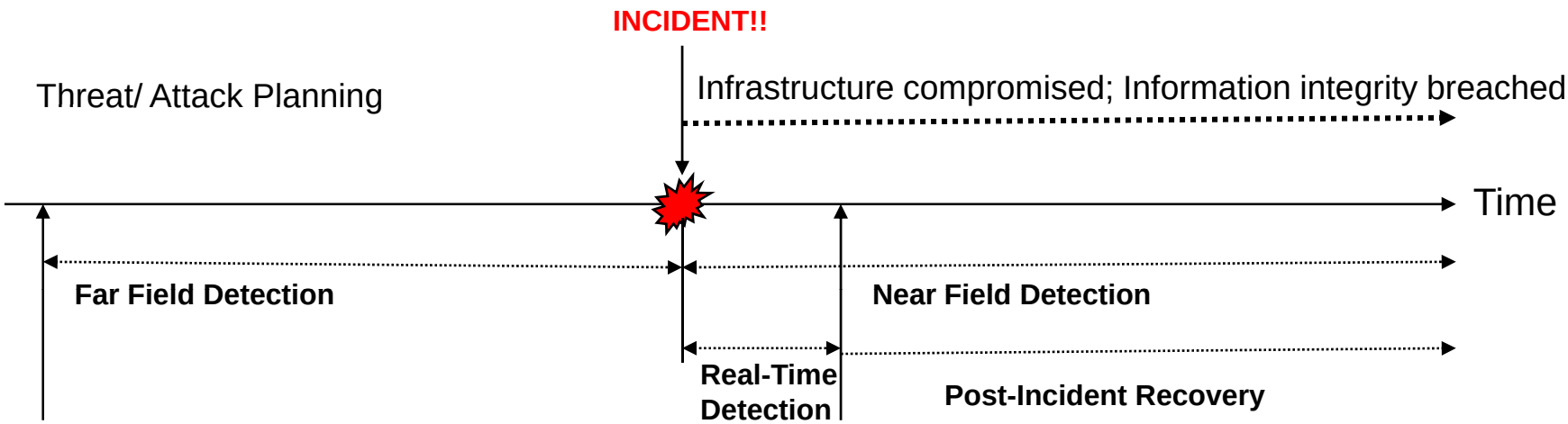
3. Capturing behavior models across the entire landscape will facilitate continuous integrity management



3. Behavior Models from human, social networks, threats, system, and lifecycle of intellectual properties are often tightly coupled



3. Mitigate the explosive growth of insider threats by using behavioral analytics and far-field detection techniques.



- Detecting and preventing abuse of authorized access is key to preventing insider attacks.
- *Far Field Detection*: Behavior monitoring of users to systems and networks as well as an analysis of user profiles, their business relationships and social networks can provide early warning indicators (in temporal, spatial and spatio-temporal dimensions) of insider attacks.
- Maintaining provenance of information and processes can improve auditability and accountability and facilitate information sharing without compromising security and privacy.

Summary: Moving to a more proactive and predictive stance is critical to tackling the challenge of Cybersecurity for Intellectual Properties

- Situational awareness is key and requires a wide range of sensors and systems that can operate both prospectively and in real-time
- Attack attribution is important
- Cyber defenders will have to deal with rapidly evolving situations as attackers use a wide range of techniques with widely ranging timescales, and can be expected to be able to rapidly switch among pre-loaded attacks as the situation evolves.
- Increasingly, systems will need to not only detect the problems but be able to implement a wide range of adaptive defenses either automatically or semi-automatically, examine the results of the defenses, and alter them accordingly
- Defense requires proactive preparation of home-court

Questions?

Please feel free to contact

Tilak Agerwala (tilak@us.ibm.com)

Chung-Sheng Li (csli@us.ibm.com)

J. R. Rao (jrrao@us.ibm.com)

Backup Charts

Intellectual Properties

wikipedia.org

- **Intellectual property** (**IP**) is a term referring to a number of distinct types of creations of the mind for which a set of exclusive rights are recognized—and the corresponding fields of law.
  - Under intellectual property law, owners are granted certain exclusive rights to a variety of intangible assets, such as musical, literary, and artistic works; discoveries and inventions; and words, phrases, symbols, and designs.
  - Common types of intellectual property include copyrights, trademarks, patents, industrial design rights and trade secrets in some jurisdictions.

- The existence of IP laws is credited with significant contributions toward economic growth.
  - Economists estimate that two-thirds of the value of large businesses in the U.S. can be traced to intangible assets.
  - "IP-intensive industries" are estimated to generate 72 percent more value added (price minus material cost) per employee than "non-IP-intensive industries".

- A joint research project of the WIPO and the United Nations University measuring the impact of IP systems on six Asian countries found "a positive correlation between the strengthening of the IP system and subsequent economic growth."

32% of the losses due to cyber attack result in theft of intellectual property; serious cost incurred on 92% of the loss cases for enterprises

Source: *Symantec 2010 State of the Enterprise Security*

- Most common losses are
  - Theft of customer personally identification information (32%)
  - Downtime of environment (32%)
  - Theft of intellectual property (32%)
  - Theft of customer credit card information

- Most common costs are
  - Lost productivity
  - Lost revenue
  - Loss of customer trust

- Average combined cost to enterprise: 2M/year (2.8M for large enterprise)

Companies lost on average $4.6M worth of intellectual property in 2008

- **Globalization**: More and more vital digital information, such as intellectual property and sensitive customer data, is being transferred between companies and continents—and lost. The average company has $12M worth of sensitive information residing abroad. Companies lost on average $4.6M worth of intellectual property in 2008.
- **Perfect information security risk storm**: as increased pressures on firms to reduce spending and cut staffing lead to more porous defenses and increased opportunities for cybercriminals. 42% respondents interviewed said laid-off employees are the biggest threat caused by the economic downturn.
- **Geopolitical Perception**: Elements in certain countries are emerging as clear sources of threats to sensitive data, in particular to intellectual property. Geopolitical perceptions are influencing data policy reality, as China, Pakistan, and Russia were identified as trouble zones for various legal, cultural and economic reasons.
- **Intellectual Property - the new currency**: Cyberthieves have moved beyond basic hacking and stealing of credit card data and personal credentials. An emerging target is intellectual property. Why sink all that time and money into research and development when you can just steal it?

Source: Purdue University Center for Education and Research in Information Assurance and Security, *Unsecured Economies: Protecting Vital Information*, 2009.

Case Study: Unfair competitive Advantage

- An employee at Acme Tele Power Private Limited, an India-based company, allegedly leaked the software component of Acme's patented product, Power Interface Unit (PIU), to Lambda Eastern Telecom, Acme's competitor, in June 2006. Soon after the leak, the employee left Acme and joined Lambda, reportedly for a large pay increase. Acme claims that Lambda developed its product, BTS Shelter, based on the stolen research and development (R&D). Acme alleges that Lambda could not have made their product in such a short period of time without illegally using Acme's intellectual property. The police were called to investigate and did eventually arrest the accused employee, although he was later released on bond. The role of Lambda in the incident remains unclear. Acme later moved its $10 million R&D operations to Australia, in hopes of finding a more business-friendly intellectual property protection environment.

- In 2008, a former Intel Corporation employee allegedly downloaded one billion dollars' worth of confidential intellectual property documents before leaving the company to join AMD, a competitor. The U.S. Federal Bureau of Investigation (FBI) found more than 100 pages of sensitive documents and 19 computer-aided design (CAD) drawings of future processor chips at the home of the accused. The U.S. Department of Justice and the FBI was called after another Intel Corporation employee learned that the accused had started working for AMD before terminating employment with Intel, and that sensitive information had been accessed during that time frame. The former employee was charged in September 2008 with five counts of stealing trade secrets and wire fraud. He faces up to 90 years in prison if convicted on all counts. AMD did not use the information, but another company may not have been so ethical.

Source: Purdue University Center for Education and Research in Information Assurance and Security, *Unsecured Economies: Protecting Vital Information*, 2009.

Case Study: Protecting Trade Secrets

- A former product engineer at Ford Motor Co. has been charged with stealing sensitive design documents from the automaker worth millions of dollars. Xiang Dong Yu, of Beijing – also known as Mike Yu – was arrested at Chicago's O'Hare International Airport upon his entry into the U.S. from China, where he is working with a Ford rival.
- Yu, 47, was charged with theft of trade secrets, attempted theft of trade secrets, and unauthorized access to protected computers. Yu had access to trade secrets contained in Ford system design specification documents. The documents contained detailed information on performance requirements and associated testing processes for numerous major components in Ford vehicles.
- The documents, created and maintained by subject matter experts at Ford, are used by design engineers when building new vehicles and by suppliers providing parts to the company. According to the indictment papers, Ford has spent "millions of dollars and decades on research, developing, and testing" to create the requirements in the system design documents. Yu allegedly attempted to sell the stolen documents to a Ford competitor in China

Source: The financial management of cyber risk, internet security alliance