Jaffe
JAFFE RAITT HEUER & WEISS

# Data Privacy & Cybersecurity

## Cybercrime is big business. Is your data protected?

October 29, 2020

# Today’s presenters

**Jon Sriro, Partner**
Presenter
Data Privacy & Cybersecurity

**Shaunté Wilcher, Attorney**
Moderator
Data Privacy & Cybersecurity

Jaffe
JAFFE RAITT HEUER & WEISS

# Agenda

- Latest threats and trends
- Examples and implications of a data breach
- Learning to identify a potential threat
- Best practices to help avert an attack  (contracting, training)
- The first steps when a data breach occurs
- Questions and answers

# Cybersecurity goal

- Staying ahead of threats vs. managing them later
- Old adage in information security: “Every company gets penetration tested, whether or not they pay someone for the pleasure.”

# Goal of Data Security

- Maintain:
  - **C**onfidentiality
  - **I**ntegrity
  - **A**vailability

# Latest threats and trends

- Cyber Threat Trends Arising In The Increasingly Inter-Connected COVID-19 World:
  - **DISRUPTION** results when a hacker takes advantage of a company’s reliance on connectivity.
  - **DISTORTION** occurs when the integrity of data is lost due to misinformation being circulated or data changed.
  - **DETERIORATION** happens when controls are eroded by regulations and technology.

# Examples and implications of a data breach

- Common Attack Vectors:
  - Phishing/Vishing/Social engineering attacks
  - Cloud service attacks
  - Ransomware
  - Insider threats
  - Man-in-the-Middle Attacks
  - Compromised Credentials

# Examples and implications of a data breach

- Legal Implications?
  - Personal Information
    - Employee
    - Customer
    - Service Provider
    - Visitor
  - Proprietary Information
  - Entrusted Confidential Information

# Examples and implications of a data breach

- Effect of Disclosure of Information
  - Statutory obligations for notification.
  - Contractual liabilities.
  - Statutory liabilities.

# Identify a potential or existing threat

- Slow network
- Ransomware message
- Fake warning messages and Unwanted Pop Ups
- Unwanted browser toolbars
- Internet searches are redirected
- Password is not working
- Steady stream of error messages between network devices
- Webcam flickers on briefly

# Identify a potential or existing threat

- Unexpected software installs
- Mouse moves between programs and makes selections
- Task Manager or Registry Editor is disabled
- Online accounts are missing money
- Strange network traffic patterns
- Email attachments from people claiming to be someone they are not
- Strange large files appear on the network

# Best practices to help avert an attack

- Reviewing Your Data security Safeguards
  - Important Data Security Safeguards
    - Physical Safeguards
    - Administrative Safeguards
    - Technical Safeguards
  - Internal Security
  - Service Providers

# Best practices to help avert an attack

- Why do we care about our vendor’s data security program?
  - Your data security is only as strong as the data security of your weakest vendor processing your data.
  - You are responsible for your vendor’s data security failures just as if you committed the failure.

# Best practices to help avert an attack

- Important Contract Considerations and Terms
  - The considerations for these terms change depending on whether you are the vendor or vendee.
  - Data Breach Notification and Response
  - Disaster Recovery Plan
  - Vendor’s data security program
  - Vendor’s service providers data security program
  - Audits and third-party testing
  - Technical security audit rights of the vendee
  - Confidentiality and Data Security integration
  - Limitation of Liability
  - Limitations on usage of data
  - Compliance with data security and privacy laws

# Before and after a data breach occurs

- Before the breach
  - Develop an incident response plan so you know what to do in advance
  - Backup Data
  - Work with IT professionals to shore up vulnerabilities
- After the breach
  - Implement the incident response plan
  - Contact counsel
  - Contact insurance company
  - Contact PR firm
  - Retain forensic specialists

# Before and after a data breach occurs

- Blackbaud Case Study
  - What happened?
  - Why should it cause you to look at your service provider contracts?

# Thank you for attending

Jon is a co-chair of our Data Privacy & Cybersecurity practice group. He is a Certified Information Privacy Professional/United States (CIPP/US) with the International Association of Privacy Professionals (IAPP). Jon has extensive experience counseling clients on a wide range of privacy, cybersecurity, and information management issues in the context of vendor/vendee agreements, mergers and acquisitions, compliance, business strategy, technology transactions, and litigation, incident response preparation, insurance, data breach/incident, and regulatory compliance issues.
jsriro@jaffelaw.com
313.800.6502

Shaunté is an attorney in our Data Privacy & Cybersecurity practice group. She counsels clients who have experienced a data breach/incident and have compliance issues. Shaunté has particular experience counseling on HIPAA and the California Consumer Privacy Act compliance.
swilcher@jaffelaw.com
248.727.1637

Jaffe
JAFFE RAITT HEUER & WEISS