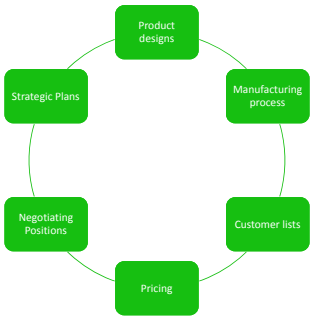
Protect Your Technology, Your Information, Your Business

ADVANCE Resources & Consulting

What is Your Stuff?



Who We Are

PURE MICHIGAN

- Michigan consulting firm with a mission to help Michigan companies protect their **people, technology** and **competitive edge** while growing their business in risk-prone foreign markets
- Former Senior Executive level intelligence and security professionals with experience operating overseas and in consulting for clients across a broad range of industries
- MEDC vendor supporting Michigan exporters with Intellectual Property protection and security assessments in high-risk foreign markets

ADVANCE Resources & Consulting

Does This Really Happen?

DUPONT, PIONEER A DuPont Company, NORTHROP GRUMMAN, BOEING, Westinghouse, Google, LOCKHEED MARTIN, Ford, DOW Dow AgroSciences, GM, valspar, USG, ALCOA, 3M

What is the Threat?

- Foreign governments…
- Competitors…
- Hackers…

WANT YOUR STUFF

Does This Really Happen?

SONY make.believe

Does This Really Happen?

Response

- *Understand the Threat*
- *Assess Your Vulnerabilities*
- *Prioritize Your Risks*
- *Implement Defenses*

Why Does It Matter?

JOBS

IP Theft costs US economy $300 billion per year*

= 2 Million Jobs**

*according to The IP Commission Report, May 2013
**estimate by the US International Trade Commission, 2011

Understand the Threat

Which Technologies Are at Greatest Risk?

- Aerospace
- Agriculture
- Alternative Energy
- Automation
- Automotive
- Biotechnology
- Chemicals
- Computers
- Environmental Technology
- Information Technology
- Manufacturing
- Materials
- Medical/Pharmaceuticals
- Satellites
- Telecommunications

Does This Really Happen?

- Traverse City
- Cadillac
- Grand Rapids
- Kalamazoo
- Marshall
- Marquette

Understand the Threat

Which Countries Present the Greatest Risk?

- China
- Russia
- India
- South Korea
- Taiwan
- France
- Brazil
- Israel

Understand the Threat
China

- Responsible for 80% of IP/Trade Secret theft against the US (FBI)
- Responsible for more cyber attacks against US targets than any other actor (US National Counterintelligence Executive; Mandiant)
- 96% of cyber attacks for economic espionage conducted by China (Verizon)
- Its technological development strategy is built on acquiring and adapting foreign technology – legally or illegally

Understand the Threat
How Do They Do It?

- Human Collection
  - Elicitation at conferences, meetings
  - Recruitment of employees (insiders)
  - Exploitation of business relationships



Understand the Threat
Who Do You Need to Worry About?

- Foreign intelligence services
- Foreign government funded institutes, universities
- Competitors (state-owned enterprises)
- International partners
- Freelancers, hackers
- Compromised insiders

Understand the Threat
Where Do They Do It?

Where you are most vulnerable…

- In their country
- In other countries
- In the US

Understand the Threat
How Do They Do It?

- Technical Collection
  - Cellphone, laptops
  - Cyber attacks
  - "Bugs" in hotels, meeting rooms, cars



Case Study: AMSC

Massachusetts-based company producing wind turbine control software

- Started in 1987 by 4 MIT professors
- Hired CEO with extensive Asia experience in 2006
- Partnered with Chinese company Sinovel
- China accounted for 2/3rds of revenue of $315 million

Case Study: AMSC

Technology lost in spite of strong security measures

- CEO personally interviewed 400+ candidates for 30 positions in China
- Factory assembled; firmware all shipped from US
- Software design server *not connected to internet*

Case Study: AMSC

Lessons Learned

- Foreign companies are not bound by the same rules, ethics as U.S. companies – *no level playing field*
- The danger from China's unfair competitive practices extends *beyond China*
- Focus on the ***human factor***

Case Study: AMSC

Technology Loss

- March 2011: AMSC techs in China discovered pirated software in wind turbine
- March 2011: Sinovel rejects $70 million shipment
- *March 2011: AMSC Software engineer at research facility in Austria traveled to Beijing*
- Investigation showed he:
  - Accessed software code from a laptop in China
  - Lived in apartment provided by Sinovel
  - Had 6-year, $1.7 million contract, signed by Sinovel CEO, to provide AMSC code and assist Sinovel

Break…

Case Study: AMSC

Impact

- Lost China market ($700 million unfulfilled contracts)
- Stock price dropped 84%
- Laid off 2/3^{rds} of workforce

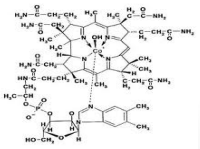
What Can You Do?

- Assess your vulnerabilities
- Prioritize your risk
- Implement defenses
  - Human vulnerabilities
  - Cyber vulnerabilities

Assess Your Vulnerabilities

Where Does Your Technology Rank?

- Know what they're looking for
- Is your technology unique?
- What are its applications?
- Supply chain vulnerabilities?



Assess Your Vulnerabilities

Places You May Not See as Risky

China "owns" the IT infrastructure in:

- Europe: Belgium, Romania, Turkey
- Africa: Nigeria, Tanzania, Angola
- Asia: Singapore, Thailand
- Middle East: Qatar, Saudi Arabia, UAE
- Latin America: Mexico, Guyana

Assess Your Vulnerabilities

Where Does Your Technology Rank?

China's 7 Strategic Emerging Technologies:

- Information Technology
- New Energy Technology
- Alternative Energy Auto Technology
- Advanced Manufacturing Technology
- Advanced Materials Technology
- Environmental Technology
- Biotechnology

$230 billion devoted to collecting these technologies over 5 years

Assess Your Vulnerabilities

Do You Have Foreign Business Relationships That Can Be Exploited?

- JV's, Acquisitions
- Suppliers, Vendors, Distributors
- Outsourcing
  - HR/payroll
  - Security
  - Legal

Assess Your Vulnerabilities

What Is Your Footprint Outside the US?

- In countries that target your technology
  - Permanent presence
  - Travel

- In other countries where it is easy for them to get at you

Prioritize Your Risks

What Would Shut You Down?

- Theft of product designs?
- Loss of one large customer, market share in one country/region?
- Loss of key employees?
- Loss of reputation in industry?

➢ *Focus defenses on areas of greatest risk*

Implement Defenses

Human

- Background Investigations
- Due Diligence
- Security policies, protocols
  - External drives
  - Cameras
  - Travel
- Training
- Company Culture

Implement Defenses

Cyber

- Network security tools
- Security training
- Appropriate connectivity precautions

- Managing credentials
- Vetting of administrators
- Auditing, monitoring

Travel Security Precautions

- Don't travel with information you don't need
- Take a travel laptop, cellphone – clean hard drive; do not connect those devices to network when returning home
- Carry any sensitive information on a thumb drive and keep that with you at all times

Summary

- Understand the threat
- Know where you're most vulnerable
- Prioritize your risks
- Defend your technology, your information, your people

Travel Security Precautions

- Use VPN for email; avoid public, unsecured wifi hotspots
- Don't leave laptop, phone in hotel room unattended
- Don't insert thumb drive given to you, found by you
- Don't access bank, credit card websites during travel
- Change email password when you return home
- Make sure firewall and virus protection are up to date and adjust security settings
- Minimize internet surfing; beware of phishing scams

Don't Be a Target of Opportunity

Thank you

ADVANCE
Resources & Consulting

250 Monroe Ave., Suite 400
Grand Rapids, MI 49503
(616) 608-2777
thys@advancerandc.com
www.advancerandc.com