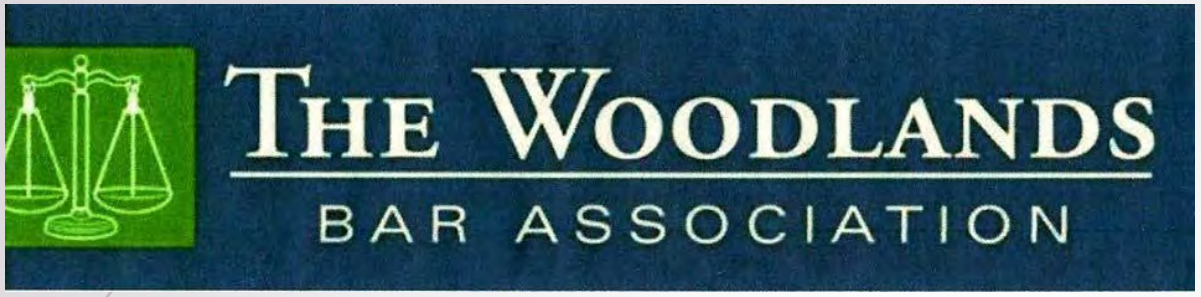
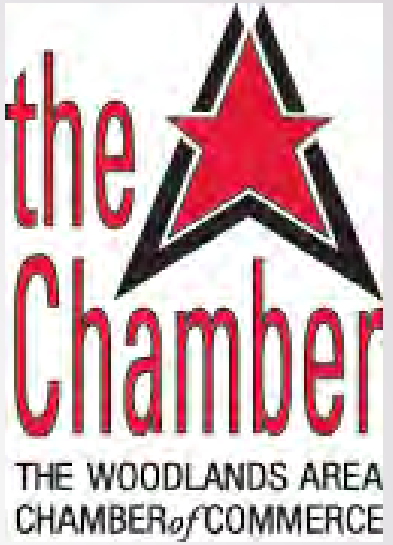



# Trade Secrets in a World of Devices

## Risks and Rewards of Bring Your Own Device ("BYOD")

Fall 2017 – Presented by Bret L. Strong

Presentation will be available on our website at
https://www.thestrongfirm.com/woodlands-media-and-events/2017-media-events/

# My Background

- **Approaching 30 year resident of The Woodlands**
- **20+ years of legal practice in The Woodlands**
  - Commercial Real Estate
  - Oil and Gas
  - General Corporate
- **Community Involvement including:**
  - Woodlands Bar Association Founding Board Member (2006-2008)
  - Chamber of Commerce (1998-present)
    - Chairman of the Board (2008-2009)
  - YMCA – Board Member (1996-2011)
    - Chairman of the Board (2002-2004)
  - United Way Board Member (2007-2010)
  - CISD Facilities Planning Committee (2003 and 2007)
  - Leadership Mo. Co. – Class of 2005 and Board (2014-2016)
  - Interfaith "Hometown Hero" (2014)
  - Sponsoring Partner and Representative on C.R.E.A.M. Board

- **Legal Representation of:**
  - The Woodlands Convention and Visitors Bureau
  - The Woodlands Township
  - Local/Regional Commercial Real Estate Developers
  - Local Small Businesses (retail, restaurant, service & manufacturing)
  - Local/Regional/National/International Oil and Gas Clients
  - Local Restaurants
  - Local Medical Professionals

# Bring Your Own Device (BYOD)

- Benefits of BYOD
- Risks of BYOD
- Insurance Implications
- Importance of Workplace Policies
- Legal Challenges

# Benefits of BYOD

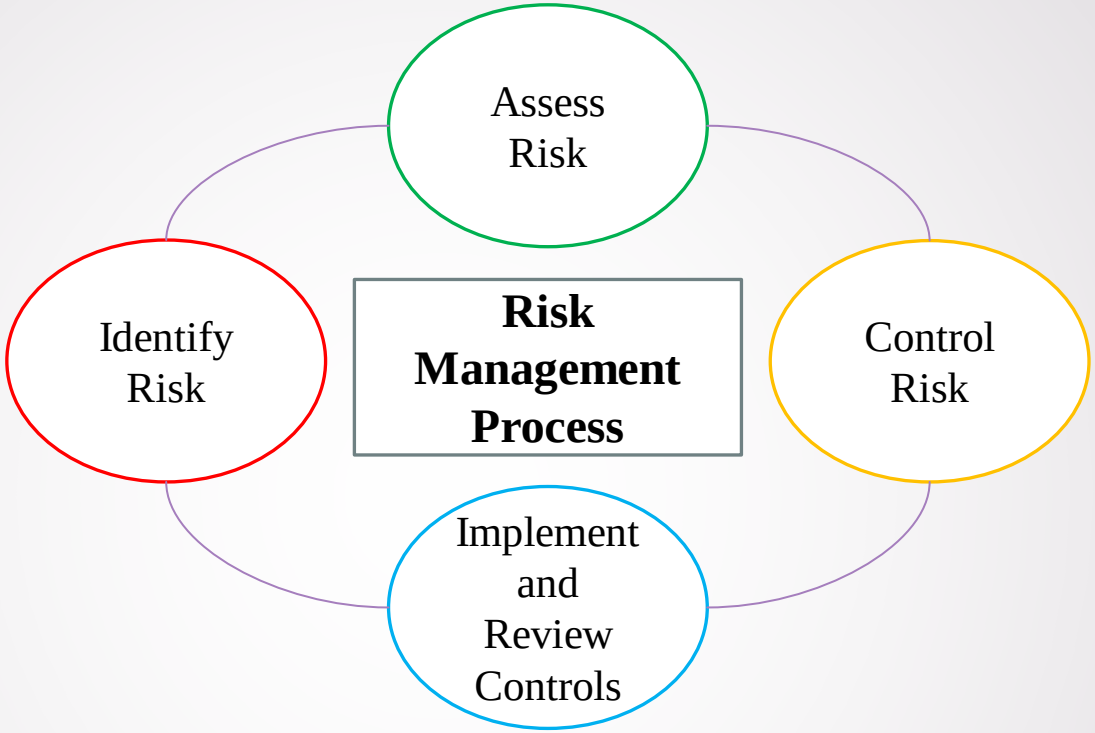
- Avoid Duplicate Device and Software Costs
- Employee Convenience and Job Satisfaction
  - Work/Life Balance Enhanced
  - Employee has Freedom to Update Hardware As Needed
  - Flexibility for Employee as Technology and Preferences Change
  - Employees Trust Their Own Device
- Increased Productivity
  - Employees are more efficient using a device with which they are comfortable
  - Technology stays up to date as employees keep up with trends

# Risks of BYOD

- Compromised Security and IT Control
  - Lack of Proper Passwords
  - Less Control of Hardware and Software on Device
  - Lack of Firewall and/or Anti-Virus Protections
  - Handling of Lost or Stolen Devices
  - Accessing Internet With Devices Via Unsecured Wi-Fi
- Handling Abrupt Dismissal From The Company
  - Theft of Trade Secrets
  - Inability to Retrieve Data
  - Risks of Deleting Valuable and/or Personal Data of Employee
- Employee Privacy
  - Potential Company Access to Personal Digital Images and Data
  - Legal Issues When Searching Devices
- Federal Fair Labor Standards Act
  - Exempt and Non-Exempt Employees
- Effective Handling of Expense Reimbursement
- Criminal Investigations
- Lower Productivity Due to Multiple Devices and/or Technology


*"See? I told you it was possible to mix business with pleasure."*

# Insurance and Risk Management Implications




- Cyber Liability Insurance
- Mobile Device Management Technology

# Workplace Policies

- Certain Industries Face Particular Challenges in Maintaining Compliance
  - Electronic Communications Privacy Act
  - Other Privacy Protection Acts
  - HIPPAA
  - Dodd-Frank
  - Open Records/Open Meetings
- Satisfying Electronic Discovery Request Guidelines
- Possible Risks Due to Confidential Data on Any Device
  - Failure to Properly Secure
  - Phishing/Ransomware
  - Accidental Sharing of Confidential Information
  - Inappropriate Access to Private Data
- Use of “Rogue” Devices
- Policies Regarding Personal Use While Working
- Determine Who is Eligible (Exempt vs Non-Exempt)
- Use of Enterprise Mobility Management (“EMM”) Technology
- Use of Authentication Software

# Struggles in a Digital World

# Legal Challenges

- Complexity of Searching Personal Devices
  - Legal Ramifications of "Discoverable" Information
  - Action Following Discovery, i.e. Release from Employment
  - Discovery of Illegal/Criminal Activity
  - Expectation of Privacy?
- Liability When "Wiping" the Device
  - Accidental deletion of personal information
- "Bring Your Own Device Policy" **MUST** be clear, clearly communicated and properly implemented

# The "Rajaee" Risk

- *Rajaee v. Design Tech Homes, Ltd.*, S.D. Texas, No. H-13-2517 (2014)
  - Company remote wiped Rajaee's phone upon his termination deleting photos, business contacts, etc., including significant personal data.
  - Rajaee sued under various federal and state laws related to management of data and access to it.
  - Federal Court ruled against Rajaee, but several lessons learned:
    - You MUST have a policy that employees agree to if you expect employees to use their own device to access and store company information which is subject to being "wiped".
    - There is software available to segregate company and personal data and if a reasonable person would use it, you should!
- *AND THE REAL STORY…….Rajaee v. Design Tech Homes, Ltd.*,281st District Court, Harris County:
  - Confidential Settlement and Dismissed


The
Strong Firm
Attorneys
P.C.


· SINCE 1996 ·
EMPLOYMENT LAW UPDATE
THE WOODLANDS AREA CHAMBER OF COMMERCE
IN PARTNERSHIP WITH
THE WOODLANDS BAR ASSOCIATION