Setting the Roadmap for Data Protection

Raising the Stakes

James D. McCartney CIPP/G, CITRMS

Identity Management and Privacy Specialist

The World Has Changed

- The risks businesses face have changed, but the way in which they are addressed have not
- Rapid increase in ability to access the information, and the information is more valuable
- Approach to protection has changed
  - Nature of regulation/legislation
  - Boundaries of protection have expanded

The Challenge of Risk

- **Fundamentally, we are bad at making decisions about risk**
  - **We react to our feelings, not reality**
  - **We underestimate risks over which we believe we have control**
  - **Lack of evidence is viewed as success**
- **The less we hear about the risk, the more we should worry about it**
- **Inherent problem of low probability events**
- **We need better models**

www.ted.com The Security Mirage Bruce Schneier

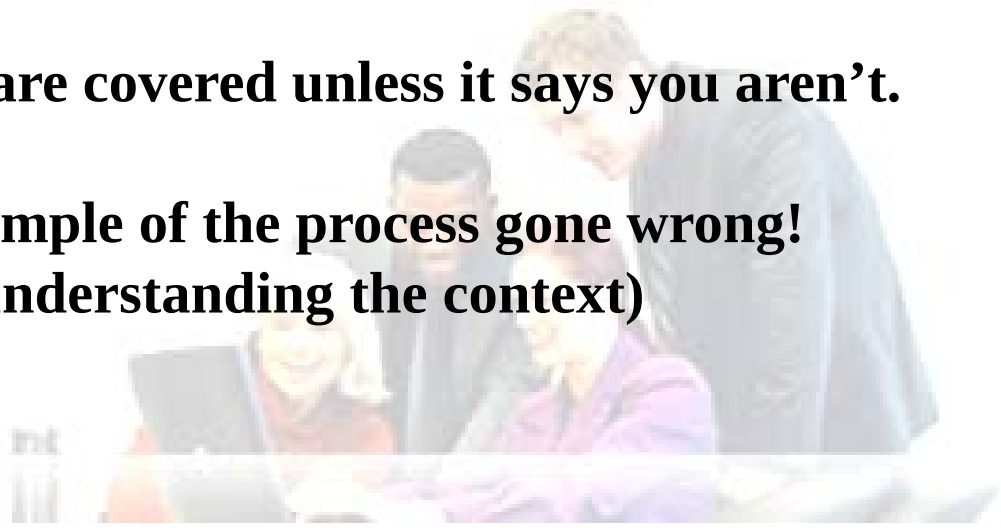
Accountability Based Regulation

Traditional regulatory regimes are insufficient for technical issues. Legislation and Regulation is obsolete before it is passed.

Accountability-based regulations are descriptive, not prescriptive. They state what is to be accomplished, not how.

Inclusive vice exclusive. You are covered unless it says you aren't.

Red Flags Rule is the best example of the process gone wrong! (People – read AMA – misunderstanding the context)



Securing The Data Based You

HITECH, RFR, HIPAA, other State & Federal Laws

Businesses must Insure that they Share ,Sell, Give, Information with /to ONLY Those Vendors and Business Associates with these same measures in place. Reduces risk of individual becoming a victim through a 3rd Party Vendor with which the victim has no direct relationship

Red Flags Rule (RFR) State Immigration Acts

Requires Businesses to Authenticate the Identity of Their Patients/Employees – Helps reduce the risk of perpetuation of a crime against an innocent victim

Data Security Laws, HIPAA, GLB & SC ID Theft Law

Requires Businesses to Protect Personally Identifiable information Reduces threat of thief gaining access to information which can be used to corrupt an individuals records

Privacy Laws, HIPAA, HITECH; GLB & State Laws

Requires Businesses to Limit Access to and Keep Private Personally Identifiable Information - Reduces access to information & protects individual's privacy; Only allows permissible access with permissible uses

FACTA – Document Destruction Rule – State Laws

Businesses must Destroy/Shred All Documents or Digital Media Containing PII or NPI upon Disposal - Reduces threat from loss & resulting misuse of PII or NPI which can be used to steal someone's identity

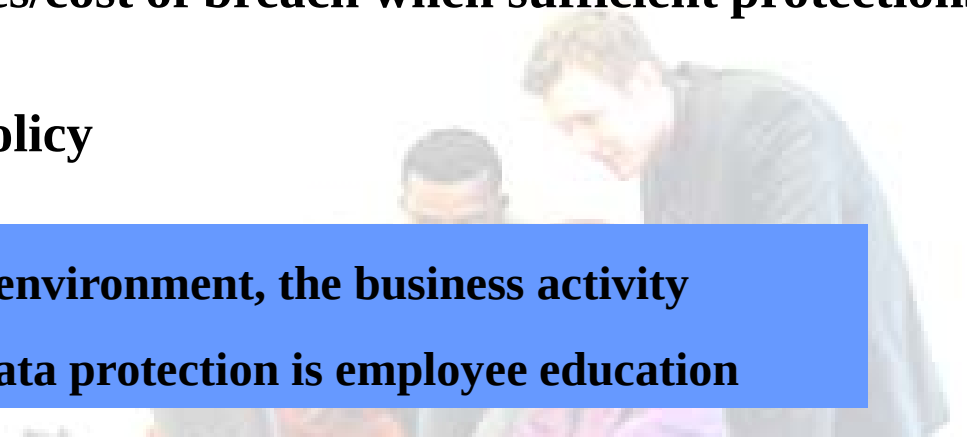
These issues, although separated by the legislative process, are not so cleanly separated in our day to day practices.

Compliance ≠ Liability Reduction

'a covered entity or business associate cannot assert an affirmative defense associated with its "lack of knowledge" if such lack of knowledge has resulted from its failure to inform itself about compliance obligations or to investigate received complaints or other information indicating likely noncompliance.' ***Federal Register. Vol. 75, Vol. 134, July 14, 2010. Page 40878***

Risk Assessment & Management

- **Yes, it's required by HIPAA, but more broadly tells you where to where your risk is and what you can do about it**
- **Risk Assessment is not about Risk Elimination, but Risk Avoidance, Reduction and Management**
- **Should be conducted on a regular basis**
- **Appropriate documentation is critical**
- **Significant reduction in losses/cost of breach when sufficient protections in place**
- **Have to match reality, not policy**



In a resource constrained environment, the business activity with the highest return for data protection is employee education

Putting it Together

- **While technology is a piece this is not a technology problem**
- **Risks don't end at your doors, you are responsible for the actions of your vendors and business partners**
- **While it is nice to think people will do the right thing, they may need additional motivation**
- **There are real consequences – despite general beliefs**
- **Effective does not mean complicated**
- **Cost effective resources are available**

You get what you INSPECT, not what you EXPECT.

-ADML Hyman G. Rickover

Questions?

Contact Information

James D. McCartney

CIPP/G, CITRMS

jmccartney@deloitte.com

571-263-1612

If You are Me, Then Who am I?

The Personal and Business Reality of Identity Theft

Available at *www.amazon.com*