We never got our arms around the root causes and consequences of systemic risk in financial systems, or the cyber impacts upon them

- ***Consider a different way*** to look at financial institutions
- ***And a different way*** to quantify risk consequences to stakeholder and national interests
- **It may lead to more effective, measurable ways to manage Financial Enterprise Risk**

Andrew Haldane, Executive Director of the Bank of England, recently observed:

"…systemic risk in the financial system is analogous to the reliability risks posed by complex networks encountered in fields such as ecology, epidemiology, biology and engineering…"

A Financial System Risk Dilemma

Critical infrastructure systems[(1)] are complex "systems-of-systems" with thousands of interdependent components and myriad channels.

As financial instruments, the organizations that hold them and the cyber technology that manipulates them, become more complex, they present *systemic risks* and *exploitable vulnerabilities* that - once triggered – have a runaway effect, with severe public consequences and enterprise costs.

This changes everything!

- IT controls all information and every transaction
- Outsiders are insiders
- 2nd/3rd order threats *(e.g. counterparty risks)* are in the same league as liquidity or market risks
- Highly sensitive corporate information is exposed
- Small incidents have current period enterprise consequences

(How) can we protect our most vital Information Assets?

(1) e.g. DoD Global Information Grid, the electric power "Smart Grid", Refineries, Financial Systems, etc.

System characteristics – complexity, real-time speed, constant change

Significant Cyber impact • Information Asset privacy breach has enterprise risk implications • Affected by SW defect density • McKinsey comments regarding bank counterparty risk(1) **"… IT plays a major role in all four pillars…"**	Level threat field • Outsiders are insiders • 1st, 2nd, 3rd order risks have similar impact
Real-time dynamics: asset value, balance sheet fluctuations • Mark to Market • Money Market values • High-speed trading	Hides perpetrators • Cyberspace presents "covert channels" • Attribution is almost impossible
Exposure from major corporate transition programs • M&A blending • Cloud adoption	May combust spontaneously • Hair trigger instabilities

(1) *Getting to grips with counterparty risk* McKinsey Working Paper on Risk, No 20
Nils Beier, Holger Harreis, Thomas Poppensieker, Dirk Sojka and Mario Thaten

High-impact[(1)] Consequences – Financial, Reputation, Regulatory

Good IT hygiene contains up to 95% of cyber risk
and most consequences may be reversed or financially mitigated

When enterprise, stakeholder interests may be directly affected, fiduciaries look to these risk indicators:

1. Does it compromise company-private and insider information?
   - Corporate financials, executive communications and operations info are subject to leaks
2. Does it incite regulatory (and legal) overreach?
   - Even the *appearance* of compromised consumer privacy or share value erosion may incite regulatory response
3. Will we incur unplanned costs?
   - Costs to repair, respond and remediate breaches, fines and PR activities may have P&L or share value impact
4. Does it impact Public/Consumer Confidence?

(1) Almost 50% of Global 1,000 companies lost 20% or more in share price in less than a month during the past 10 years - some never recovered

Most major losses were as a result of a series of high-impact but low-likelihood events…"
Deloitte report, *Disarming the Value Killers — A Risk Management Study*

The Challenge

Identify hi-impact, enterprise risk to information assets with current period enterprise implications

1. Make order out of the complex system chaos

ASSETS	THREATS	VULNERABLITIES
Loans	Overall Economy	Terms & Conditions
Deposits	Industry Economy	Product Diversity/Concentration
Equipment Leases	Interest Rates	Counterparty Diversification
FX	Currency Fluctuations	Contingency Liquidity
Derivatives	Market Volatility	Leverage
Warrants	Market Liquidity	Liquidity
Stocks	Potential Changes in Tax Law	Transparency
	Competition	Predictability of Asset Demand
	Inside fraud	Capital Adequacy Position
	APTs	

2. Measure/rank order risks by consequence
3. Allocate Information Privacy resources commensurate with exposure

DataVantage®
Direct Computer Resources, Inc.

How?

Identify high-impact Information Assets

- See the whole picture
  - ✓Discover and maintain Enterprise Risk Architecture
  - ✓Apply a numerable asset-threat-vulnerability taxonomy
- Prioritize Information Assets by quantified potential exposure
  - ✓FMEA system engineering techniques
  - ✓Actual value vs probable value
  - ✓Current (10Q) financial consequence & brand impact

Protect high-impact Information Assets (and control signals)

- Protect the DNA from inside – *beyond simple encryption*
- Adopt a consequence-based Risk Triage policy – a crisis response "knee board"

Identify high impact information assets

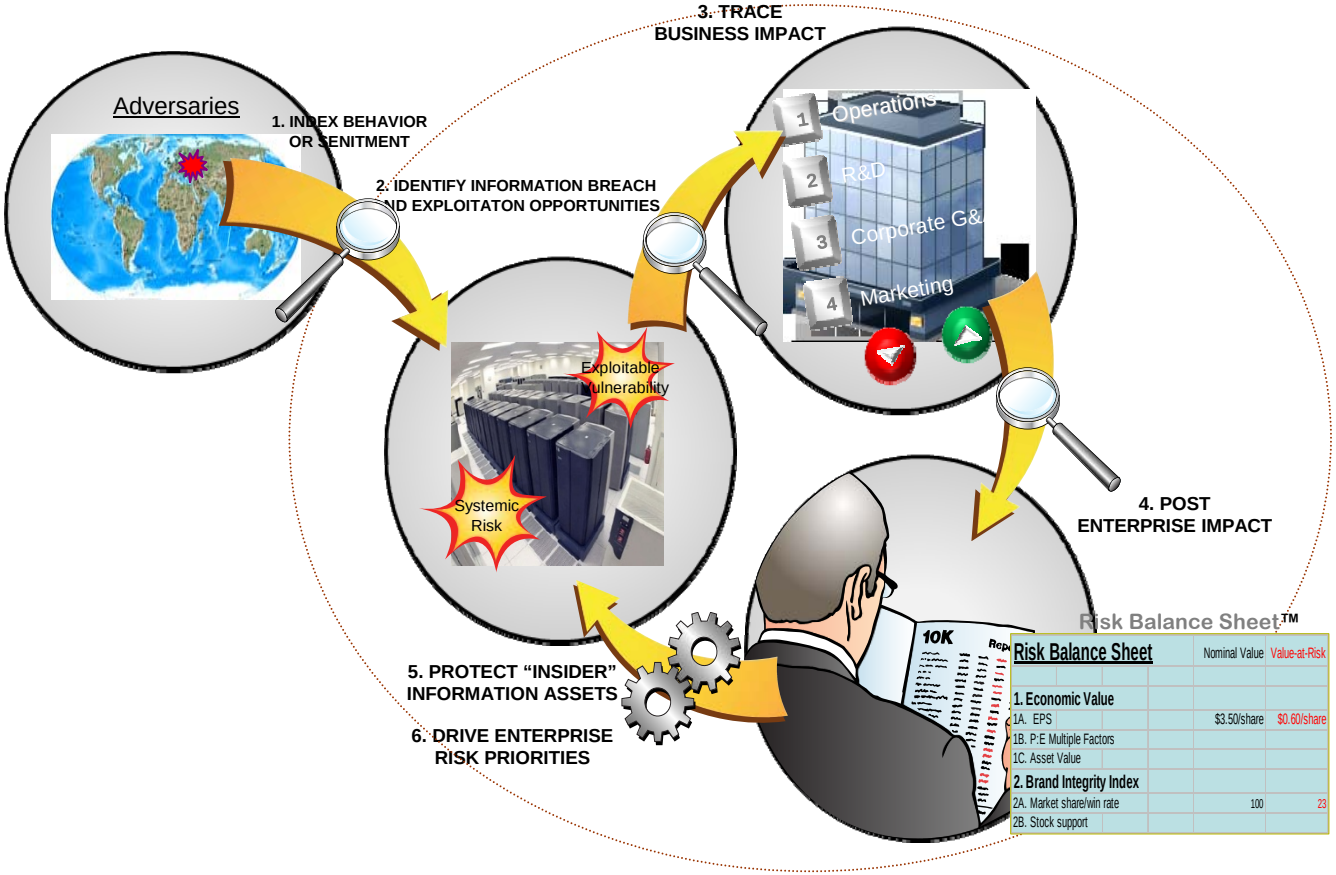
"Discover" Enterprise Risk Architecture

Trace propagation of breach incidents "from stakeholder to wiring closet to board room".

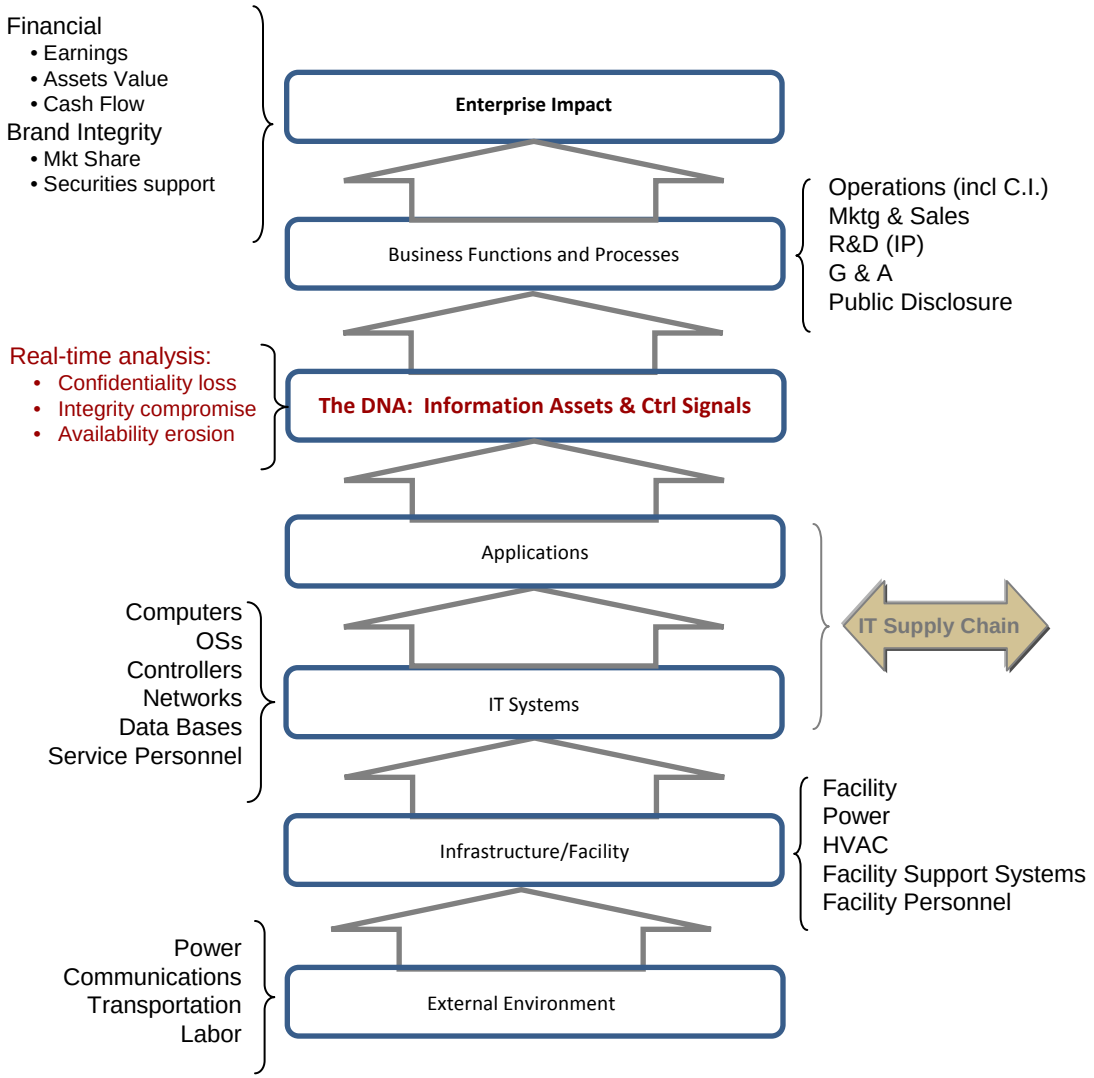
- Quantify Financial Consequences
- Measure evolving stakeholder sentiment

Drive expenditures from a risk balance sheet

- commensurate with Financial and Brand (Political) Exposure



A simple Enterprise *Risk* Architecture line of sight



Protection from inside – beyond simple encryption

Render high-impact corporate information *(DNA)* near-tamperproof

- Protect from within so that WHEN it is found, it cannot be compromised
- Encryption is part of a complete solution

Encryption

- Hides/un-hides data, but the original data are not altered
- Data are either completely hidden or *completely revealed*
- All data are affected and *nothing sensitive is removed*

Data Masking

- Alters data to permanently "remove" data or parts of data that are not to be revealed (that is, private or sensitive)
- Due to implications and the arrangement of the data, often large amounts of data must be masked
- Large amounts of data affected which *substantially reduces value for testing*

Information **Obfuscation**

- Alters permanently the "information" content that the data represents
- Generally only major relationships need to be altered
- Generally a small fraction of the data is affected resulting in much less processing

Future Preparation

Short term: Adopt a Risk Triage policy

- Many attacks rely on saturation
- Prioritize and focus resources on high-impact incidents

Long term: Re-arrange coupling of critical information (and control signal) processing "islands"

- Apply resilient interconnection architectures
  - ✓Public networks
  - ✓Highly controlled access (guards and information diodes)
  - ✓Air gaps
- Apply DHS Safety Act designated information protection

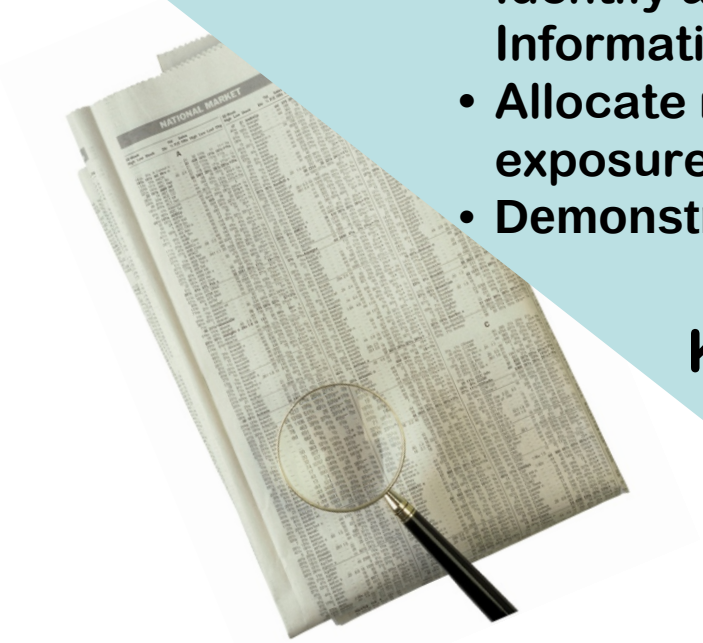
Educate Executives, Fiduciaries, Board Members

Become aware of enterprise implications of cyber risk

Imbed cyber risk in Enterprise Risk Policy

- **Identify and Protect High-impact Information Assets**
- **Allocate resources commensurate with exposure**
- **Demonstrate due care**

Know when you're done!



Robert K Gardner
NWTP@comcast.net