CYBERSECURITY AND TRADE SECRET THEFT

WILLIAM D. FURNISH – OSBORN MALEDON P.A.

TAG Law Conference - Atlanta
October 24, 2018
What is a Trade Secret?
What is a Trade Secret?

Examples:

• Customer lists / information
• Employee lists
• Cost, price, billing and profit information
• Designs, methods, formulae, processes, code, algorithms
• Business plans
• Negotiations
Legal Definitions – Common Thread

EU Directive – (1) secret; (2) commercial value; and (3) subject to reasonable steps. . . . Art 2.1.

UTSA – (1) information; (2) economic value; and (3) the subject of efforts, reasonable under the circumstances to maintain its secrecy. UTSA § 1.4.

DTSA – (1) information; (2) reasonable measures to keep such information secret; (3) independent economic value. 18 U.S.C. § 1839(3).

What are these measures/steps/efforts up against?
Scope of the Threat

- Recent examples of cybersecurity breaches?
- No such thing as perfect cybersecurity
- Often a lag between breach and detection
- IP Theft is costly
  - Estimated $250 billion in US industries in 2012*
  - Estimated $300 billion in annual losses to US economy in 2013*

- Trade secrets are typically the most vulnerable type of IP cybersecurity risks, especially from insiders

Recent Trends in Threats to Clients

Business Segments Impacted by 2017 Data Breaches

- 24% of breaches affected healthcare organizations
- 15% of breaches involved accommodation and food services
- 14% were breaches of public sector entities
- 58% of victims are categorized as small businesses

Recent Trends in Threats to Clients

2017 trends:

• Increase in mobile malware
• Decrease in number of ransomware
• Increase in coin mining
• Increase in software supply chain (i.e., updates) attacks
• Increase in attacks on IoT devices

Recent Trends in Threats to Clients

Recent Trends in Threats to Clients

Threat Sources

- **State-sponsored entities**
  - *United States v. Dong* (alleged PRC)
  - *United States v. Xu* (alleged PRC)
  - *United States v. Park* (alleged DPRK)
  - *United States v. Morenets* (alleged RF)

- **Competitors / Former Employees**
  - Uber / Waymo
  - HP / IBM
  - Lutonix / Urotronic

- **Organized crime – “Carder.su”**
Threat Sources

• Current employees
  • *United States v. Xu (alleged PRC)*
  • *United States v. Snowden*
  • *Enargy Power Co. v. Wang*
  • *Charles Schawb & Co. v. Carter*

• Others with access
  • Potential business partners
  • Contractual counterparties
  • Supply chain (e.g., Super Micro Computer, Inc.)
Threat Reduction
Threat Reduction

What steps do you advise your clients to take?

What reasons do clients give for not using those precautions?

What has worked in the past?
Threat Reduction – Low cost /tech

• Don’t overshare information externally
• Restrict physical access to data / trade secret
• Employee training – have a plan
• Use in-program passwords
• Restrict cameras / recording equipment
• Update software and firmware including security patches (Mossack Fonseca)
Threat Reduction – Low cost /tech

- Employee policies and agreements
  - Robust Non-Disclosure agreements
  - Develop and implement security and confidentiality employee policies, including BYOD policy
  - Restrictions on use of personal devices

- Thorough exiting / exit interview process
Threat Reduction – Personal Devices

Personal Mobile Device Vulnerability

<table>
<thead>
<tr>
<th>Rank</th>
<th>Category</th>
<th>Percent Malware</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Lifestyle</td>
<td>27.3</td>
</tr>
<tr>
<td>2</td>
<td>Music &amp; Audio</td>
<td>19.7</td>
</tr>
<tr>
<td>3</td>
<td>Books &amp; Reference</td>
<td>9.9</td>
</tr>
<tr>
<td>4</td>
<td>Entertainment</td>
<td>6.2</td>
</tr>
<tr>
<td>5</td>
<td>Tools</td>
<td>5.5</td>
</tr>
<tr>
<td>6</td>
<td>House &amp; Home</td>
<td>4.5</td>
</tr>
<tr>
<td>7</td>
<td>Education</td>
<td>3.9</td>
</tr>
<tr>
<td>8</td>
<td>Art &amp; Design</td>
<td>3.7</td>
</tr>
<tr>
<td>9</td>
<td>Photography</td>
<td>2.7</td>
</tr>
<tr>
<td>10</td>
<td>Casual Games</td>
<td>2.2</td>
</tr>
</tbody>
</table>

Threat Reduction – Exiting Employees

Terminated / Resigning employees are a significant risk for theft

• Collect all business-owned devices (if any)
• Remove network access immediately
• Create an archive of the former employees email and data and preserve it
• Follow up with a reminder about confidentiality obligations
• Consider legal action sooner rather than later

Threat Reduction – Higher Cost

- Firewalls / Website Access Blocking / Internet Use Restrictions
- Data encryption / File locking
- Segment network data
- Data use tracking software
- Diligence on counterparties’ practices
- Separate modular products, don’t overshare
- Patent your trade secret
- Legal action

Once there has been a data breach, clients will have reporting requirements and may face fines:

- **GDPR**
- New York, California, several other states rolling out legislation
- **SEC / FTC / CFPB / Irish DPC**
  - Breach and failure to report has resulted in fines for: Equifax, TransUnion, Yahoo, Facebook, Vtech, Lenovo, Uber, D-Link, PayPal/Venmo
  - May result in fines for: Facebook, Google+
- **Private lawsuits**
Resources

- Elizabeth A. Rowe, RATs, TRAPs, and Trade Secrets, 57 B.C. L. Rev. 381 (2016).