

A Case For Information Protection Programs

Mike Annis

HUSCH BLACKWELL

Protection Programs – why have one?

“There are only two categories of companies affected by trade secret theft. Those that know they have been compromised – and those that don’t know it yet.”

– U.S. Attorney General Eric Holder, 2013

Protection Programs – why have one?

- 65% of IT professionals do not know what files and data leave their firms.
- 57% of employees save work files to external devices every week.
- 60+% of employees (including executives) walk out with data from prior employment.
- Estimated cost of data theft to an individual company averages \$2 million per year.
- Recent verdict in Virginia - \$2 billion in damages

What Constitutes a “Trade Secret”?

Uniform Trade Secrets Act (UTSA)

- ***information***, including formula, compilation, program, pattern, method, device, process, technique;
- that derives **independent economic value** from not being generally known or readily ascertainable by proper means by others who can obtain economic value from its disclosure; and
- is the **subject of reasonable efforts** under the circumstances to maintain its secrecy.

Problems with Trade Secret Litigation

- Expensive
- Difficulty in defining the trade secret allegedly misappropriated.
- Difficulty in marshaling evidence and presenting of proofs.
- **There is always a defense**, even if your defendant is a dirty rotten thief.

Common Defenses to Trade Secret Misappropriation

- It isn't a secret
 - Reasonable steps have not been taken to protect the secret nature of the info
 - Too much/broad access within the company
 - Not kept segregated/not passcode protected
 - Information shared with non-related third parties (i.e., pricing)
 - “Got it off your website”
 - Alleged “trade secret” is not a secret within the industry – it is industry-known information (maybe disclosed in a patent)
- Independent development/reverse engineered

What is an Information Protection Program?

- A customized management program to identify, define, designate, and preserve a business' sensitive or valuable business information.
- Addresses two categories of risk:
 - Your data/information gets misused
 - You are accused on misusing others info

Information Protection Programs Protect More Than “Trade Secrets.”

Also protects:

- Confidential/Proprietary Information
- Costs/Pricing Strategies
- Research and Development
- Customer/Vendor/Supplier Information
- Employment/Workforce Information
- Database Compilations
- More...

Benefits of an Information Protection Program

- Acts as a deterrent for theft in the first instance
 - Diligence Creates Deterrence
- Establishes employee expectations and understanding
- Cost-efficient/less risky
- Provides assurance of “Reasonable Efforts to Protect Secrecy” of information

What Does an Information Protection Program Look Like?

Three Common Components:

Contracts:

NDA's

Non-Competes

Invention Rights
Assignments

Policies / Systems:

New-Employee Intake
Procedures/Exit
Interviews

Handbooks

Training / Reinforcement:

Train and Refresh

Develop a Culture of
Information Protection

© 2018 Husch Blackwell LLP

HUSCH BLACKWELL

Setting It Up

- Conduct self-analysis
 - Identify what you have & what do you need to protect
 - Categorize/classify by type
 1. Trade Secrets
 2. Proprietary/confidential information
 3. R&D
 4. Other business info
 - Helps identify what is unprotected or under protected
- Develop plan
 - Who, what, when, where
- Maintain the plan

Setting It Up - Classify Data

Create and stick to a “need-to-know” system

- Restrict employee ability to access certain data
- No need for all employees to be able to view a company’s research and development data or strategic business plans
 - Only employees with an absolute need to see such vital info should be able to do so
- Have a simple and flexible policy

Limiting Access to Data

- In practice, companies can limit access to certain info in a variety of ways:
 - Pass keys to physical premises
 - Locking file cabinets
 - Marking confidential documents
 - Creating password protected access to databases
 - Encrypt sensitive information or data transfers

Classify - Info You May Want to Protect

- **Product Information:** New hardware designs; adaptations/updates of existing products
- **Research & Development:** Long-term R&D; basic or applied research
- **Critical & Unique Business Processes:** Inventory/distribution; manufacturing processes; business model based on application of processes
- **Sensitive Business Information:** M&A prospects/plans; market research/studies; customer list/information

Front End Procedures

- Employee uptake/on boarding
 - Thoroughly vet new employees
 - Establish culture of confidentiality
 - Execute non-compete, non-disclosure, confidentiality, and invention agreements
 - Execute uptake agreements
 - Did not bring anything with them from prior employment
 - Not using anything from prior employment
 - Are not subject to non-disclosure/no compete agreements

Key - Confidentiality and Non-Disclosure Agreements

- Agreement not to “disclose” materials that may not be “trade secret”
- Includes duty not to “misappropriate”
- Know-how/proprietary information
- Define “confidentiality” broadly – UTSA
- Could prove to be your only line of protection

Employee Handbooks/Manuals

- Define “secrets” and “confidentiality”
- Duty to maintain secret nature of info
- Define e-mail, social media, data access, transmission and copying protocols/rules
- Address policy regarding use of personal technology at workplace
- Identify conflicts of interest

Example - Restrictive

CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT

THIS CONFIDENTIALITY
into this ____ 10th ____ day of
____ and ____ and ____
referred to as "The Parties."

WHEREAS The Parties seek
The Parties for purposes of discussion

WHEREAS The Parties seek
confidential.

IT IS AGREED that The Parties
from the meeting on or about ____
but not limited to, all data reports,
or otherwise reflecting information
alliances, forecasts, financial information,
analysis reports, and any customer
which The Parties will provide or
but not limited to, any written, oral,
or personnel.

IT IS FURTHER AGREED
provided solely for the purposes of
disclose or disseminate such confidential
Parties.

IT IS FURTHER AGREED
understanding that any breach of this
expressly agree that in addition to
party shall be entitled to specific
this Confidentiality and Non-Disclosure

IT IS AGREED that The Parties will maintain as confidential the information shared on from the meeting on or about _____, 2013 and continued discussed thereafter including, but not limited to, all data reports, computer tapes, notes, interpretations, and records containing or otherwise reflecting information concerning marketing plans, business plans, strategies, alliances, forecasts, financial information, supplier information, technical information, statistics, analysis reports, and any customer information which is not available to the general public and which The Parties will provide or has previously provided at any time and in any form including, but not limited to, any written, oral, or electronically transferred from The Parties' representatives or personnel.

IT IS FURTHER AGREED that The Parties will use any confidential information provided solely for the purposes of discussion of potential business relationship and will not disclose or disseminate such confidential information except upon the written consent of The Parties.

Example – Non-restrictive

AGREEMENT FOR SUBMISSION OF IDEAS

This is an agreement ("A
individuals and/or entities subm
(hereinafter collectively referred t
Missouri corporation, having a pr
The PROPOSER wishes
matters attached below relating to
"Proposal"). In consideration of
the sufficiency and receipt of whic
following terms, conditions, repre

1. The PROPOSER und
basis, and that
agrees and acknowle
whatsoever without
2. The PROPOSER und
expressed or implied
unless and until a wr
provide for use of the
connection with the
3. If the PROPOSER ha
copyright registration
with a copy

protection be at least applied for before any Proposal or submission is made.

1. The PROPOSER understands and agrees that ~~EAGLE~~ will not accept any Proposal on a confidential basis, and that ~~EAGLE~~ specifically disclaims any confidential relationship. The PROPOSER further agrees and acknowledges that ~~EAGLE~~ may freely disclose the Proposal to any individual or entity whatsoever without any obligation to maintain the secrecy or confidentiality thereof.
2. The PROPOSER understands and agrees that ~~EAGLE~~ has assumed no obligation of any kind either expressed or implied by its review of the Proposal and further that no obligation of any kind shall arise unless and until a written contract has been completed and executed by both the PROPOSER and ~~EAGLE~~. ~~EAGLE~~ has the exclusive right to decide what compensation or consideration, if any, it will provide for use of the Proposal. ~~EAGLE~~ is under no obligation to return any materials provided in connection with the Proposal.

Employee Confidentiality

EMPLOYEE CONFIDENTIALITY AND ASSIGNMENT AGREEMENT

IN CONSIDERATION of my employment and payment of compensation to me by _____ (herein "_____") and in view of the position held by me in which I will or may work with and/or have access to Confidential and/or Trade Secret Information in connection with the activities of _____, I hereby covenant and agree with _____ as follows:

I. CONFIDENTIAL AND TRADE SECRET INFORMATION

I agree to keep _____ consent of an officer of _____ exposed or which of my employee _____ Secret Information including, but not limited to manufacturing and plans.

I further agree to _____ and/or other property not limited to that

II. INVENTIONS

I agree to promptly assign and hereinafter including but not inventions and discoveries and/or conceived

I agree, when required by _____ and convey to _____ derivative works Information to _____ the world. "Inventions" no equipment, software used and which will be the actual or deemed result from any work which I perform for _____.

I hereby appoint any officer of _____ as my irrevocable attorney-in-fact, coupled with an interest, to execute on my behalf any and all such documents contemplated by this Agreement if I am unable or unwilling to execute such documents.

I. CONFIDENTIAL AND TRADE SECRET INFORMATION

I agree to keep confidential and not use for my own account or the account of any other entity without the written consent of an officer of _____, any Confidential and Trade Secret Information to which I may be exposed or which comes into my possession, or which I may develop, either solely or jointly with others, as a result of my employment by _____. For purposes of this agreement, the term "Confidential and Trade Secret Information" shall include all information of _____ which is not available to the public, including, but not limited to the following types of information: marketing, sales, customers, suppliers, manufacturing and production, machinery, technical, engineering, scientific, and business or new product or process plans.

Onboarding: Avoid Contamination

- Check that new hires do not have/are not bringing in confidential information from their former employers
 1. Removable storage devices (flash/thumb drives, etc.)
 2. Personal computers/phones
 3. Personal web-based email accounts/ cloud storage accounts (Google Drive, Drop Box)
- Engagement/offer letters or declarations/affidavits – certify:
 1. Will **not disclose or use** old employer's confidential info
 2. Are **not in possession of any non-public information** from prior employer
 3. Are **not going to provide ideas** to derived from old employer

Onboarding: Protect Your Trade Secrets

- Begin education early & establish culture of confidentiality
 - Emphasize importance of confidentiality
 - Teach what it is and how to treat confidential info
 - Give practical guidance
 - On the IT front, equip employees to protect
 - Remote workplace considerations
 - Define access rights (need-to-know basis)

During Employment

Education and training are key to successful deployment of program

- Teach and remind employees about the rules - reinforce culture
 - Periodic reminder materials sent to employees
 - ✓ Shows you have been “ever vigilant”
 - ✓ Keeps secrecy/confidentiality requirements top-of-mind
 - Provide training on a regular basis
 - Monitor usage
 - Passcode protect
 - Mark/Segregate

Back-End: Departing Employee Activities

- Conduct exit interviews
 - ✓ Where they are going, what they will be doing
 - ✓ Look for red flags
- Execution of affidavits/check-in procedures
 - ✓ did not take anything or have returned everything they had
 - ✓ Remind and seek affirmation of contractual obligations
 - ✓ Take care all company property and data has either been returned or destroyed
- Review of IT activity
 - ✓ Check for suspicious computer and premises access

IT Strategies to Minimizing Leaks

- **Segregate** data by category
- **Establish electronic protocols** that catalog access to highly sensitive data and that restrict access, transfer and copy of that data to unauthorized users
 - Only the most senior management should be given access to the most sensitive data
- **Encrypt** – regardless whether sensitive data is “in motion,” “at rest,” or at an “end point,” it should be encrypted

Problems in the Information Age

- External devices
 - Risks posed by external devices are heightened with employees working remotely
- Options to address
 - Use software that allows for a secure connection to your network
 - Monitor activities on electronic devices and limit access to critical information
 - Make sure information on external hard drives, thumb drives or employee's personal computers is well protected and can be recovered
 - Have policies in place to address if a device is lost or stolen
 - Monitor sizable downloads or emails with large attachments

Try to Limit Use of Personal Devices

- Employees should sign agreement indicating they are aware of the company's policy and that any "private" device or program used to conduct business or that is accessed from the company will be subject to inspection, copy and seizure.
- Employees should be advised that communications to and from work carry no expectation of privacy and that the company periodically monitors e-mails for compliance with its protocols.

Not All Business Is Cloud Business

- Must take reasonable steps to protect
 - Q: What is “Reasonable?”
 - A: Look at nature of info and circumstances in which data is stored and used.
 - More important the data, the more security measures must be taken to protect
- **Highly sensitive data should not be stored with a third party.**