EMPLOYER CYBERSECURITY:

PROTECT YOUR COMPANY'S DATA AND TRADE SECRETS

WHAT I'M NOT COVERING

- ***External Threats.***
    - Phishing.
    - Malware / Spyware.
    - Ransomware.
    - Social engineering.
- ***My focus today.***
    - Internal fraud, theft, and destruction – employees and management.
    - Issue spotting.
    - Spot checking.
    - Resources.

WHICH HANDBOOK POLICIES MUST I IMPLEMENT NOW, BEFORE A DATA BREACH OCCURS?

Our current environment.

- Employee mobility.
- Electronic media and data.
- Information sharing.

- Business collaborations.
- 25% of data loss incidents in 2013 happened, not because of hacking, but because of human error.
- Another 14% were caused because of theft or loss of devices.

Association of Certified Fraud Examiners - 2015 Study on Occupational Fraud.

- $6.3 billion in losses over 2,410 fraud cases in 2015.
- 30% of fraud cases occur in small businesses.
- Over half of small businesses never recover losses caused by occupational fraud.

COMMUNICATION - Make clear in policies what constitutes "Employer Property"

- Baseline – sometimes it's truly unclear to an employee WHO owns an invention or emails. So you should spell it out in your policies and employee agreements.
- Sample provision.
    - All files, records, proposals, specifications, or other documents, and all electronically stored information, computer software, software applications, **EMAILS**, files, data bases, and the like relating to the business of the employer or which contain Proprietary Information, **whether prepared by me or otherwise coming into my possession**, shall remain the exclusive property of the employer. Upon the termination of my employment, for any reason, I will promptly deliver to the employer all such material in my possession, custody, or control.

- **THEFT VS DESTRUCTION of electronic data.**
    - It's property, but not like your typical property – employees can duplicate with relative ease, and without drawing attention.
    - But still damaging in multiple ways; interruptions, disclosure to competitors, use for own purposes and in competition.
    - If destroyed…
        - Business continuity problems.
        - Client/customer materials gone.
        - Violates record retention policies and requirements imposed by governmental entities.
    - If taken. . .
        - Strictly prohibit employee duplication or "backups."
        - Policies should spell out that the taking of electronic data, including emails, constitutes theft, and will be treated as theft.
        - Require return of all data upon termination of employment.

CONFIDENTIALITY/NON-DISCLOSURE AGREEMENT

- STATE SPECIFIC REQUIREMENTS.
- Non-Disclosure clauses
    - Applies to what? Proprietary information - broadly define for maximum protection.
    - Sunset provisions on non-disclosures – make **indefinite**.

- **Non-Solicitation Agreements.**
    - Customers.
    - Clients.
    - Vendors.
    - Employees.
    - Existing and Prospective.

WHAT ARE BEST TECHNOLOGY PRACTICES TO PREVENT AND ADDRESS DATA THEFT AND DESTRUCTION?

I. ***Prevention***

- Talk to your IT department, and consider consulting with an IT security expert and digital forensics firm ***before*** something goes sideways.
    - They can do a vulnerability test.
- **ISO 27001 Information Security Policy.**
    - The main purpose of the policy is that the top management defines what it wants to achieve with information security.
    - The second purpose is to create a document that the executives will find easy to understand, and with which they will be able to control everything that is happening within the ISMS – they don't need to know the details of, say, risk assessment, but they do need to know who is responsible for the ISMS, and what to expect from it.
- End-to-end encryption of data.
- Keep software up to date with all recent patches.

- Ensure access to data is only given to those who need it to perform their job responsibilities.

- **Ethics and Security Hotline or dedicated email account.**

    - Most fraud tips come from company hotlines; 50% of tips come from employees/co-workers.

    - Report suspicious employee activity.

    - Confidential.

    - Create a policy, but also foster a culture encouraging use.

    - For data and proprietary information violations, make sure the report is immediately routed to the pertinent person, e.g., a Security Director, IT Manager, Chief Security Officer.

- **Annual audits and certifications.**

    - Management oversight.

    - I certify that the Division has a Crisis Management and Business Continuity Plan and an annual test was conducted . . .

- **Employee off boarding.**

    - Revoke access: passwords, remote logins; email accounts, etc.

    - Replicate computer, laptop, and email account – then inspect. Give counter-example where client replicated but failed to inspect until two years later – and discovered employee suspiciously deleted emails over particular timeframes.

- Who is responsible for doing this? Coordinate IT and HR.

- **Business Continuity Plan (BCP) incorporating data breach policies.**

    - The BCP is a comprehensive document designed to ensure the business unit can continue operations in the event of significant business interruptions.

    - Do you have protocol for a serious data breach?

    - Complements and syncs with your Data Breach Response Plan?

II. ***Mitigation.***

- **Routine Backups, including email.**

- **Data Breach Response Plan.**

    - Breach notification to customers and governmental entities.

    - Companies that can swiftly conduct IT and computer forensics to figure out what happened.

    - How quickly does your DBRP allow you to return.

    - Data backup / system redundancy.

- **Cybersecurity Insurance for data breaches:**

    - What does it cover?

        - Intellectual Property insurance.

        - network security and privacy liability.

        - plaintiff lawsuits.

        - computer forensics investigations.
        - breach notification mailings.
        - regulatory defense, penalties and fines.
        - attorney fees.

- **General liability policy is no longer enough.**
    - It covers third-party claims of bodily injury or property damage, but the trend among insurance providers is to exclude electronic records and data.
- **Cookie-cutter policies do NOT work.**
- **Different industries have different kinds of risks –**
    - financial services.
    - health care.
    - retail.
- **What does it cost?**
    - Depends on size and industry, but many annual premiums range from $6,000 to $37,000.
    - KNOW WHAT YOU'RE BUYING.
    - Shop for a policy based on the limits, exclusions, and conditions, and less so on cost.

- **Exclusions.**
    - If a data breach happens, coverage will be denied for companies that failed to use their best efforts to install software updates or releases.
    - Disclosure of personally identifiable, confidential corporate, or personal health information due to $$$$$$$$$.
    - Claims brought by the government or regulators, including the Office of Civil Rights, the Department of Health and Human Services, and the Office of the Attorney General.
    - Negligent computer security and policies.
- Which brings us full circle: <u>have the right IT and employment policies</u>.

Cybersecurity insurance takeaways.

- Insurance is smart if you're smart about picking your policy.
- But it cannot repair your reputation.
- And no matter how good the coverage the loss IP and data, and related business interruptions, can be game-enders.
- Cyber insurance policy premiums are "not one size fits all", as premiums are factored on a company's industry, services, type of sensitive data stored/collected/processed, total number of PII/PHI records, data risks and exposures, computer and network security, privacy policies and procedures and annual gross revenue, and more.

HOW DO I WIELD THE NEW DEFEND TRADE SECRETS ACT TO PROTECT MY COMPANY?

- ***Why?***
    - Before passing the DTSA, much of the discussion in Congress centered on protecting U.S. businesses from trade secret misappropriation abroad.
    - Senate Judiciary Committee's Report - American losses due to trade secret theft exceed $300 billion and 2.1 million jobs annually. S. Rep. 114-220 (2016).
    - The report concludes with the observation that "[a]s trade secret owners increasingly face threats from both at home and abroad, the [DSTA] equips them with the tools they need to effectively protect their intellectual property and ensures continued growth and innovation in the American economy." Id.
- ***What?***

    Protects TRADE SECRETS – as title might suggest—from MISAPPRO-PRIATION.

    What is a trade secret?

    1. Secrecy (not generally known or readily ascertainable)
    2. Derives independent economic value from not being generally known or readily ascertainable by others.
    3. Subject to reasonable efforts to maintain secrecy.

What is misappropriation?

1. Wrongful *acquisition.*

2. Wrongful *disclosure.*

3. Wrongful *use.*

So What?

- Actual Damages PLUS taking whatever money the employee (or competitor) made from the trade secret.
- Multiply the above by two, in essence DOUBLE damages as a penalty ("exemplary damages").
- ATTORNEY FEE'S & The American Rule.
- Before, no federal civil cause of action available to private litigants for trade secrets misappropriation.
- Unless diversity jurisdiction, or some other federal issue, like a patent lawsuit, there was no way to get into federal courts for trade secret misappropriation.
- You get access to federal courts and judges – speak to in-house; some people prefer, and it's always nice to have options.

What you need to do to ensure DTSA is available to you

- DTSA Whistleblower Immunity.
- Immunity from liability and prosecution for trade secret misappropriation under specified conditions.
- Ability of employee to disclose trade secrets in retaliation action under specified conditions.

- NOTICE REQUIREMENT and consequences.

- Employers must provide employees notice of the new immunity provision in “any contract or agreement with an employee that governs the use of a trade secret or other confidential information.”

- Notice requirement met if employer provides a “cross-reference” to a policy given to the relevant employees that lays out the reporting policy for suspected violations of law.

- IF NO NOTICE, EMPLOYER MAY NOT RECOVER EXEMPLARY DAMAGES OR ATTORNEY FEES IN AN ACTION AGAINST AN EMPLOYEE TO WHOM NO NOTICE WAS EVER PROVIDED.

- Definition of employee includes contractor and consultants.

- SAMPLE PROVISION for your handbook or non-disclosure/confidentiality agreement:

> The Defend Trade Secrets Act of 2016 (“DTSA”) provides that an individual shall not be held criminally or civilly liable under any federal or state trade secret law for the disclosure of a trade secret that is made (i) in confidence to a federal, state, or local government official, either directly or indirectly, or to an attorney, and solely for the purpose of reporting or investigating a suspected violation of law; or (ii) in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal. In addition, the DTSA provides that an individual who files a lawsuit for retaliation by an employer for reporting a suspected violation of law may disclose the trade secret to the attorney of the individual and use the trade secret information in the court proceeding, if the individual (i) files any document containing the trade secret under

seal; and (ii) does not disclose the trade secret, except pursuant to court order.

Computer Fraud and Abuse Act.

- Federal cause of action that sometimes applies where the DTSA does not, e.g., when an employee destroys work emails that do not rise to level of Trade Secret.

- Example of successfully using the CFAA: in International Airport Centers, L.L.C. v. Citrin (2006), defendant Citrin deleted files from his company computer before he quit, in order to conceal alleged bad behavior while he was an employee. Court authorized employer to proceed against Citrin on CFAA theory.

Recap Table

Item	Do I have?
Data Breach Response Plan?	
Business Continuity Plan?	
Data Breach Insurance?	
Automated Backups?	
Offboarding procedures that include replication and review of electronic devices?	
DTSA Whistleblower Immunity clause to ensure you can recover double damages and attorney fees?	
Confidentiality/non-disclosure agreement?	
Non-solicit agreement?	
Handbook clearly define what is “employer property” – including data and emails?	