Big Data As a Threat?
An Alternative Approach to Cybersecurity

February 11, 2015

Brian Finch, Pillsbury Winthrop Shaw Pittman
Brian Fox, PwC

Data Breaches and Cyber Attacks

- Exposure of corporate secrets, trade secrets, and other proprietary information
- Exposure of personally identifiable information (employees and customers), including health information
- Disruption/destruction of operations

- Attacks are cheap: ($2 for crashing a website; $30 for malware verification; $5,000 for “zero day”)
- Malware now tends to be “one time use”

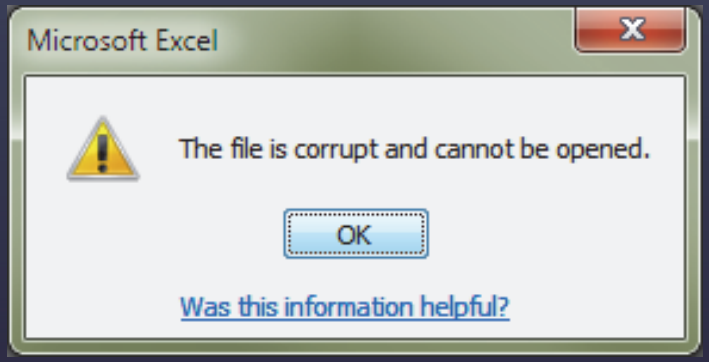
pwc pillsbury

Who is Conducting Cyber Attacks?

pwc pillsbury

Data-Borne Problems

- End-of-Life Issues
- “Insider Threat”
- Corrupted Data

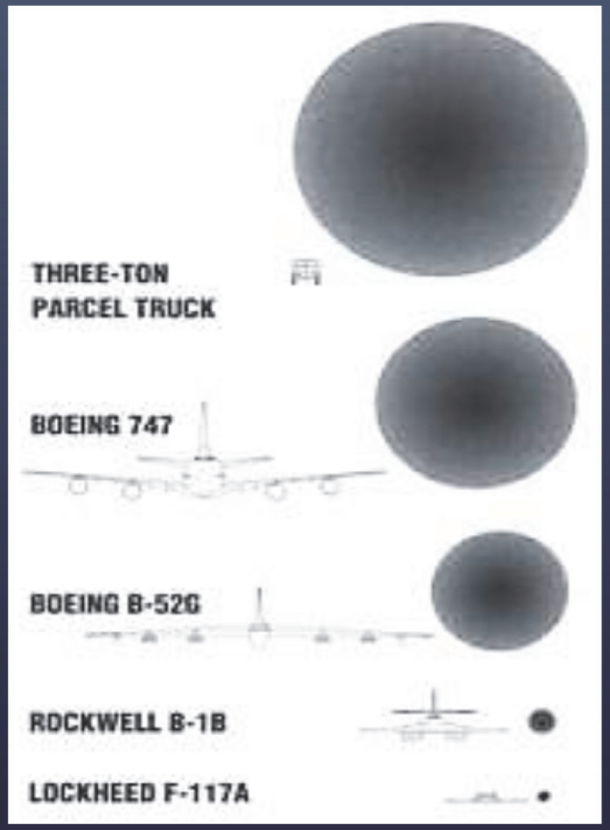


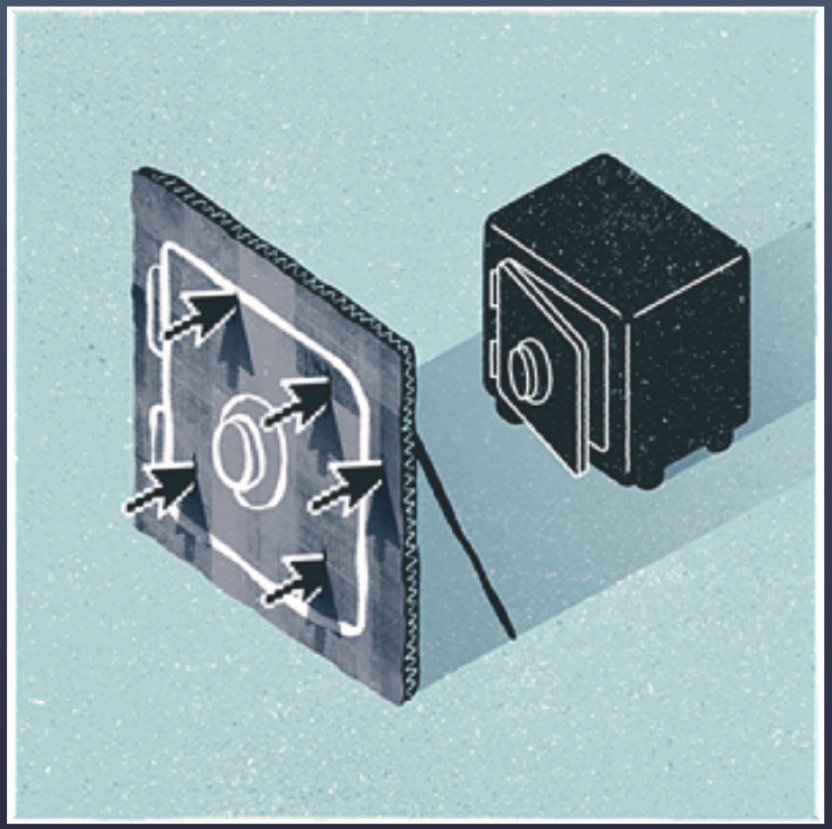
pwc pillsbury

Too Much Data?

pwc pillsbury

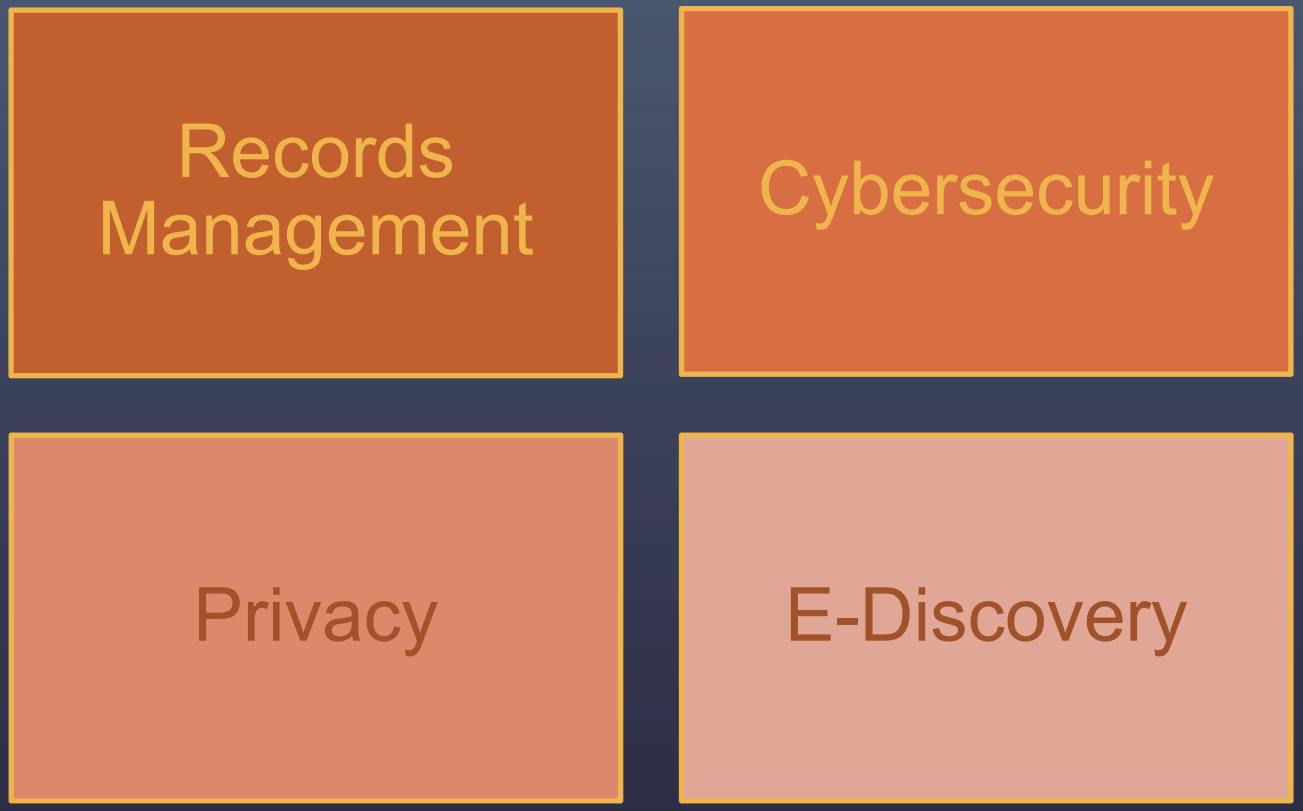
Reduce Your Value





pwc pillsbury

Disparate Information Risk Management



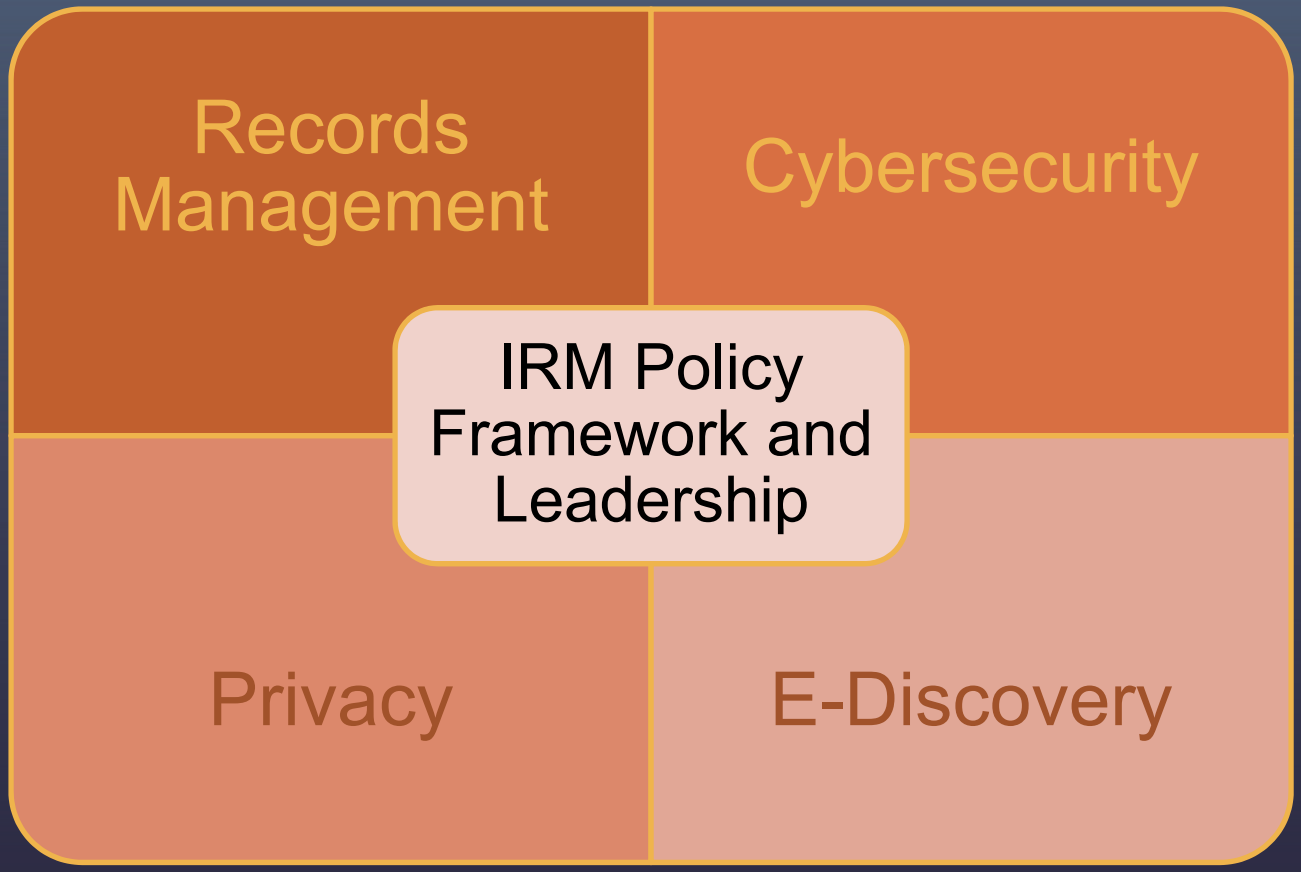
pwc pillsbury

Information Risk Management

- Companies are starting to understand how fundamentally these information risks are related
- Projects in the various areas often overlap or produce conflicting work products
- Training efforts developed separately create feeling of training overload
- Companies want:
  - Holistic view of information and data
  - Understanding of what you have and where you have it
  - Ownership over information in the business
  - Disposal of unnecessary data
  - Better identification of high-value information assets
  - Improved protection, security and access

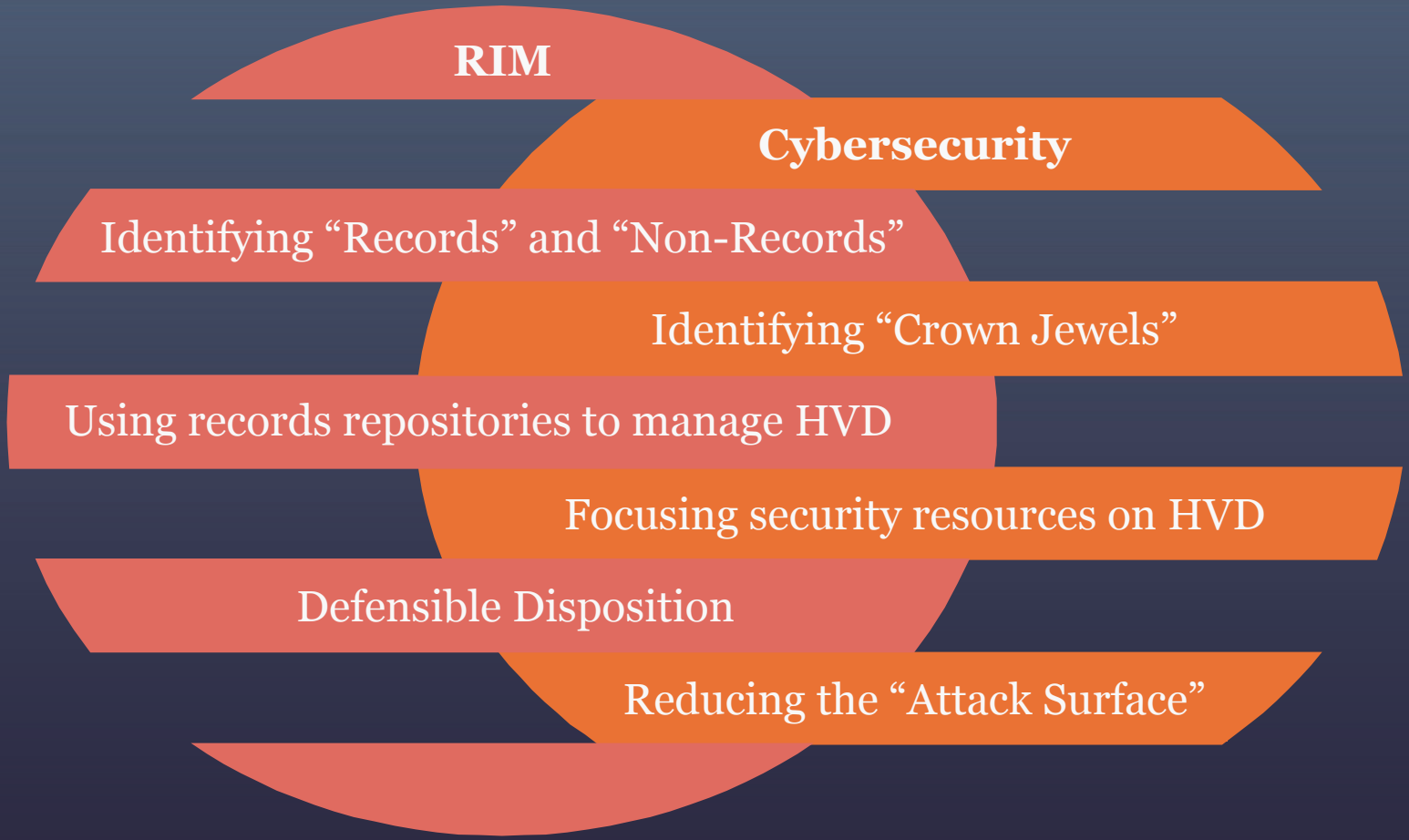
pwc pillsbury

Integrated Information Risk Management



pwc pillsbury

Records & Information Management "RIM" and Cybersecurity Complement Each Other in the Management of High Value Data ("HVD")



pwc pillsbury

Key Elements of an Integrated Program

Data inventory and Business Process Taxonomy

Identify the types & categories of data stored

- Surfaces what you have and where you have it
- Provides context for ownership and enrichment of data
- Information about how data should be stored, protected and managed can be derived through *inference* rather than direct analysis

pwc pillsbury

Key Elements of an Integrated Program

Facilitate routine, policy-driven disposition

Develop a risk-based, phased approach to the disposition and remediation of legacy data

- Less data means less legal risk & less info to protect, produce & recover
- Centralization can manage redundancy, offering greater insights into data & increased access to data
- Routine disposition creates a culture in the organization of separating high-value data from low-value data

pwc pillsbury

Many Theories of Liability

- Shareholder claims/ SEC Disclosures
- Loss of IP/trade secret claims
- Negligent selection, design or contracting
- Failure to take “reasonable” security measures for threats that a company knew or “should have known” about
- Strict liability
- FTC/State UDAP claims, international regulator liability

pwc pillsbury

What Would Litigation Look Like?

- From ***FTC v. Wyndham***
- Failure to:
  - remedy “known security vulnerabilities” such as allowing insecure server/network connections
  - employ commonly used methods to require user IDs and passwords that are difficult for hackers to guess
  - adequately inventory computers in order to manage network devices
  - employ reasonable measures to detect and prevent unauthorized access or to conduct security investigations
  - follow proper incident response procedures, including failing to monitor computer network for malware used in a previous intrusion
  - adequately restrict 3d party vendor access
  - share threat information/act upon shared information
- How can you make sure you are taking “reasonable” cyber security measures?

pwc pillsbury

The SAFETY Act

"**S**upport **A**nti-Terrorism by **F**ostering **E**ffective **T**echnologies Act"

- Part of the Homeland Security Act of 2002
- **Eliminates** or minimizes tort liability for sellers of DHS-approved "technologies" should suits arise after an attack (physical or cyber), including:
  - SAFETY Act protections obtained only by submitting an application to DHS
  - ***Applies to services, products, policies***
    - *This includes* ***self-deployed programs***
  - Protections apply even if approved technologies are sold to **commercial** customers or if the attack originates from **abroad** so long as US interests implicated (i.e., economic losses)

pwc pillsbury

Act of Terrorism = Cyber Attack

- Any cyber security product, service, and/or policy is eligible for SAFETY Act protections
- Cyber attacks are encompassed under this definition
- There is NO requirement that the attacker's identity or motivation be identified/proven:
  - Only mention of "intent" potentially relates to intent to cause injury or loss, NOT traditional "terrorist" intent
- This means that ANY cyber attack could potentially trigger SAFETY Act liability protections

pwc pillsbury

Designation vs. Certification

- Two levels of protection under the SAFETY Act
- Under “Designation”:
  - Claims may only be filed in Federal court
  - Damages are capped at a level set by DHS
  - Bar on punitive damages and prejudgment interest
- Under “Certification” sellers also receive a presumption of immediate dismissal
- In both circumstances claims against **CUSTOMERS are to be immediately dismissed**

pwc pillsbury

Key Questions and How To Use

- Any costs for filing a SAFETY Act application? **N**O
- What kind of cybersecurity products are eligible for SAFETY Act protections?
  - All *PRODUCTS, SERVICES, AND/OR POLICIES, INCLUDING INTERNAL POLICIES*.
- What is the practical effect of obtaining SAFETY Act protections?
  - ***A cap on damages or immunity*** from damages arising out of or related to cyber attacks.
- Can I realize SAFETY Act benefits just by purchasing and using SAFETY Act approved cyber security solutions? **YES**
- Can I require SAFETY Act approval in procurements? **YES**
- What kind of claims will this help mitigate/eliminate?
  - **Negligence, third party liability, failure to take reasonable mitigation steps, D&O claims**

pwc pillsbury

Thank You for Participating!

Brian Finch, Partner
Pillsbury Winthrop Shaw Pittman LLP
Phone: 202.663.8062
brian.finch@pillsburylaw.com

Brian Fox, Principal
PwC
Phone: 646.471.3398
brian.t.fox@us.pwc.com