7 Steps to Protecting Your Trade Secrets

Definitions

- Trade Secret – has economic value, it's not generally known to the public and is reasonably protected.
- Trade Secret Theft – The unlawful or clandestine targeting or acquisition of sensitive financial, trade or proprietary information or critical technology.

Why Care?

- The U.S. Patent and Trademark Office estimates the value of U.S. intellectual property at $5 trillion dollars and the loss is estimated at $250 billion each year.
- Trade Secret Theft – Potential to put your company into financial ruin or out of business.
- 64 GB thumb drive holds 4 million pages (18 wheeler semi-truck).

"7" Steps to Preventing Trade Secret Theft

1. Identify your "secret sauce".
2. Provide physical security.
3. Provide cyber security.
4. Know your insider threats.
5. Provide training.
6. Appoint a trade secret POC.
7. Have an incident response plan.

Step 1.

"Identify your secret sauce."

Step 2.

"Provide Physical Security"

1. Have a "visitor" protocol.
2. Video surveillance on sensitive security areas.
3. Employee ID badges with control access.
4. Lock restricted areas.
5. After hours security monitoring.
6. Maintain logs of facility access.

Step 2. (Cont'd)

"Provide Physical Security"

7. Keep an inventory record of all IP documents.

8. Are you disposing of sensitive information properly?

9. Brief and de-brief employees after overseas travel.

10. Mark your most sensitive documents with watermarks and tracking information.

11. Suspicious behavior reporting system.

12. Employee termination plan.

13. Restrict recording or photographic devices in areas with sensitive information.

Step 3.

"Provide Cyber Security"

1. Maintain computer event logs.
   - Dates/Times of log in/out
   - Files/Networks accessed
2. Mandate routine password changes.
3. Quarantine e-mails sent to large number of employees or company executives.
4. Provide employees with clean laptops or external devices when traveling.
5. Track and limit all data downloads from company computers.
6. Require multi-factor authentication for computer access.
7. Limited remote access to company's computer network.

Step 3. (Cont'd)

"Provide Cyber Security"

8. Limit access to unauthorized websites or social media accounts.

9. Have up-to-date anti-virus or malware software installed.

10. Have a suspicious e-mail reporting system in place.

11. Apply digital watermarks or fingerprints to electronic files.

12. Have an intrusion attempt or actual cyber attack plan.

13. Know the open doors to your computer network.

Step 4.

"Know your insider threats."

Thief, Competitor or Adversary?

- Thief – Wants your intellectual property.
- Competitor - Wants what you have in the future: market share, jobs, “brand”.
- Adversary – Wants you out of business.

Insider Threat Indicators
" Personal"

1. Disgruntled.
2. Poor performance ratings.
3. Exhibits "above the rules attitude".
4. Routinely goes to executives and by-passes supervisor.
5. Undisclosed foreign travel.
6. Excessive or unusual foreign travel.
7. Unjustified work pattern (nights, weekends).
8. Numerous security infractions.
9. Excessive use of copier, scanners or faxes.
10. Chronic expression of being under recognized at work.
11. Unexplained affluence.

Insider Threat Indicators
" Technology"

1. Increased non-business related activities on internet (web surfing, job hunting, social media).
2. Increased foreign IP traffic.
3. Increased e-mail and USB storage/transfers.
4. Repeated responder to phishing attacks.
5. Purging or wiping system prior to termination.
6. Posting sensitive information on social media.
7. Speaks out against company leadership or company on social media.
8. Conducting unexplained network or company database searches.
9. Attempting remote access after being laid off or terminated.
10. Encrypting e-mails to private or personal accounts.

Trade Secret Theft and Economic Espionage "How They Do It"

- Actively recruit an employees to steal.
- Try or do establish professional collaborations.
- Social Engineering.
- The "bump".
- The "honey pot".

Trade Secret Theft and Economic Espionage
"Other, How They Do It"

- Company Collaborations
- Joint Ventures
- Front Companies
- Burglary
- Dumpster Dive

Step 5.

"Provide Training"

1. Determine frequency of training.
2. Determine topics or material to be covered.
3. Determine delivery method.
4. In-house or outsourced.
5. Link completion to employee access?

Step 6.

"Appoint a company trade secret POC."

Someone serious about the mission.

Step 7.

"Have an incident response plan."

Have an Incident Response Plan
"Things to Consider"

1. Outline steps to be executed in the event of an intrusion or theft of IP.
2. Identify the information that has been stolen.
3. Determine how much of the network needs to be shutdown, quarantined or isolated.
4. Secure or archive all relevant security activity.
5. Document who discovered the theft or intrusion.
6. Have a reporting system.
7. Determine when the theft occurred and is it ongoing.
8. Have an employee termination procedure in place.

"Things law enforcement will ask or want."

1. Is there a physical or digital employee reporting form?
2. Do you have a written security policy?
3. What was the cost to develop the trade secret?
4. Why is it a trade secret and what makes the information unique?
5. Describe the physical and cyber security measures you had in place.
6. Who had access to the trade secret?
7. List of recently terminated, laid-off or disgruntled employees.
8. Have any civil actions been filed related to the theft?
9. Is the information publically available?
10. Have you conducted an internal audit or investigation of the incident?
11. Have you attempted to prevent the stolen information from being used through civil remedies?
12. Have you estimated the loss of the stolen IP to your company?