Cyber risk may have consequences that affect your next 10Q filing

"If Boards and senior management were paying more attention to the privacy and security of their digital assets, there may not be such a clamor on the Hill for legislation that would mandate cybersecurity requirements and/or standards"[(1)]. Boards must address the *Enterprise* exposure of cyber risk.

Today's Financial Systems are more complex and dynamic – due in part to the extreme integration of cyber control. The collection of cyber-powered financial enterprises and institutions comprise a complex system-of-systems with many interdependent parts connected through myriad channels. A failure or breach in one part of the system has the potential to cascade throughout with potentially serious consequences.

> *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…"*

Fortunately, most risks from cyber accidents, mischief, and even criminal penetrations may be mitigated by diligent IT hygiene[(2)]. And Advanced Persistent Threats (APTs) from adversarial nation states are tracked and managed by Federal agencies and Corporate members of the Defense Industrial Base.

However, there may still be high-impact risks[(3)] that compromise enterprise sensitive information, transaction integrity or consumer privacy. A security breach in these areas will have consequences which have material shareholder impact. ***These may in turn affect SEC filings, cause regulatory or legal overreach, and erode brand integrity and public confidence***. All of which threaten financial health and share value.

Fiduciaries and Boards must step up. However, they need better risk consequence information, quantified in terms of financial impact and stakeholder sentiment. Such information enables them to allocate risk management resources commensurate with exposure, demonstrate due care and pursue a prudent messaging and disclosure policy.

And that requires a different analysis – a different way to see financial institutions' cyber systems, a different risk narrative.

(1) *Boards Are Still Clueless About Cybersecurity;* Jody Westby, Forbes May 16, 2012

(2) NGOs, Trade Associations and Federal agencies (e.g. ANSI, ISA and NIST) publish sound cyber-care guidelines and best practices.

(3) 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 financial system isn't at all what is used to be

We used to think of the financial system as a collection of assets, transactions, instruments and institutions. Today it is a 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.

Our modern systems exhibit increasing, indeed runaway complexity, real-time dynamics and are subject to significant enterprise transition programs, as well as other risk inducing characteristics, as summarized below:

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

This requires a different look at the cyber infrastructure.

The cyber systems that manage, store, communicate and control virtually all financial activity, the "central nervous system" of the financial industry, behaves more like a real-time process control system, or SCADA (Supervisory Control and Data Acquisition) system than a traditional management information system. And it is itself very complex, with a high defect density (modern software has approximately one functional error or security hole for every 150,000 line of code. Do the math!) And, it is so tightly imbedded in individual institutional systems as well as the integrated financial eco-system, that cyber vulnerabilities are virtually indistinguishable from financial activity or process vulnerabilities. This is indeed a system engineer's prescription for systemic risk.

We may gain deeper insights into systemic risk applying lessons from other complex-adaptive systems-of-systems. One such approach—from the field of system engineering [4]—holds special promise in this regard.

(4) Field of study attributed to AT&T Bell Laboratories

Looking through the shareholders lens, aligning with Boardroom risk deliberations

Boards have a duty to protect the assets, including the digital assets, of their companies and to protect their shareholders' interests. To that end, they consider factors affecting earnings per share (EPS) and the price-to- earnings ratio (PE Multiple) that reflects the leverage upon EPS that drives share value, represented in the simple formula:

Share value = EPS X P:E Multiple

High impact financial and brand (public sentiment) factors, such as cash, revenue or profit margin erosion, competitive position and adverse publicity, which may have a current reporting period impact on financial statements and concomitant share value, are of particular importance.

When the extent of that erosion is quantified as exposure, management selects a *risk response strategy* to mitigate such exposure, which may include one or more of:

1. Avoidance: exiting the activities giving rise to risk
2. Reduction: taking action to reduce the likelihood or impact related to the risk
3. Response: providing emergency response, disaster recovery programs to limit risk impact.
4. Hedge or Insure: transferring/sharing a portion of the risk,
5. Accept: And disclose that acceptance

Total expenditures to mitigate risk can be contained commensurate with exposure only if and when such exposure is quantified. Prudent disclosure of which may quell concerns and adverse reactions of customers, investors and regulators alike.

This discussion occurs in critical infrastructure industry Boardrooms for non-cyber issues - but have not included serious cyber issues that should receive Enterprise Risk attention or resources. They seem only to provide a modest uptick in CISO budgets, and perhaps a few minutes of board meeting time to hear from CISOs.

Why?

Part of the reason appears to be that Cyber professionals, even officers such as CIOs and CROs have not presented the situation in a true Enterprise Risk context.

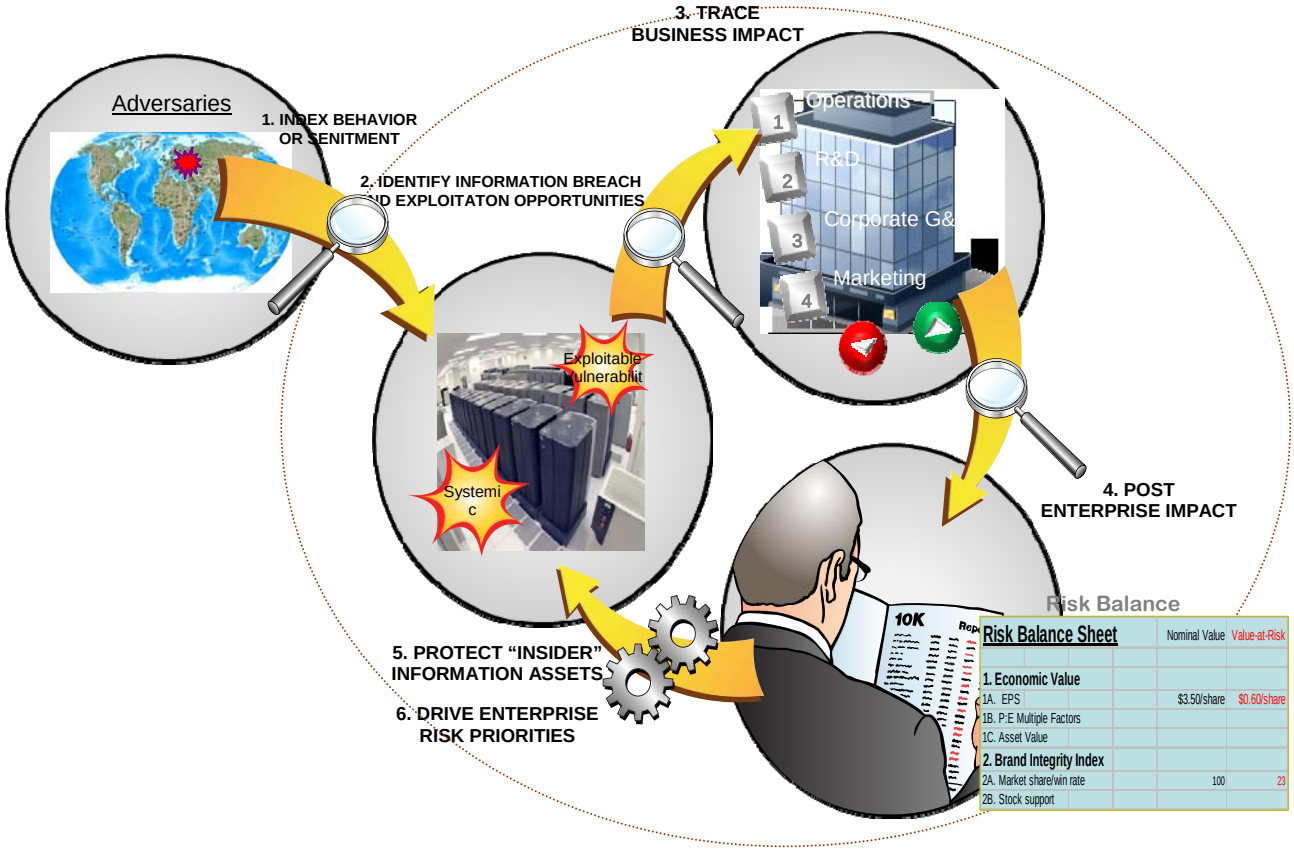
- **Chicken Little syndrome:** Executives have been overwhelmed by fearsome rhetoric surrounding cyber security. They hear about APTs and impending crises from industry (and government) spokespersons who present well intentioned *fear-uncertainty-and-doubt* (FUD) arguments for the cyber security case. And CFOs believe they have been cornered into funding the latest cyber security widgets and services to prevent the newest Threat du Jour. And still they are not sure what good it has done.
- **From the lens of the wiring closet instead of the Balance Sheet:** Causes and consequences that do not immediately relate to the enterprise risk narrative and presented in business rather than technical (geeky) terms as described above cannot be received, understood and integrated into the larger Enterprise Risk calculus.

What can be done?

First, know what needs protecting.

A consequence-driven, enterprise risk analysis must be pursued that recognizes the analysis target as a complex real-time system (rather than a traditional IT information system). In order to inform executives with information that can result in resource allocation decisions, results must quantify exposure in financial terms as well as stakeholder sentiment indices. A three stage process is required:

1. An Enterprise Architecture framework is "constructed" which presents the widest perspective – from adversary to wiring closet to Balance Sheet. And it must be detailed, with measurable elements that facilitate tracing and quantifying consequences of incidents as they propagate – as potentialthreat vectors passing through progressive vulnerability matrcies.These will calibrate both systemic risks triggered or exacerbated by cyber incidents as well as highly exploitable vulnerabilities.
2. Posting financial and brand results in a Risk Balance Sheet, appropriate to each subject institution.
3. Rank ordering Information Assets by their respective net exposure in order to highlight high-impact items, those above a risk graph inflection point, that require specific protection.



Then, protect what matters most

Information assets that have been identified as vital (i.e., assets that are equivalent to the corporation's "DNA") should be rendered near-tamperproof. While encryption should be a part of the protection tool kit, enterprises should also utilize DHS Safety Act designated Qualified Anti-Terrorist Technology (QATT) and other data masking and information obfuscation techniques and tools.

These inside protection measures are key to risk reduction strategies designed to reduce high-impact Enterprise incidents or their consequences.

They are also necessary to consider for significant enterprise transition initiatives, such as during Cloud Adoption efforts, digital system blending from M&A activities or Main Frame to Distributed conversions. These activities tend to employ 3rd party transition teams and transition test procedures which introduce new failure mode and/or tampering vulnerabilities.

In summary

Only executives and Boards can integrate Cyber Risk into the Enterprise Risk Governance of their companies. The consequences of not doing so could have current reporting period consequences and incite regulatory and legal overreach. The process of doing so does not require extraordinary measures or expenditures. But it does require a new perspective:

1. Executives and Boards should become aware of the enterprise exposure from cyber risk and imbed that into their enterprise risk policies by:
    a. Identifying and protecting high impact information assets;
    b. Allocating resources commensurate with cyber exposure; and
    c. Demonstrating due care with prudent cyber risk actions and disclosures
2. Cyber teams must pursue a different analysis – a different way to see financial institutions' cyber systems, a different risk narrative.