Cyber Insecurity Meets Trade Secret Law

Scott Breedlove
Vinson & Elkins LLP
Dallas, TX

Association of Corporate Counsel – Austin Chapter
September 17, 2015
Austin, TX

“The ongoing cyber-thefts from the networks of public and private organizations, including Fortune 500 companies, represent the greatest transfer of wealth in human history.”

– General Keith B. Alexander, 2012
(then-Director of the NSA, Commander of U.S. Cyber Command, U.S. Army General)
https://www.nsa.gov/research/trw/trw194/article2.shtml
# Trends in cyber-espionage and cyber-theft

Intel Security official: These kinds of sites contain almost everything you need to get into hacking for profit. You can hire people to do the individual components of a scam, or outsource it altogether.

## In the news . . .

**DARKODE**

- taken down in July by coordinated action between law enforcement agencies in almost 20 countries
- major cybercrime “forum” – one of many forums that are the primary hub for criminal hackers

Intel Security official: These kinds of sites contain almost everything you need to get into hacking for profit. You can hire people to do the individual components of a scam, or outsource it altogether.
**BUTTERFLY**

- Discovered in early July
- Infiltrating major corporations world-wide for the last 3 years
- Targeting big business in technology, internet, commodities, and pharmaceutical sectors
- Going after high-level corporate data, not customer databases or credit card details
- For financial gain, not state-sponsored

_In the news . . ._

"[Butterfly’s] success can be attributed to one thing above all: its single-minded and professional approach to compromising, extracting, and leveraging business-confidential information and intellectual property."

"[C]yberespionage is simply part of the global competitive landscape upon which businesses are competing today"

Overview: Crimes, torts, and remedies

Economic Espionage Act of 1996 (EEA)
18 U.S.C. §§ 1831-1839

- trade secret theft for the benefit of any foreign government or for the economic benefit of another
- amendment in 2012 to expand to trade secret misappropriation related to a product or service used in or intended for use in interstate or foreign commerce
- FBI has investigative responsibility; plus U.S. Customs Service for importation of goods which use the misappropriated trade secret
- No private right of action
Computer Fraud and Abuse Act (1986)  
18 U.S.C. § 1030

- Whoever “accesses a computer without authorization or exceeds authorized access” to thereby obtain information from any protected computer, or to cause damage and loss by such conduct, violates the CFAA
- Provides private right of action

Congress “added a provision to penalize those who intentionally alter, damage, or destroy data belonging to others. This latter provision was designed to cover such activities as the distribution of malicious code and denial of service attacks.”

MALWARE
DDOS
Computer Fraud and Abuse Act (1986)
18 U.S.C. § 1030

(d)(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.

Federal Law Enforcement

Computer Crime and Intellectual Property Section (CCIPS)

Criminal Division, U.S. Department of Justice
1301 New York Avenue, N.W., Suite 600
Washington, DC 20530
Tel: 202-514-1026
Fax: 202-514-6113
http://www.cybercrime.gov
http://www.usdoj.gov

Responsible for prosecution of, and guidance, support, resources, and materials for prosecuting, domestic and international network crime offenses; development of network crime policy; and support and coordination of the federal prosecution of network crimes.
### Overview: Crimes, torts, and remedies

#### Federal Law Enforcement

<table>
<thead>
<tr>
<th>Agency</th>
<th>Division/Department</th>
<th>Address</th>
<th>Contact Information</th>
<th>Web Link</th>
</tr>
</thead>
</table>

Responsible for all network crime investigations. For a list of field offices, see [http://www.fbi.gov/contact/fo/fo.htm](http://www.fbi.gov/contact/fo/fo.htm).

<table>
<thead>
<tr>
<th>Agency</th>
<th>Division/Department</th>
<th>Address</th>
<th>Contact Information</th>
<th>Web Link</th>
</tr>
</thead>
</table>

Investigative responsibilities include computer and telecommunications fraud, financial institution fraud, false identification documents, access device fraud, electronic funds transfers, and money laundering as it relates to these violations. For a list of field offices, see [http://www.secretservice.gov/field_offices.shtml](http://www.secretservice.gov/field_offices.shtml).
Overview: Crimes, torts, and remedies

International Enforcement

International Trade Commission

ITC “Section 337” investigations are available when extraterritorial misappropriation leads to unfair competition and unfair acts in the importation of articles.

_TianRui Grp. v. ITC_, 661 F.3d 1322, 1328 (Fed. Cir. 2011): Section 337 applies “to imported goods produced through the exploitation of trade secrets in which the act of misappropriation occurs abroad.”

International: Trade secret protection regularly discussed and negotiated in Europe, Asia, etc.


“The Special 301 Report is the result of an annual review of the state of intellectual property rights (IPR) protection and enforcement in U.S. trading partners around the world, which the Office of the United States Trade Representative (USTR) conducts . . . .”
Overview: Crimes, torts, and remedies

State Crimes

**Texas Penal Code Chapter 33 – Computer Crimes**

“A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.”

**California Penal Code Section 502**

“It is the intent of the Legislature in enacting this section to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems.”

**New York Penal Code Article 156**

(1) unauthorized use of a computer, (2) computer trespass, (3) computer tampering, (4) unlawful duplication of computer related material, and (5) criminal possession of computer related material.

---

Overview: Crimes, torts, and remedies

State law civil trade secret action

**Uniform Trade Secrets Act – Texas Style**


“misappropriation” includes “acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means”

“improper means” includes “espionage through electronic or other means”

“trade secret” means information . . . that: (A) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and (B) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.
<table>
<thead>
<tr>
<th>Regulations</th>
</tr>
</thead>
<tbody>
<tr>
<td>• HIPAA/HITECH (personal health information)</td>
</tr>
<tr>
<td>• Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley)</td>
</tr>
<tr>
<td>• 2002 Homeland Security Act, including the Federal Information Security Management Act (FISMA) (federal agencies)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Regulations</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Section 5(a) of the FTC Act for unfair or deceptive acts</td>
</tr>
<tr>
<td>✓ Misleading representations regarding data security</td>
</tr>
<tr>
<td>✓ Lax data security is “unfair”</td>
</tr>
<tr>
<td>✓ No specific standards – “particularly well-suited to case-by-case development”</td>
</tr>
</tbody>
</table>
### Regulations

- **Federal Communications Act**
  - Prohibits practices that are “unjust and unreasonable”
  - Restricts telecom firms’ use of “customer proprietary network information”

### Overview

- **State data security statutes**
- **State notice statutes**
### CybersecurityRegs, Standards, Guidelines

**Overview**

#### Standards and Guidelines

- **NIST Framework** for Improving Critical Infrastructure Cybersecurity
- Energy Sector Cybersecurity Framework
  - **Implementation Guidance**
  - Department of Energy, Jan. 2015
  - specifically for the energy sector to implement the NIST Framework

---

### CybersecurityRegs, Standards, Guidelines

**Overview**

#### Standards and Guidelines

- **ISO/IEC 27001:2013** information security management system standard – International Organization for Standardization and the International Electrotechnical Commission
- **IASME** UK-based certification standard for small-to-medium enterprises
- **NERC 1300**, version CIP-002-3 – CIP-009-3 Critical Infrastructure Protection to secure bulk electric systems – North American Electric Reliability Corporation
- **ISA/IEC-62443** procedures for implementing electronically secure industrial automation and control systems – International Society for Automation
I. Trends in cyber-espionage and cyber-theft
II. Overview: Related crimes, torts, and remedies
III. Overview: Cybersecurity regs, standards, guidelines
IV. Case studies: “Secrecy” in the UTSA
V. Implications for electronically accessible IP
VI. Other case studies: Plaintiffs’ allegations
VII. Practical suggestions to prepare, defend, and counter
### Case Study: “Secrets” of the Uniform Trade Secrets Act

#### Reasonable Efforts

“Trade secret” means information . . . that:

(A) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and

(B) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.


#### Efforts to look for:

- Password procedures
- Encryption, firewalls, and other security software
- Network monitoring and other detection practices
- Segregated data / segmented networks
- Policies on remote access and personal devices
- Employee agreements and training
- “Need to know” access restrictions
- Use of NDAs with third parties

- Dumm mistaeks, a.k.a. gross negligence
Case Study: “Secrets” of the Uniform Trade Secrets Act


 Plaintiff insurance company . . .

✓ maintains its customer information on a secure computer system at its home office
✓ grants access to employees on a need-to-know basis
✓ agent agreements contain a provision designating the information as “trade secrets”
✓ requires the agent to return such information upon termination of the agreement
✓ enforces this provision with litigation

“This is enough for a reasonable juror to conclude that American National takes reasonable efforts to maintain secrecy.”


 Plaintiff loan company . . .

✓ allowed employee loan originators computer access only to their own customers’ information
✓ user identification and password required for data
✓ maintained computer security: encryption, servers in locked room, password restricted generally
✓ remote access by employees required company to set up their home computers
✓ company periodically tracked remote access (by reviewing logs to determine type of access granted)
Case Study: “Secrets” of the Uniform Trade Secrets Act


Plaintiff loan company . . .

- cont’d

✓ had policy not to permit sharing of the customer information with third parties
✓ employee handbook set forth confidentiality policy and was reviewed with all employees annually
✓ required customer information to be stored only in the protected database

“. . . makes out a prima facie case for a violation of CUTSA.”

Case Study: “Secrets” of the Uniform Trade Secrets Act

UTSA Case 3: Farmers Ins., 2013 U.S. Dist. LEXIS 104606 (EDCal 2013)

Plaintiff insurance company . . .

✓ maintained customer information on a password and user-ID protected system
✓ required NDAs from each employee or agent
✓ issued policies regarding access to the information
✓ requires agents to acknowledge confidential nature when accessing computer system
✓ periodically reminds agents via bulletins

“These allegations are adequate . . . .”
### Case Study: “Secrets” of the Uniform Trade Secrets Act

#### Plaintiff bank...

- required employees to use security codes to access computer system
- instructed employees on how to remove confidential information from personal iPads
- employed confidentiality agreements and educated employees
- had policies requiring employees to encrypt data before copying it onto laptops or USB storage

#### BUT Plaintiff bank...

- permitted defendant employee to use his company iPad for personal use and failed to inspect it for confidential data
- IT staff told employee he could email confidential data to his personal account and advised him to back up contact list (including confidential data) onto his own thumb drive

"These steps are reasonable as a matter of law... The failure to **totally secure** confidential information from every conceivable risk of disclosure by an employee entrusted with such information... is not the sine qua non of reasonable protective measures. Perhaps in retrospect Plaintiffs could have done more...”
Case Study: “Secrets” of the Uniform Trade Secrets Act

UTSA Case 5: The Ingle Co., 1997 U.S. App. LEXIS 423 (9th Cir. 1997)

Plaintiff TV show producer . . .

✓ limited access to confidential research files to Research Department personnel (not departing employee)
✓ distributed research files on a need-to-know basis
✓ segregated computer networks
✓ created limited access research databases

“Ingle satisfied its burden of showing that it undertook reasonable efforts to protect the secrecy of its research material . . . .”

Case Study: “Secrets” of the Uniform Trade Secrets Act

UTSA Case 6: LaPointe, 437 S.W.3d 126 (Ark. App. 2014)

Plaintiff manufacturer . . .

✓ limited access to confidential customer data to owners and immediate family members, who were employees
✓ allegedly stored customer CAD data securely behind a firewall with password protection

BUT . . .
Case Study: “Secrets” of the Uniform Trade Secrets Act

UTSA Case 6: LaPointe, 437 S.W.3d 126 (Ark. App. 2014) – cont’d

Plaintiff manufacturer also . . .

✓ disclosed some customer data to broad group of customers, with no confidentiality agreements
✓ failed to enter confidentiality agreement with shareholder-departing employee
✓ failed to include indication on CAD drawings of trade secret status

“We cannot say that the trial court clearly erred in finding that NTI’s confidential information constituted trade secrets for this closely held corporation with few employees.”

UTSA Case 7: Patriot Homes, 2007 U.S. Dist. LEXIS 70697 (N.D.Ind.)

Plaintiff homebuilder . . .

✓ limits disclosure of manufacturing information to proper state agencies
✓ maintains written computer use policies restricting use of computer records
✓ uses password and firewall protection
✓ limits access on need-to-know basis

“This Court recognizes the many retrospective and creative suggestions by [competitor] Sterling regarding possible precautions that Patriot could have taken . . . . Here, reading the facts in the light most favorable to Patriot, the measures taken by Patriot were reasonable.”
**Case Study: “Secrets” of the Uniform Trade Secrets Act**


Plaintiff software developer . . .

- did not have NDAs with technical personnel, nor formal confidentiality policies or manual
- tried to secure NDAs from technical personnel but was rejected → “put it on notice that its intellectual property was vulnerable”

“In light of this situation, plaintiff’s failure to institute further measures to secure its intellectual property was not reasonable under the circumstances.”

**Case Study: “Secrets” of the Uniform Trade Secrets Act**

**UTSA Case 9: Columbus, 2011 Ohio App. LEXIS 5655 (Ohio Ct. App. 2011)**

Plaintiff bookkeeping company . . .

- kept client lists on computers with password protection
- “employees freely shouted passwords” in the office or kept them on their computers or desks
- computers were routinely left on at night, eliminating need for password (e.g., by janitor)

“Even within the office, secrecy was not maintained.”
**Case Study: “Secrets” of the Uniform Trade Secrets Act**

**UTSA Case 10: Defiance Button Machine Co., 759 F.2d 1053 (2nd Cir. 1984)**

Plaintiff manufacturer . . .

- kept confidential customer data on discs in a locked room
- sold computer assets to competitor, but failed to delete the customer data
- passwords to access the data were available in documents also sold to competitor

“Hence, even though C&C may have obtained the lists by improper means – paying [plaintiff’s former employee] to extract the information from the computer – . . . [plaintiff] had forfeited the protections of trade secret law.”


Plaintiff deposition services company . . .

- made “no real effort” to identify customer lists as confidential
- “computer security was very lax”
- “made no effort to close known security holes in their computer system”

“On this record, we find no abuse of discretion in denying a preliminary injunction with respect to plaintiffs’ trade secrets claim.”
### Implications for hacked IP

**Five Scenarios**

<table>
<thead>
<tr>
<th>Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Password = “password”</td>
</tr>
<tr>
<td>b. Ex-employee retains network access</td>
</tr>
<tr>
<td>c. Fail to patch OS security flaw known for a year</td>
</tr>
<tr>
<td>d. Over-disclose to XYZ manufacturer under NDA; fail to assess XYZ security; password = “password” 😊</td>
</tr>
<tr>
<td>e. Undetected cyber-intruder for 3 years, then payday</td>
</tr>
</tbody>
</table>

---

### Other case studies: Plaintiffs’ allegations

**Consumer Cases**

- Wyndham Hotels and Resorts
- Adobe
- Target
2008-2009 Data Breach

“The FTC alleges that, at least since April 2008, Wyndham engaged in unfair cybersecurity practices that, ‘taken together, unreasonably and unnecessarily exposed consumers’ personal data to unauthorized access and theft.’”

- No encryption of PCI
- Weak password protection
- No firewalls
- Reckless connections to computer systems of partners/affiliates
- Inadequate access restrictions for vendors
- Unreasonable detection and incident response
October 2013
Data Breach

April 2014 Consolidated Class Action Complaint

“Adobe did not develop or maintain PCI-compliant security protocols . . .”

“Adobe’s security processes and protocols also failed to meet industry standards . . .”

- Failure to detect anomalies
- Inadequate network level system controls
- Inadequate incident response
- Insufficient segmenting of data and source code
- Deficient hashing of customer passwords
- Excessively weak encryption

- Relies on NIST guidelines related to cloud computing, hashing, intrusion detection, etc.
Nov.-Dec. 2013
Data Breach

“The fundamental premise of kill chain security is that hackers must proceed through seven steps to plan and execute an attack. These steps are called the ‘kill chain.’ While the hackers must complete all of these steps to execute a successful attack, the company has to stop the hackers from completing just one of these steps to prevent completion of the attack and data loss.”

-- Aug. 2014 Consolidated Class Action Complaint

Other case studies: Plaintiffs’ allegations

Nov.-Dec. 2013
Data Breach

- Pre-breach warnings from Visa: firewall, segregation of payment processing network, encryption, data deletion policies, strong passwords
- Vendor internal requirements and oversight
- Vendor network access control (two-factor authentication)
- Firewall to protect from certain Internet connections
- Failure to act on knowledge of specific alerts
- Slow response after learning of breach
Other case studies: Plaintiffs’ allegations

Nov.-Dec. 2013 Data Breach

- No network segmentation

“According to industry experts, there should never be a route between a network for an outside contractor (such as Fazio) and the network for payment data. In Target’s case, there was and the hackers found it and exploited it.”

Preparing, Defending, and Countering

Three Perspectives

- Think like a CISO
- Think like a prosecutor/plaintiff
- Think like a defendant
Preparing, Defending, and Countering

- Oil and gas company v. software developer v. telecom company v. semiconductor manufacturer v. retailer v. professional services
- Assess, and consider NIST or another framework … Consider privilege!
- Network and trade secret segmentation/segregation
- Implement proven technical solutions – firewalls, password protection, encryption, network monitoring and anomaly detection strategies, etc.

Preparing, Defending, and Countering

- Adopt good employee practices – CISO, training, confidentiality forms, “need to know” access
- Adopt effective policies – personal device, remote access, etc.
- Avoid over-disclosing or over-reliance on NDAs
- Weigh CS in patent v. trade secret assessment
- Excel at detection
Preparing, Defending, and Countering

- Have a response plan. Hint: Outside counsel → cybersecurity consultant → law enforcement, and potentially a PR firm
- Avoid the temptation to hack back