



The Business Case for Risk  
Management – Protecting  
Intangible Assets to Drive  
Value for the Business

SARMA Conference  
Robert P. Liscouski

May 13, 2008

**STEEL  
CITY  
RE**

# Highlights

- **Security affords physical and emotional benefits**
  - Prevents future adverse effects
  - Creates a belief state of stability and reduced risk
- **Security creates intangible asset value**
  - Value to business stakeholders of risk mitigation, resilience, and enterprise value protection
- **The business value of intangible assets can be quantified**
  - Superior managers of their intangible assets reward their shareholders with above average financial returns
- **Businesses should manage security as a valuable intangible asset**
  - Realizing value from investment in security happens when companies become superior managers of their intangible assets

# Business Risk

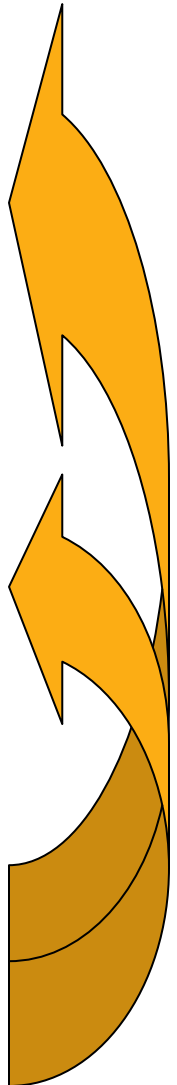
- This country has not suffered from a terrorist attack on its soil in the six years since the September 11th attacks. However, the threats are real, continuous and dynamic.
  - The USG focuses on hardening critical infrastructure and related targets.
    - Al Qaeda (and its surrogates) are intent on conducting attacks in the US that damage our economy and impact the American psyche.
  - Future targets are likely to be “Icons” (well known brand) or business/sector leaders.
    - These businesses (soft targets) will be the focus because of their readily identifiable “American” iconic value and psychological and economic impact if attacked.
      - (Results of the attack on the World Trade Center in 2001 surprised even Bin Laden.)
    - This is a MO that has been demonstrated since the USG has been collecting data on terrorist attacks world wide.
  - The value of iconic targets is mostly intangible.
    - An attack resulting in a loss of Intangible Asset value (reputation, brand, security, quality, trademarks, patents, copyrights, trade secrets, or confidence in a company’s ability to stay in the marketplace) could put the company’s valuation in free fall, and lead to business failure

# Private Sector Responsibility

- The government lacks complete knowledge of vulnerabilities of private sector infrastructure and related threats.
  - More importantly, the government views protection as the responsibility of the respective companies that comprise critical and other infrastructure components and soft targets.
  - Private sector companies (which own over 85% of the critical infrastructure) are challenged to make security investments to achieve the “right” level - if it could be defined.
  - USG, State, Local Law Enforcement, and the Private Sector have invested \$billions to secure infrastructure and this nation,
- What is “secure enough” and how would we know when it is achieved?

# CEO & Board Concerns in a Dynamic Business Environment

- Reputation (Recent CEO survey)
- Revenue
- Growth
- Sustainability
- Market Perception
- EBITDA, Earnings
- Stock price
- Where to invest the next \$1 – Sales, Operations, R&D
- Security, Disaster Recovery Plans, Business Continuity
  - Where are these issues on the CEO & Board radar?



# Central Business Challenge

- Defining the priorities for protection and the “right” level of security:
  - Linking priorities for protecting the company to priorities for protecting the country (what are the metrics?)
  - Managing Risk - Balancing investment in security and resilience with competing priorities to drive the business (are they mutually exclusive?)
- The “right” question is
  - How does management adopt best practices to
    - Manage security,
    - Communicate the value it’s created through security, and
    - Protect the value it’s created through security

# Defining the challenges to securing your business

- Identifying the priorities
  - Cyber Risk
  - Physical Risk
  - Personnel Risk (Insider Threat)
  - Interdependency Risk/Supply Chain Risk (you are both part of it and dependent on it at the same time)
  - Protection vs. Resilience (or both?)
  - Intangible Assets - Reputation and Brand Risk
- Managing Risk in a Dynamic and Ambiguous Threat Environment –
- Ensuring Commitment
- Making the Business Case
- Battling Complacency

# First, Set Priorities

- Linking priorities for protecting the company to priorities for protecting the country
  - What sector is your business in?
    - Critical Infrastructure?
    - Soft Target?
    - Supply Chain?
  - What are the critical business functions
    - Identify the tangible and intangible assets related to those functions
    - Link best practices to the critical business functions
- Managing Risk - Balancing investment in security and resilience with competing priorities to drive the business (are they mutually exclusive?)
  - Protect the right assets – At the right time – Drive value for the company

# Second, Identify and Manage Ambiguous Threats

- Effective identification and management of risk in today's dynamic threat environment requires the following:
- Clear understanding of the baseline threat environment
- Accurate identification and assessment of an entity's baseline vulnerabilities and security/mitigation measures
  - Vulnerabilities at a baseline level (normal operating environment) – Measures required when baseline changes:
    - People processes
    - Physical Measures
    - Cyber Measures

# Third, Commit

- Ensuring Commitment

- An organization must engage its leadership at the highest level
- Culture of communication
- Culture of Action

# Fourth, Invest

- **Making the Business Case**
  - **Justifying the long term investment**
    - Effective
    - Consistent
    - Sustainable
  - **Who pays** – Driving value into the business with the right solutions
    - Risk mitigation measures that contribute to corporate value
    - Protection and resiliency – i.e.. strong supply chain security = sustainability in the market place
  - **Measures to reduce vulnerabilities above the baseline as the threat changes**
    - Need to maintain flexibility to adjust to changing threat environment
  - **Where is the benefit** – the market needs to see action to reward behavior, so communicate
- **Insurance/Financial Incentives are a key part of the solution**

# Fifth, Combat Complacency

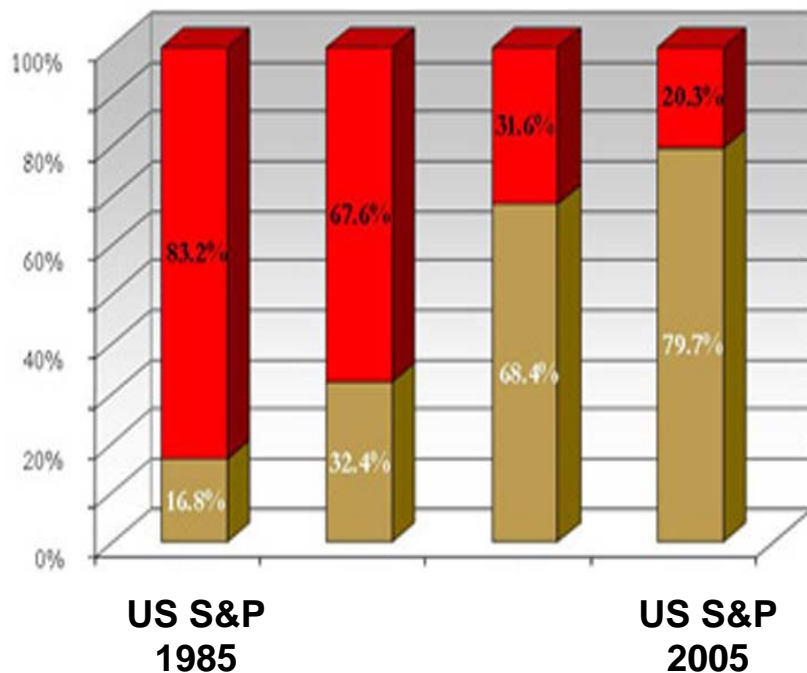
- “Eternal vigilance is the price of liberty”
  - Success in efforts may lead to lack of focus over time
  - Leadership may question sustainability of investments – unless material metrics are used
  - Metrics – can be difficult to obtain - Feedback for correlating threats to mitigation programs/effectiveness and continuous process improvement – *resulting in financial value*
    - Metrics must be constantly evaluated
    - Testing assumptions
    - Correlate actions to delivering value

# The Business Case for Security Recap

- What should be protected?
- What is the right level of investment
- Calculate ROI for security investment
  - The return is measured at the enterprise level
  - The return is embedded in the financial metrics that show how you've become a preferred business partner to stakeholders

# Defining Priorities - What Should Be Protected?

- Intangible Assets are the dominant form of value in your company.



- Intangible assets are generally not as well managed financially (or protected) as tangible assets.

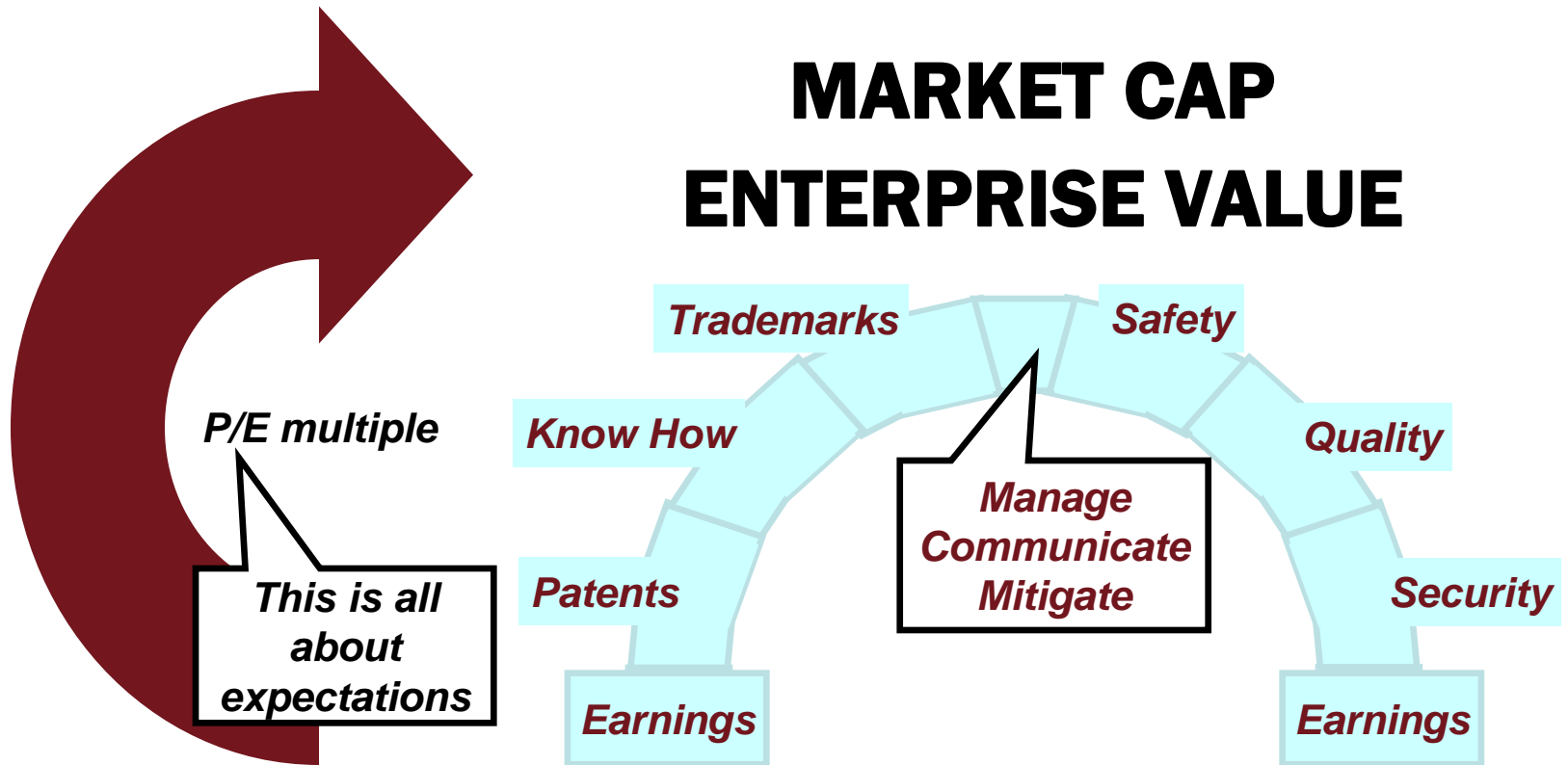
*Today, nearly 70% of the aggregate value of the broad US stock market is based on intangible assets.*

## Intangible Assets comprise...

Brand / Reputation	Copyrights
Patents	Quality / Integrity
Trademarks	<i>Security</i>
Know How	<i>Safety</i>
Trade secrets	<i>Resilience</i>

These are the key areas that differentiate the leading businesses from the competition.

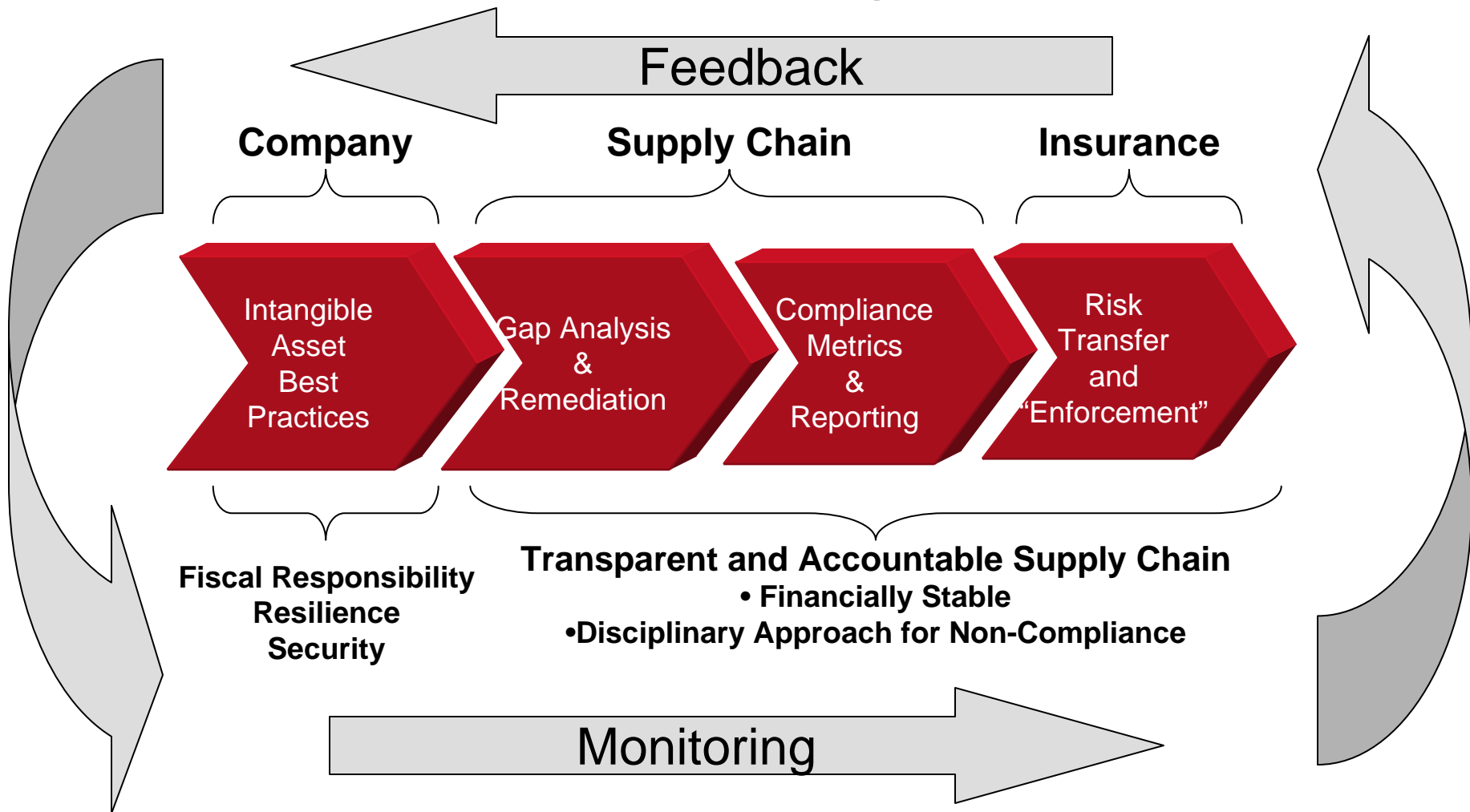
# Superior management of intangible assets supercharges your value



# Superior Intangible Asset Management Reward Shareholders

- Greater Sales
- Higher Gross Margins
- Greater EBITDA
- Higher Price / Earnings Multiples
- Greater Enterprise Value
- Stronger Market Capitalization

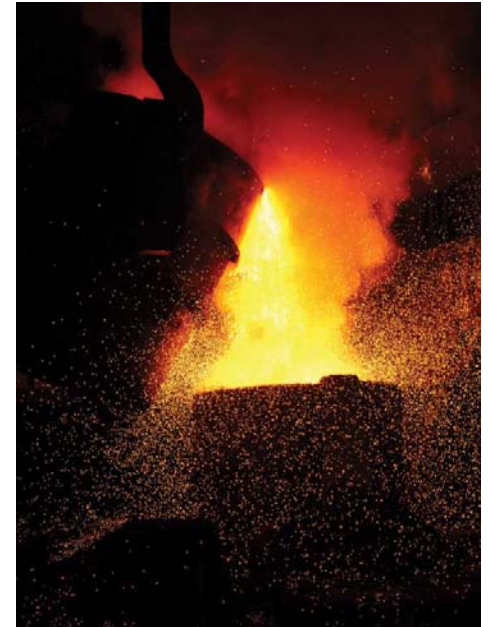
# Intangible Asset Protection and Resilience Cycle



# About Steel City Re

Robert Liscouski  
President, Advisory and Forecasting  
Steel City Re  
Henry W. Oliver Building  
535 Smithfield Street, 13th Floor  
Pittsburgh, PA 15222-2304 USA

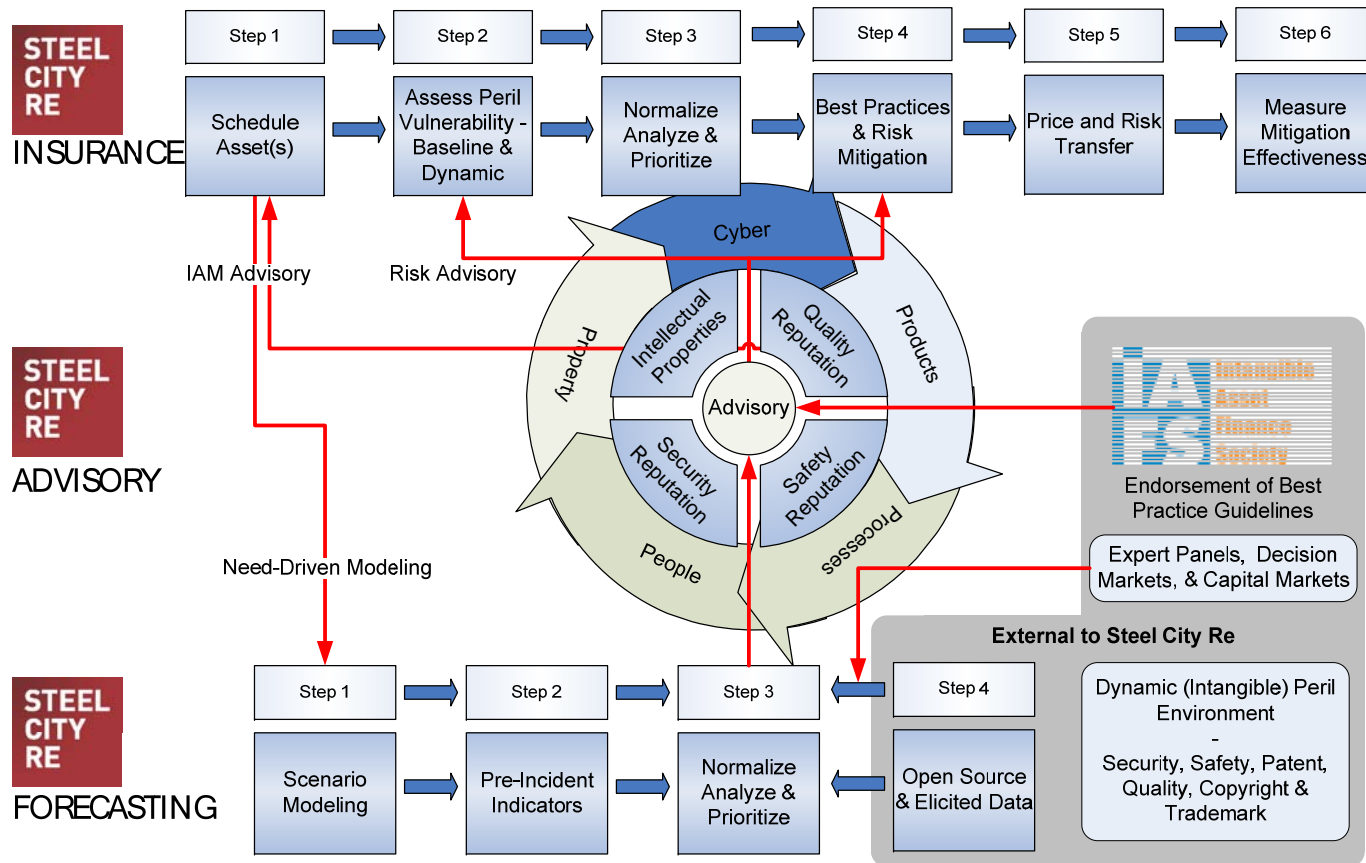
(412) 661-7076 x213  
(412) 291-3155 Fax  
[rliscouski@steelcityre.com](mailto:rliscouski@steelcityre.com)  
[www.steelcityre.com](http://www.steelcityre.com)



# Background

- **Senior Principals**
  - Nir Kossovsky, M.D, CEO; Robert P. Liscouski, President, Advisory; Peter J. Gerken, President, Insurance
- **Focus**
  - Helping our clients increase, protect and recover intangible asset value for more than 10 years.
- **Services**
  - Advisory, Forecasting, and Risk Transfer/Insurance
- **Sector Knowledge and Relationships**
  - Finance, risk, and intangible asset management
- **Qualifications Recap**
  - Proprietary and unique quantitative approach to enterprise value creation through intangible asset (reputation) management best practices

# Comprehensive IA Value Solutions



# Summary

- Address the new security risk paradigm
  - Soft Target Focus
- Protect (natural and manmade disasters) your business by engaging senior leadership & thinking broadly about creating enterprise value
  - Sustainability in the Marketplace – Security and Resilience
- Create value by managing your intangible assets
  - Identification of Intangible Assets + Gap Analysis + Best Practices for Intangible Asset Management + Compliance Measurements (Metrics) + Monitoring of the Business Operating Environment (Threats)+ Best Practice Adjustments for Changing Threats