Cybersecurity Summit:

Protecting Your Business

April 28, 2016

BUTZEL LONG

Claudia Rast | Butzel Long | Ann Arbor, MI | rast@butzel.com

Managing Cyber Liability

PRIVACY vs. SECURITY, LIABILITY & BEST PRACTICES

“Data Privacy” and “Data Security”

- ***Data Privacy***: the relationship between the collection, storage, use, dissemination and security of information identifiable or defined as private, the varying public expectations (or not) of privacy, and the attendant legal and political tensions
- ***Data Security***: the protection of data from any unauthorized access in violation of policy, law, regulation or rule

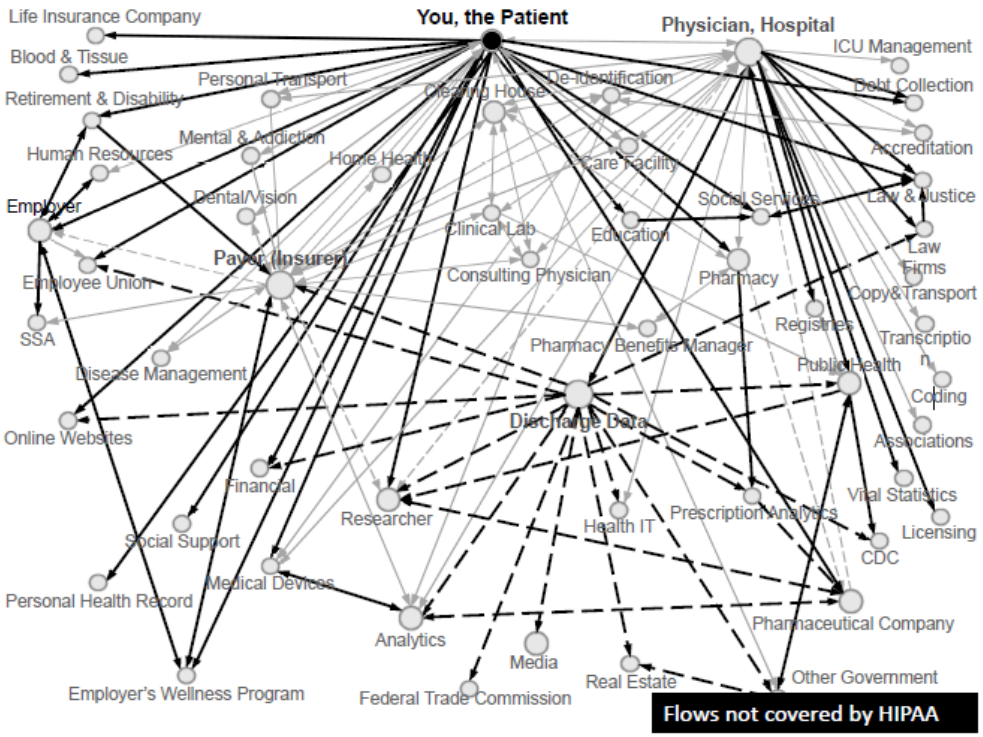
Current International Activities

- EU Court of Justice Struck Down Safe Harbor Framework on October 6, 2015
- Now the “Privacy Shield”
  - June 2016 targeted for adoption by EU Member States
- EU General Data Protection Regulations
  - Could require explicit consent for each “use” of data
  - Should be adopted in July 2016 with two-year “adjustment period” before enforcement begins
  - Applies to all companies providing services on the EU Market

Current Federal Activities

- Cybersecurity Information Sharing Act of 2015
  - President Obama signed December 18, 2015
- Requires DNI, DHS, DOD, and DOJ to develop and promulgate procedures to promote:
  - the timely sharing of classified and declassified cyber threat indicators in possession of the federal gov't with private entities, non-federal gov't agencies, or state, tribal, or local governments;
  - the sharing of unclassified indicators with the public;
  - the sharing of cybersecurity threats with entities to prevent or mitigate adverse effects
- Permits private entities to detect, prevent, or mitigate
  - Broadens private company activity formerly restrained by Electronic Communications Privacy Act of 1986
- Certain antitrust exemption for "cybersecurity purposes"
- DOJ to review privacy and civil liberties guidelines
- Provides liability protection if acting "in accordance with Act"

Executing a Data Flow: A Health Care Example



The FTC charted data flow and the applicability of the law in the transactions, which underscored the importance of knowing where the data is going in any transaction, system or platform.

Health Data Flows, Latanya Sweeney, Chief Technologist, FTC (May 7, 2014)

BUTZEL LONG

Understanding Data Flow Issues in Products

- What types of data exist?
  - Geo-location
  - Vehicle behavioral data
  - Event Data Recorder (“EDR”)
- How is it generated?
  - Automatically (EDR)
  - Opt In (Apple Play)
- Where is it kept?
  - Locally (the vehicle)
  - The “Cloud”
  - Data Centers (foreign and domestic)

When Negotiating…

- Security/Privacy Representations
- What type of Data
- Compliance with Laws (US, EU?)
  - Privacy Shield/Data Privacy
- Indemnification
- Insurance (Cyber Liability Coverage)
- Server Locations
  - In state? Out of state? Out of the country?
- Security protocols for breach notification

LIABILITIES

Sources, Targets & Risks: It's Us!

Source

- Mobile Computing *(controlling BYOD)*
- Social Media *(online & customer service)*
- 27% Employees would sell passwords
  - 2016 SailPoint Market Pulse Survey

Target

- Critical Infrastructures *(electric, oil, gas, water, traffic, ports, chemical)*
- Trust Infrastructures *(finance, insurance, accounting, legal)*
- The Cloud *(who owns, who controls, where located)*

Risks

- Communication Breach: Data Center → ≠ Board Room
- Target Breach: Auto Breach Detection turned "Off" by IT

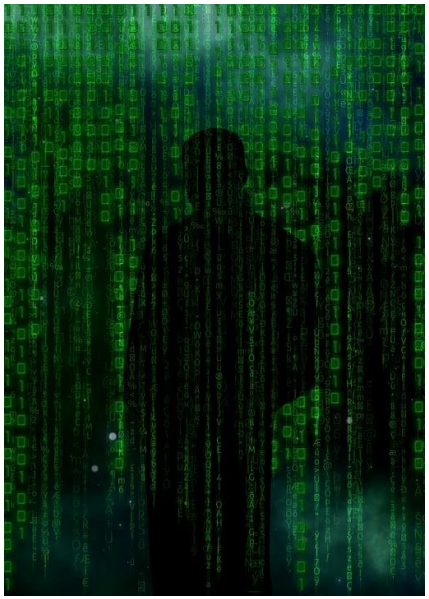
CERT Insider Threat Profile

- More than 30% of Insider Saboteurs had prior arrest history (2011 study showed 30% of U.S. adults arrested by age 23)
- Behavior Issues:
  - bragging about the damage they could do if they wanted (trigger: passed over for promotion)
  - Using Company resources for side business or talking about competing business
  - Coercing coworkers to get credentials
- ***More than 70% IP theft occurs within 30 days of employees announcing departure***
- More than 50% Insider Saboteurs were former employee with access via "backdoors" or credentials that were never disabled

from Carnegie Mellon's Common Sense Guide to Mitigation Insider Threats, 4th Ed. Dec. 2012

More on Insider Threats

- Typically Three Main Categories
  - Sabotage (24%)
  - Fraud (44%)
  - Theft of IP (16%)
- Most Often An Employee of Target Entity (85%)
- Most Activity Occurred During Work (72%) and at Work Site (70%)



from Carnegie Mellon's Insider Threat Blog, Oct. 17, 2013

From the Headlines

- April 18, 2016: IT engineer for Dallas law firm Locke Lord
  - Sentenced to 9 yrs
  - Ordered to pay nearly $1.7 million in restitution for a destructive computer attack on former firm
  - Accessed firm network and issued commands that resulted in “significant damage” to the network

Liabilities

- Defining the Breach/Security Incident:
  - Is it a Breach?
- Liability for Breach/Security Incident :
  - What Laws?
- Corporate Boards at Risk
- Management at Risk
- Cyber Risks for Law & Accounting Firms
  - E.g., Mossack Fonseca

Is it a Breach?

- What was Disclosed, Published, Stolen, Accessed without Authority, Not Properly Secured…
  - Personally Identifiable Information
    - Name, address, telephone #
    - SS#
    - Credit Card information
    - Financial account information
  - ePHI (personal health information)
- Was it Encrypted?
- Reasonable Belief that Breach has not or will not result in ID Theft or other Fraud?

Liability for Breach—What Laws?

- **Criminal Code**—Title 18
  - Computer Fraud & Abuse Act, 18 U.S.C. § 1030
  - Wiretap Act, 18 U.S.C. § 2511
  - Stored Communications Act (unlawful access), 18 U.S.C. § 2701
  - Identity Theft, 18 U.S.C. § 1028(a)(7) & § 1028A
  - Electronic Communications Privacy Act, 18 U.S.C. § § 2510-2522
  - Economic Espionage Act, 18 U.S.C. § § 1831-1839
- Other **Federal Civil Law & Regulations**:
  - HIPAA/HITECH (Healthcare)
  - FTC Act (Online Commerce—fraudulent and deceptive advertising))
  - GLB Act & OCC (Financial)
  - Privacy Act (Government)
- **State** Laws (47 states, DC, Puerto Rico, Virgin Islands)
- Payment Card Industry – PCI Industry-Enforced

Law Firms & Service Providers

- In 2012, Mandiant estimated that **80% of the 100 largest US law firms** were subject to successful data breaches by malicious intruders in 2011.
- March 4, 2016: FBI sends **Private Industry Notification**
  - "Criminal-Seeking-Hacker" Requests Network Breach for Inside Trading Operation
  - Financially motivated insider trading scheme targets international law firm information
  - Monitoring for material non-public information
- **Panama Papers**—40 years of client data; 2.6 TB data
- March 29, 2016: Crain's Chicago **Russian Hackers** seek Elite Chicago Law Firms' **M&A work**
- April 20, 2016: FBI **Ransomware** Alert

Many Sources for Risk

- Mobile Lawyers & Staff
  - Ubiquitous "Public" WiFi
- Diverse "Work" Venues
  - Conference Centers
  - Hotels
  - Home
  - Foreign Travel
- BYOD
- IoT
- IOLTA Accounts
- Client Trade Secrets
- Client Contacts
- Website "Success Stories"
- Document Management Systems--encryption
- PCI Compliance

Ethical Risks for Law Firms

- Duty of Competency: Model Rule 1.1
  - A lawyer shall provide competent representation
    - And "keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology"
- Duty of Communication: Model Rule 1.4
  - A lawyer shall keep the client "reasonably informed about the status of the matter"
- Duty of Confidentiality: Model Rule 1.6
  - A lawyer must take reasonable precautions to safeguard information relating to the representation of the client

Corporate Board Liability

- There is increasing importance for corporate boards (CISO) to take responsibility for cybersecurity issues.
- SEC Commissioner: boards are a critical part of risk management in cybersecurity.
- FINRA and FTC have an interest in boards working to mitigate security risks.
- NIST finds board involvement critical to successful implementation of the framework.

Breach Costs & Risk Protection

- Average cost per compromised record in 2014: $201
  - For “malicious” attacks: $246/record
  - Compare: Average cost per compromised record in 2010: $210
  - Average cost per compromised record in 2006: $138
- Companies with Incident Response Plan in place
  - Paid $17 less per compromised record
- Companies who alerted customers too soon
  - Paid $15 more per compromised record
- Building the Effective Cyber Risk Culture
  - Engage executive leadership
  - Target cyber risk management and awareness
  - Implement cost-effective technology investments tailored to needs
  - Adopt relevant cyber risk information sharing

The Costs of Breach: Target Example

- Data Breach in Nov-Dec 2013
- 40 Million Credit Card Holders
- 110 Million Total PII Compromised
- CIO fired; CEO fired; $148M in losses (2014)
- March 2015 Settlement: $10M Escrow for Victims
  - must meet criteria & apply
  - $10,000 max per victim
- April 2015 Settlement: $19M to MasterCard
  - Maintain Written Security Program
  - Appoint CISO
  - Train Employees on Security Program

Detection: Searching for Anomalies and Events

- Understand a baseline of your network operations – what is “normal” for users and systems?
- Assess unusual or anomalous events including system use and malicious code
- Determine the impact of the event
- Elevate events to key personnel
- CISA and Monitoring/Sharing

How to Catch a Vulnerability

Eliminate Information Silos…

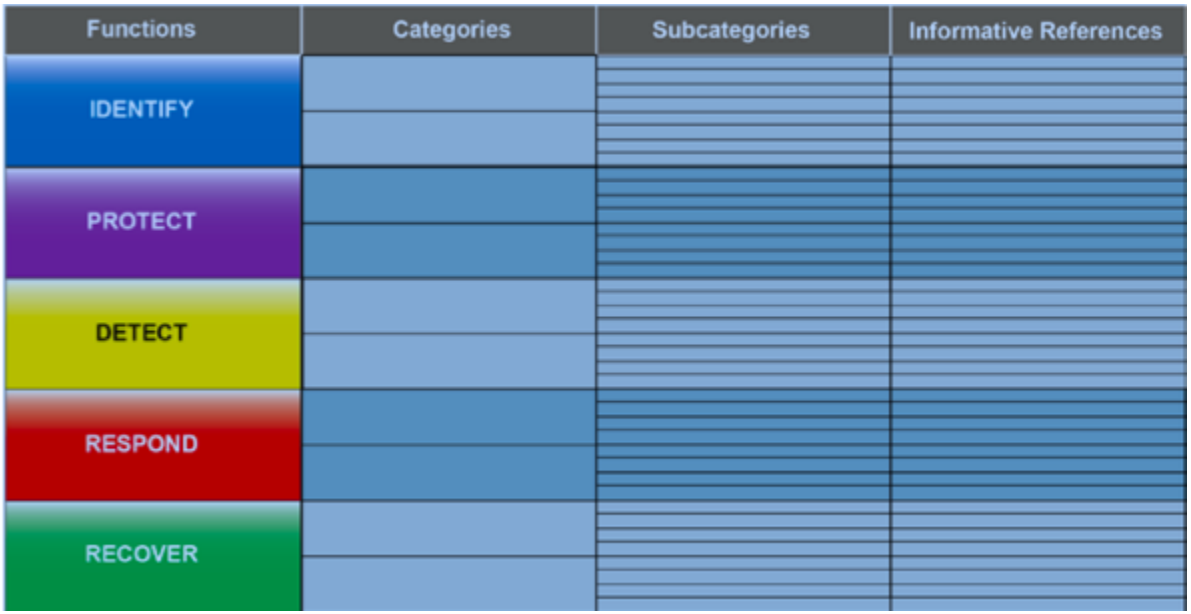
- Stay on top of the latest threats by ***signing up for email updates*** or following the RSS feed of trusted security providers.
- Calendar checkups of ***free databases of vulnerabilities*** identified by security researchers like the National Vulnerability Database (https://nvd.nist.gov/).
- ***Keep communication channels open*** with everyone up and down the chain where they can reach you if they discover a vulnerability.
- Consider a ***"bug bounty"*** where rewards are given to individuals who identify significant security vulnerabilities.

BEST PRACTICES

Current Federal Standard: NIST

NIST Cybersecurity Framework:

- Identify
- Protect
- Detect
- Respond
- Recover



Best Practices for Management

- Perform Risk Assessment (Physical Plant, IT & Staff)
- Segregate & Secure High Risk Data, Ops & Staff
- Encrypt! / Implement Robust Password Policy
- Implement Company-wide Training (Ongoing)
- Implement Cyber Incident Planning and Drills
- Acquire Cyber Liability Insurance
- Demand Compliance from Contractors & Suppliers
- Have an Expert Call List for If/When an Attack Occurs

Best Practices for IT Departments

- Adopt & Implement Doc Retention / Destruction Policy
- Evaluate Threat Landscape to Prioritize Treatment Strategy (It's not a "One-Size Fits All" World)
- Conduct Ongoing & Active Risk Analysis (Vulnerability Testing)
- Robust Firewall Configuration
- Enable Network Security Monitoring & Log File Review
- Collect, Analyze & Share Incident Data (CISA / ISAC)
- Track Workforce: Who's Who, What they Do & When they Go
- Regular Reporting Obligation to Mgt / Board

Checklist

- ✓ Encryption
- ✓ Robust Firewall Configuration
- ✓ Geoblock Countries (e.g., N. Korea, Syria, Romania, Iran)
- ✓ Backups (confirm ability to restore)
- ✓ Current Network Diagrams & Accurate Labeling
- ✓ Log Files & Monitoring
- ✓ Cyber Incident Plan & Drills
- ✓ Employee Training
- ✓ Employee Certifications & Background Checks

Thank you! Questions?

BUTZEL LONG

Claudia Rast | Butzel Long | Ann Arbor, MI | rast@butzel.com