

OVERVIEW OF CYBERSECURITY LAWS, REGULATIONS, AND POLICIES: FROM "BEST PRACTICES" TO ACTUAL REQUIREMENTS

DAVID THAW

UNIVERSITY OF PITTSBURGH



11/18/2014

(c) 2014 David Thaw -- academic use/distribution
permitted, contact author for other uses

BEFORE WE BEGIN...

- These slides are (deliberately) not comprehensive!
- Ask questions!
- No, really, ask questions!
 - There are no stupid questions. Only cybersecurity vulnerabilities (waiting to happen).
- Far more of cybersecurity is about *practices* than we care to admit...

OVERVIEW

- Structure of U.S. Cybersecurity Law and Regulation
 - Public Law
 - Private Law
- Why Focus on Private Law?
- Private Law in the U.S.
 - Security Breach Notification
 - Industry-Specific Regulation
 - General Consumer Protection (FTC)
- The Role of Criminal Law?

THE U.S. LEGAL SYSTEM

- A side note: three “categories” of regulating behavior of private actors:
 - Civil (contracts, torts)
 - Governs liability among private parties
 - Consequences are generally monetary
 - Criminal
 - Governs liability of individual persons to the state for “bad acts”
 - Consequences (“punishment”) involve loss of liberty
 - Regulatory
 - Governs liability of (usually) entities to the state for acts deemed not in the public interest
 - Consequences are financial and operational

STRUCTURE OF U.S. CYBERSECURITY LAW

- Public Law
 - Governs relationships between individuals/private entities and government agencies
 - “What *government* can/can’t do”
- Private Law
 - Governs relationships between private parties (individuals and/or private entities)
 - “What *private parties* can/can’t do”
- Why do these distinctions matter??

PRIVATE LAW

- Why focus on private law?
 - “Critical Infrastructure” mostly operated by private companies
 - Most of government uses private sector-built products
 - Who holds most of the data?
 - Hard to measure, but clearly tremendous amounts held in private hands
 - Private law (probably) reaches more entities in the information infrastructure
 - *Posse Comitatus* Act of 1878: no cybersecurity exception (yet!)
 - e.g., “we can only defend .mil!”
 - note: some exceptions (e.g., NSA “advising” Google)
- Bottom Line: Private law (currently) “where the action is”

CYBERSECURITY LAW: THE LANDSCAPE

- Industry-Specific Regulation [proactive/prevention]
 - HIPAA
 - GLBA
 - IRS Regulations
 - DoD Regulations (applicable to private contractors)
- Security Breach Notification Laws [reactive/detection]
- General Consumer Protection (Federal Trade Commission) [reactive/detection (mostly...)]
- State “Data Security” Standards [proactive/prevention]

2/26/2014

• SEC Disclosure Regulations [unclear]

(c) 2014 David Thaw -- academic use/distribution permitted, contact author for other uses

INDUSTRY-SPECIFIC REGULATION

- Nearly exclusively at the federal level
- Historically focused on consumer protection in healthcare (HIPAA) and finance (GLBA)
- Form of “Management-Based Regulatory Delegation”
 - Regulatory requirement primarily is:
 - (1) development of an information security plan; and
 - (2) adherence to that plan
 - But note: the plan must meet certain requirements (particularly with HIPAA)

GRAMM-LEACH-BLILEY ACT (GLBA)

- Gramm-Leach-Bliley Financial Modernization Act of 1999
- Two primary sets of regulations
 - Interagency Guidelines (Treasury Dep't)
 - Safeguards Rule (Federal Trade Comm'n)
- Generally speaking, require organizations to develop information security plans to address:
 - (1) Administrative risks;
 - (2) Technical risks; and
 - (3) Physical risks
- (only marginal additional detail provided)
- Requirements Exist (and organizations are following them)...
... but no major (Treasury Dep't) enforcement actions yet???
 - *Update: there was a recent action, the analysis of which is not yet complete.*

HIPAA SECURITY RULE

- Health Insurance Portability and Accountability Act (HIPAA)
 - Requires the Department of Health and Human Services to promulgate regulations establishing information security standards for the handling of Protected Health Information (PHI)
- “Security Rule”
 - Requires “Covered Entities” and their “Business Associates” to conduct risk assessments and develop plans and procedures to protect against:
 - (1) Administrative risks;
 - (2) Technical risks; and
 - (3) Physical risks
- Plans/procedures must be appropriate to the size, scope and capability of the organization
- Additional detail provided for each category
- There *has* been some enforcement activity (through OCR)

THINKING ABOUT HIPAA AND GLBA

- Management-Based Regulatory Delegation
 - **Key Point: (almost) everything is a “Business Risk Decision”**
 - What does this mean cybersecurity more broadly?
- How do we figure out what to protect and how to protect it?
 - **Risk assessments are key**
 - But, be wary of trying to “get away with” strict adherence:
- “That’s a *really* bad plan!”
 - Unencrypted emails
 - SSNs or other PII as document passwords
- Low-hanging fruit today vs. low-hanging fruit tomorrow
- Again: What does this mean for cybersecurity more broadly?

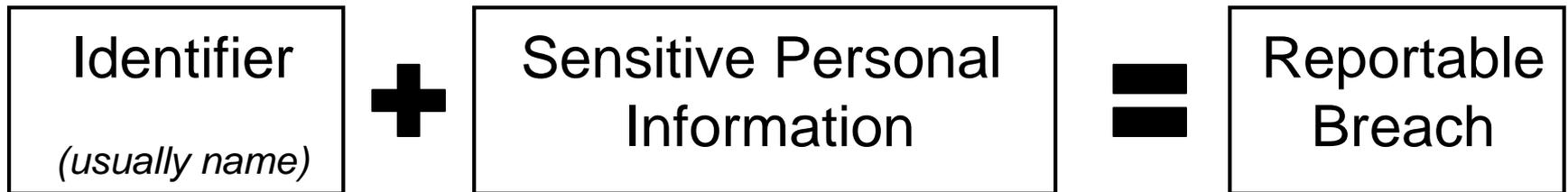
OTHER INDUSTRY SPECIFIC REGULATION

- IRS Publication 1075: Tax Information Security Guidelines for Federal, State, and Local Agencies
 - Applies to contractors as well!
- DoD Information Security Guidelines
 - They've got a few...
 - (most) apply to contractors as well
 - DoD relies more heavily on NIST publications... (more on this later)

SECURITY BREACH NOTIFICATION LAWS

- Require organizations to disclose certain types of security incidents involving the unauthorized access of “Personal Information”
 - Unless the information was “encrypted”
- 46 states, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have such laws
- Applicability is determined by the residence of the individuals *described* in the compromised data
 - *Not* by the location of the data
 - *Not* by the location of the entity experiencing the breach
- What does “encrypted” mean?
 - We’re back to “that’s a really bad plan...”
 - Why not use NIST definitions?

SBN “TRIGGERING” DATA



Three Common Types of Sensitive Personal Information:

- Social Security Number
- Payment Card/Account Number*
- Gov’t-Issued ID Number*

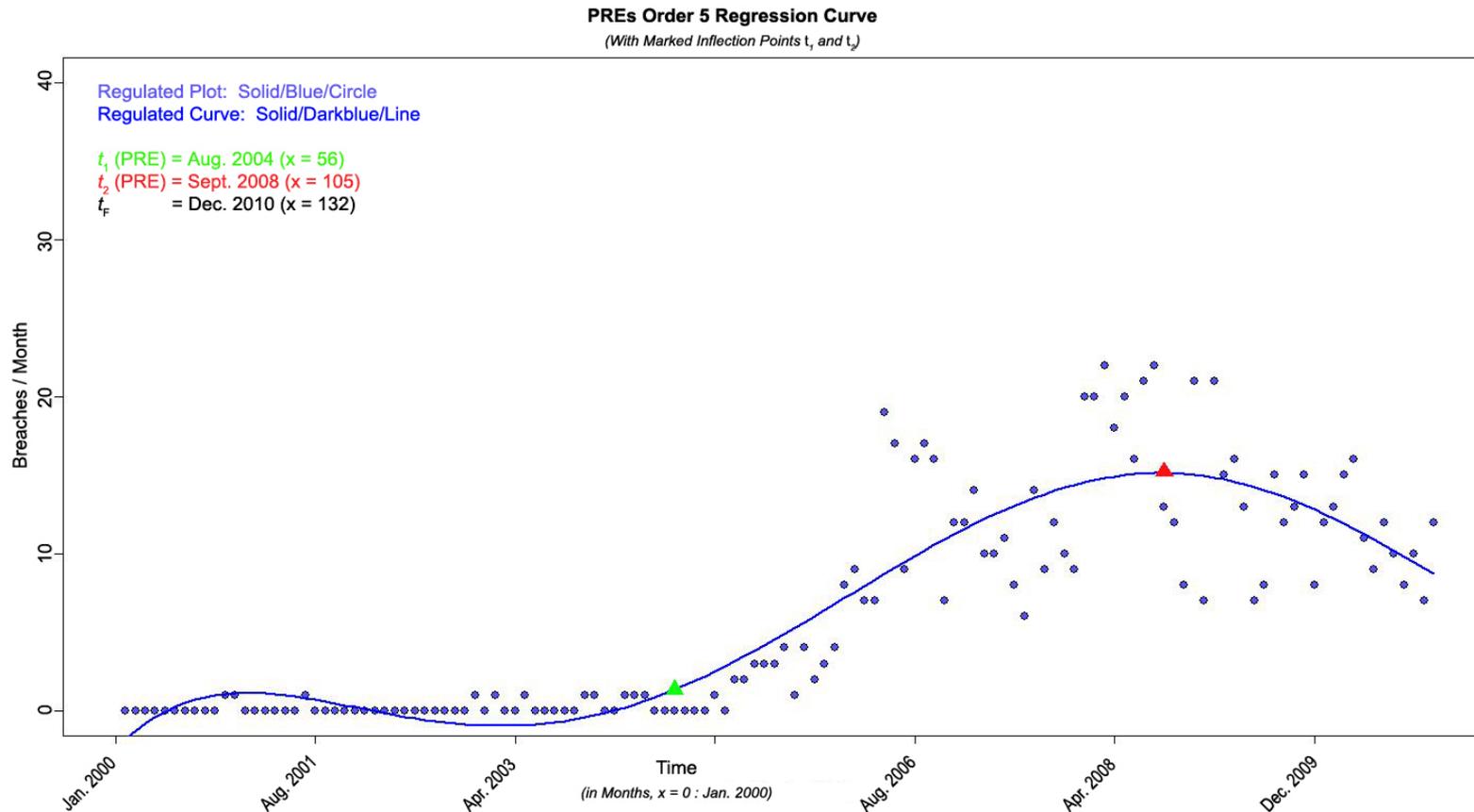
But: exception for “encrypted” data!

CISO QUOTES: EFFECTS OF SBNs

SBNs drive encryption policies:

- “. . . [SBNs] caused us to . . . in a very short period of time, encrypt 40,000 laptops . . .” (*CISO of a large healthcare organization*)
- “. . . What we have done is all computers now have to be encrypted.” (*CISO of a large telecommunications company*)
- “So what’s happened since the Notification Laws have become sort of ubiquitous in the last three years [is] the security investment is moved, essentially to crypto. If it moves, encrypt it. If it stays there, encrypt it. There’s not much reflection on whether or not actually anyone ever uses that data. It’s still a breach.” (*CISO of a large healthcare organization*)

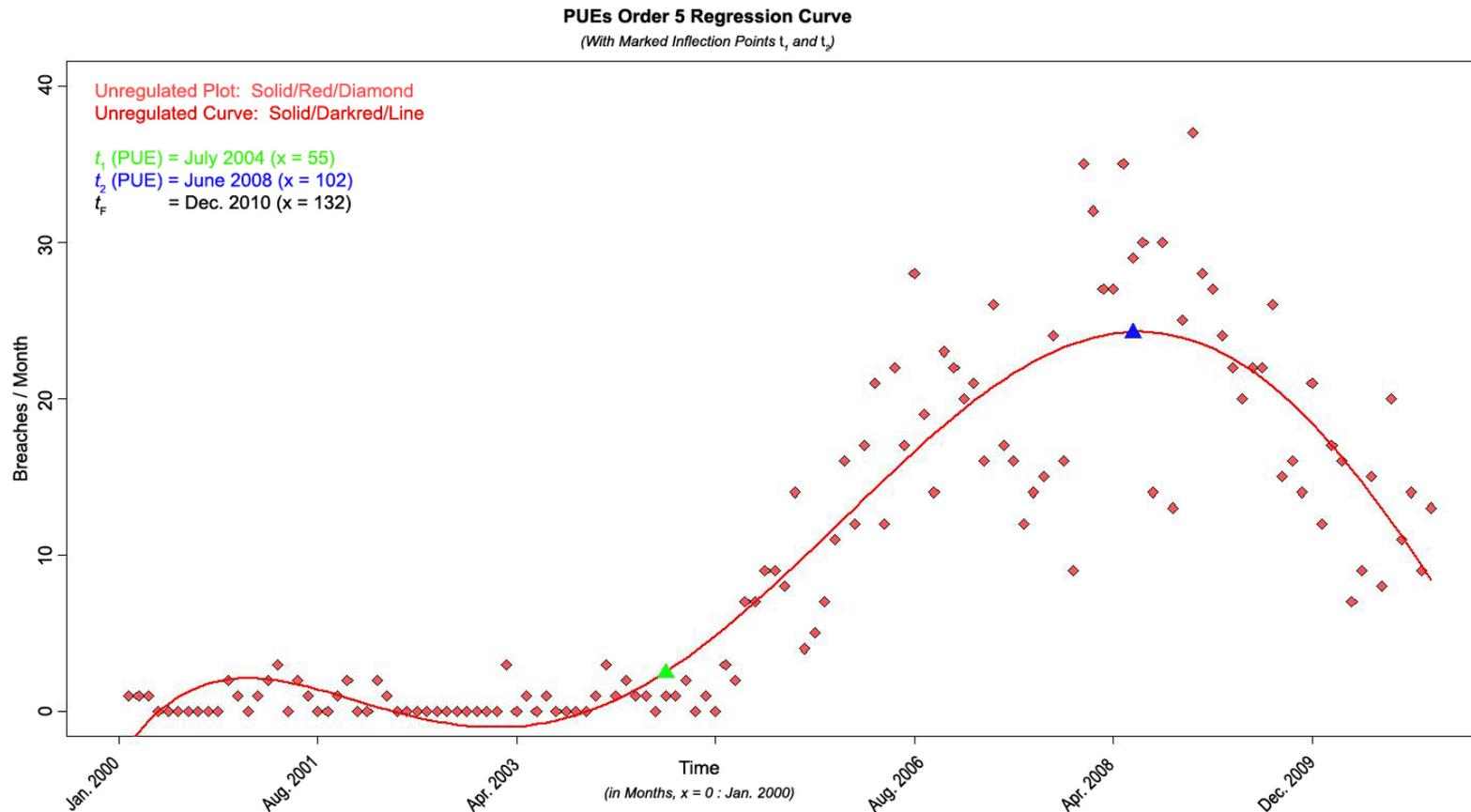
SBN EFFECTIVENESS: 2000-2010 (HEALTHCARE/FINANCE)



2/26/2014

(c) 2014 David Thaw -- academic use/distribution
permitted, contact author for other uses

SBN EFFECTIVENESS: 2000-2010 (ALL OTHER INDUSTRIAL SECTORS)



2/26/2014

(c) 2014 David Thaw -- academic use/distribution
permitted, contact author for other uses

THE FEDERAL TRADE COMMISSION

- Wait, the Federal *Trade* Commission? I thought we were talking about Cybersecurity?
 - 15 U.S.C. § 45 – “unfair or deceptive acts or practices”
- Insufficient information security practices are an “unfair and deceptive” trade practice
- To date, no Commission Enforcement Action has resulted in anything other than a settlement!
- Nature of settlements:
 - Agreement to 20 years of biennial information security audits
 - (Possible) restitution to affected consumers
 - **Agreement to discontinue the (allegedly) offending practice**

THE FTC

- Example (allegedly) offending practices:
 - Installing software to “track” consumers’ activities that captures sensitive authentication information (*Upromise, Sears*)
 - Failing to employ and require of customers secure authentication practices (*ACRANet, SettlementOne, ChoicePoint*)
 - Storing sensitive information/PII in cleartext in otherwise-vulnerable locations (*Ceridian, James B. Nutter, TJX*)
 - Improper document disposal procedures (*Gregory Navone, CVS CareMark*)
 - SQL injection vulnerabilities (*Ceridian, Compgeeks.com*)
 - Unsecured Wireless Networks (*TJX, DSW, BJ’s Wholesale*)
 - Failure to employ network security technologies including IDS/IPS and DLP (*Dave & Buster’s, TJX*)

FTC ENFORCEMENT

- When the Commission settles an Enforcement Action, it *de facto* establishes an information security standard
 - (Almost) all enforcement actions settle (**Exception:** *Wyndham Hotels*)
 - Yet we have so many “repeat offenders” – why?
- Breadth of Commission enforcement authority
- Focus on consumer protection
- There’s enough low-hanging fruit out there...
“reasonableness” is the key
 - Nearly all the Actions to date resulted from absurdly inadequate practices

2/26/2014

OTHER REGULATIONS

- State Data Security Standards
 - MA Data Security Standards (comprehensive)
 - CA, NV (limited)
 - Data disposal statutes (several states; specific in scope)
- SEC Disclosure Guidelines
 - “Registrants should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky.”
- http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm#_edn4

CRIMINAL LAW

- Computer Fraud and Abuse Act (CFAA) – 18 U.S.C. § 1030
 - § 1030 (a)(2)(C) – “intentionally access a computer without authorization or exceeds authorized access and thereby obtains information from any protected computer”
- Nearly any computer connected to the public Internet is a “protected computer”
- Definitions of “exceeds authorized access” vary widely
- This applies not just to hackers, but to *counter-attackers* as well!

WAR STORIES

- “But it’s a Mac!”
- “Well, they’re using a 32-bit *proprietary* algorithm... the client really wants this to work!”
- “The client *really* needs MS Office 2000 Encryption to work...”
 - *Remember the WEP/Wifi vulnerability? Applies to this too...*
- Delivery of sensitive Protected Health Information directly to the Dep’t of Health and Human Services *can be a “Bad Plan”*
- “Secure Email” → ***there is no such thing***

QUESTIONS?

Thank you!

David Thaw

dbthaw@gmail.com

<http://www.davidthaw.com>

2/26/2014

(c) 2014 David Thaw -- academic use/distribution
permitted, contact author for other uses