Cyber-Security Risk- IP Theft and Data Breaches

Protecting your Crown Jewels Internally and with Your Key Third Parties

Pamela Passman

President and CEO

Center for Responsible Enterprise And Trade (CREATe.org)

Glenn T. Ware, Esq.

Principal, Leader, International Anti-Corruption, Corporate Intelligence and Strategic Threat Management

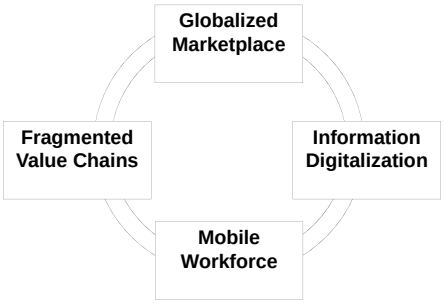
PriceWaterhouseCoopers - PwC

Luis Canuto

Global Ethics Investigations Co-Leader, Latin America Ethics Compliance Director

Dell

The Rise of IP Theft & Data Breaches



2

Cyber Risk Threat Landscape

Threat Actor	Objectives	Vulnerabilities	Risks / Outcomes
Nation States	Military technology, help national companies	△ Processes People Technology ▽	IP Theft Data Breaches Disrupted Business Reputational issues Lost revenues Lawsuits Fines
Malicious Insiders	Competitive advantage, financial gain, national goals		
Competitors	Competitive advantage		
Transnational Organized Crime	Financial gain		
Hacktivists	Political/social goals		

Source: CREATe.org – PwC Report: Economic Impact of Trade Secret Theft: A framework for companies to safeguard trade secrets and mitigate potential thefts, February 2014

3

The Reality Today

Intellectual Property

- **Counterfeits**
  - 7-8% total world trade is counterfeit
- **Piracy:**
  - Consumers will spend 1.5 billion hours and US$22 billion identifying, repairing, recovering from malware
  - Global enterprises will spend US$114 billion to deal with impact of a malware-induced cyber-attack
  - Users of stolen software are particularly vulnerable to malware and other cyber-security threats
- **Trade secret theft:**
  - 1-3% GDP of US and other advanced industrial economies

Data Breaches

- **On the rise:**
  - Malicious code and sustained probes have increased the most: average of 17 malicious codes/month, 12 probes/month, 10 unauthorized access incidents
- **Greatest threat:**
  - Malicious insider or criminal attack
- **Uncertainty about steps to take:**
  - 50% low/no confidence they are making the right investments in people, process and technologies to address threats

Source: 2014 Cost of Data Breach Study: Sponsored by IBM, Conducted by Ponemon Institute LLC.

CREATE.org

4

www.pwc.com

Role of the Legal and Compliance Departments

pwc

Legal & Compliance Roles

Regulating cyber security, IP theft and data breaches

Two types of regimes

- Substantive regimes:
  - E.O. 13636, "Improving Critical Infrastructure Security," calls for "Voluntary Cybersecurity Standards" for "Critical Infrastructure"
  - Market forces drive a trickle-down regulation environment
  - Standard of care
- Substantive regimes:
  - CF Disclosure Guidance: Topic No. 2
  - State breach notification laws

Looking Beyond

Working with 3rd parties, increased regulatory pressure

Some recent changes in the regulatory environment

1. Increase in congressional inquiries
2. FBI / USSS Cooperation
3. Increased calls for FTC involvement
4. PLA Indictment

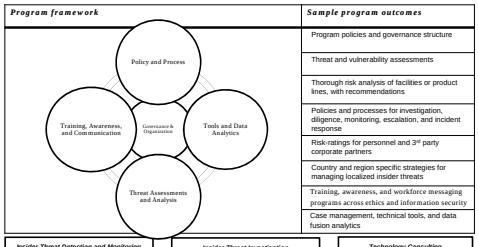
Other considerations

1. Establish line of communication in event of an attack
2. Understand obligations which result from enhanced information-sharing.

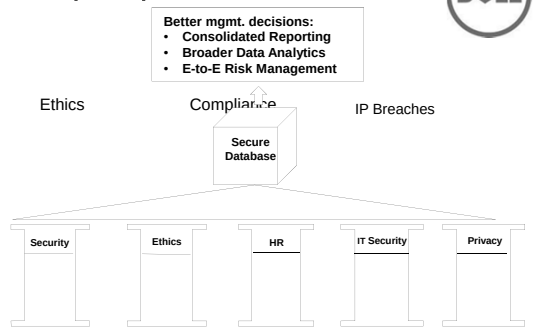
On the cyber threat landscape, insiders can potentially cause the most damage

Adversary	Motives	Targets	Impact
Nation State	• Economic, political, and/or military advantage	• Trade secrets • Sensitive business information • Emerging technologies • Critical infrastructure	• Loss of competitive advantage • Disruption to critical infrastructure
Organized Crime	• Immediate financial gain • Collect information for future financial gains	• Financial / Payment Systems • Personally Identifiable Information • Payment Card Information • Protected Health Information	• Costly regulatory inquiries and penalties • Consumer and shareholder lawsuits • Loss of consumer confidence
Hacktivists	• Influence political and /or social change • Pressure business to change their practices	• Corporate secrets • Sensitive business information • Information related to key executives, employees, customers & business partners	• Disruption of business activities • Brand and reputation • Loss of consumer confidence
Insiders	• Personal advantage, monetary gain • Professional revenge • Patriotism	• Sales, deals, market strategies • Corporate secrets, IP, R&D • Business operations • Personnel information	• Trade secret disclosure • Operational disruption • Brand and reputation • National security impact

Building a comprehensive program for insider threat management is critical to security



One-Stop Shop



10

Preventing IP Theft and Data Breaches

Legal measures			
Legislation	Laws	Contracts	Law Enforcement
Supplementing the legal approach with business processes			
Policies, Procedures & Records	IP Compliance Team	Scope & Quality of Risk Assessment	Management of Supply Chain
Training & Capacity Building	Monitoring & Measurement	Corrective Actions & Improvements	Security & Confidentiality Management

CREATE.org

11

Pamela Passman
Center for Responsible Enterprise And Trade (CREATe.org)

Glenn T. Ware, Esq.
PriceWaterhouseCoopers - PwC

Luis Canuto
Dell

12