Insider Threat and Cyber Security
A Full Spectrum and Holistic Capability

Jay McGowan
Founder, McGowan Consulting
Protect Your Intellectual Property

IP theft is an increasing threat across the globe and can go undetected for months and sometimes even years.
What is an Insider Threat?

A current or former employee, contractor or business partner who has/had authorized access to an organization’s network, system, or data.

An Insider may be witting or UNWITTING.
Is It Real?

The 2011 Cyber Security Watch Survey, conducted by the US Secret Service, the CERT Insider Threat Center, CSO Magazine, and Deloitte, found that in cases where respondents could identify the subject of an electronic crime, 21% were committed by insiders.

43% experienced at least one insider incident (2)

46% thought insider attacks were more severe than outsider attacks (2)
Can an Insider be stopped?

- Personal factors
- Organizational situations
- Behavior indicators
Partner

Leadership support should drive priorities from the top. Only 13 percent of companies have a cross-functional cyber risk team that bridges the technical, financial, and other elements of a company. (1)

- Information Assurance
- Security
- Legal
- Investigations
- Intelligence
Strategy

• Information Technology
  - How open or closed does a company need to be
  - Relate to industry standards

• Establish a program
  - Training and awareness
  - Enable technology
  - Foreign travel and contact notifications
  - Personnel security and evaluation
  - Report and analyze

• Data Management
  - Where to start

• Contingency Planning
  - Test it

• Resources
  - Law Enforcement
Information Technology

• Integrate data
  - Many datasets were never meant to be integrated
  - Correlate the entire enterprise
  - Events may begin in or out of the cyber domain

• Share appropriately
  - Competing priorities and different organizational equities

• Understand the landscape
  - Global enterprise
Establish a Program

• **Strategy**
  - Coordinate with all equities
  - Cross-disciplined team

• **Learn and improve**
  - Process is living

• **Grow**
  - 5 year plan
Data Management: Prioritize Importance
Contingency Planning

Testing
- How does it work?
  - external
  - internal
This is a Team Effort

- Educate and train on a recurring basis
- Protect proprietary information
- Screen new employees
- Provide convenient, non-threatening reporting
- Monitor networks
- Ensure personnel have necessary tools
- Get assistance