IUA Digital Risk Working Party Seminar
October 19, 2011
Security versus *Accessibility*

Cyber Risks:
Global Privacy and Data Breach Risks

Theodore P. Augustinos
Partner

Richard Graham
Partner

EDWARDS WILDMAN

© 2011 Edwards Wildman Palmer LLP & Edwards Wildman Palmer UK LLP

Summary

- Cyber Risks
- Cyber Losses
- Legal and Regulatory Framework
- Data Breach Notification
- Data Breach Response
- Developments and Trends

Cyber Risks

- 2011: The Year of the Breach
  - Increasing Incidents and Risks of Breaches

SONY	Google	epsilon Marketing As Usual. Not A Chance.™	ANONYMOUS
citibank	#ANTISEC		LulzSec
DigiNotar Internet Trust Services	EDF	Massachusetts and other governmental agency breaches	Hospitals and other healthcare providers

Cyber Risks

- The Growth in Cyber Threats

88% of US companies reported a breach in 2010. Some multiple times.

2011 Data Breach Investigations Report

The total economic burden created by data breaches in the healthcare sector is $6 billion annually.

2011 Deloitte Report

The average total cost of a data breach per company was more than $7.2 million in 2010.

2010 Ponemon Institute

92% of attacks in 2010 were not considered highly difficult and 96% of breaches were avoidable.

2011 Data Breach Investigations Report

39% of breaches in 2010 involved mistakes by third party outsourcers, and those breaches cost 48% more than internal breaches.

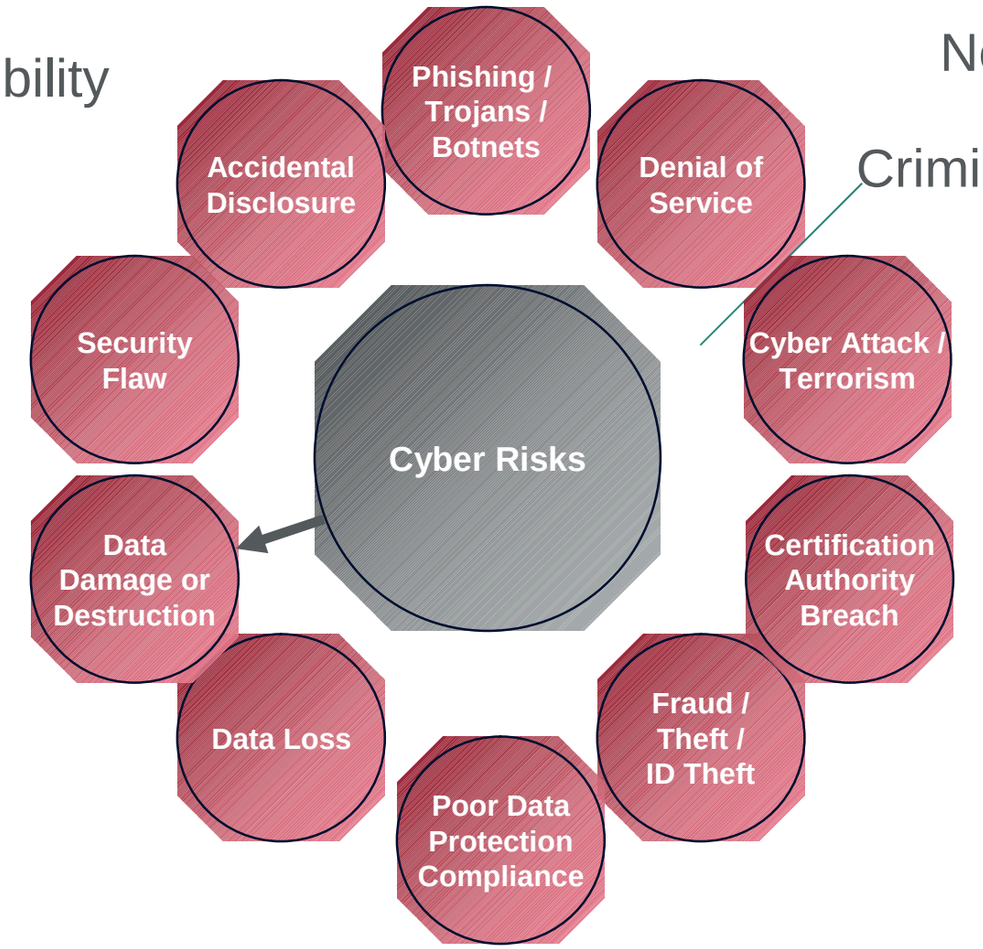
2010 Ponemon Institute

The amount of malware and spyware on mobile phones more than doubled from December 2009 to May 2010.

2011 New York Times

Cyber Risks

- Sources of and Responsibility for Breaches



Negligence or Criminal/Malicious Activity

EDWARDS WILDMAN

Cyber Losses

Reputation Management

- Crisis Management Costs
- Public Relations Costs
- New Customer Marketing Costs
- Loss of Goodwill

Direct Costs

- Forensics
- Legal
- Data Breach Notification Costs
- Remediation Services
- Card replacement costs and PCI fines

Regulatory Liability

- Regulatory Investigation and/or Audit Costs
- Regulatory Fines

Civil Liability

- Breach of Contract Costs
- Breach of Confidentiality Costs
- Third Party Liability

Indirect Losses

- Loss of Revenue or Business
- Loss of and/or Reconstitution of Data
- Loss of Anticipated Savings
- Loss of Profits

EDWARDS WILDMAN

Cyber Losses

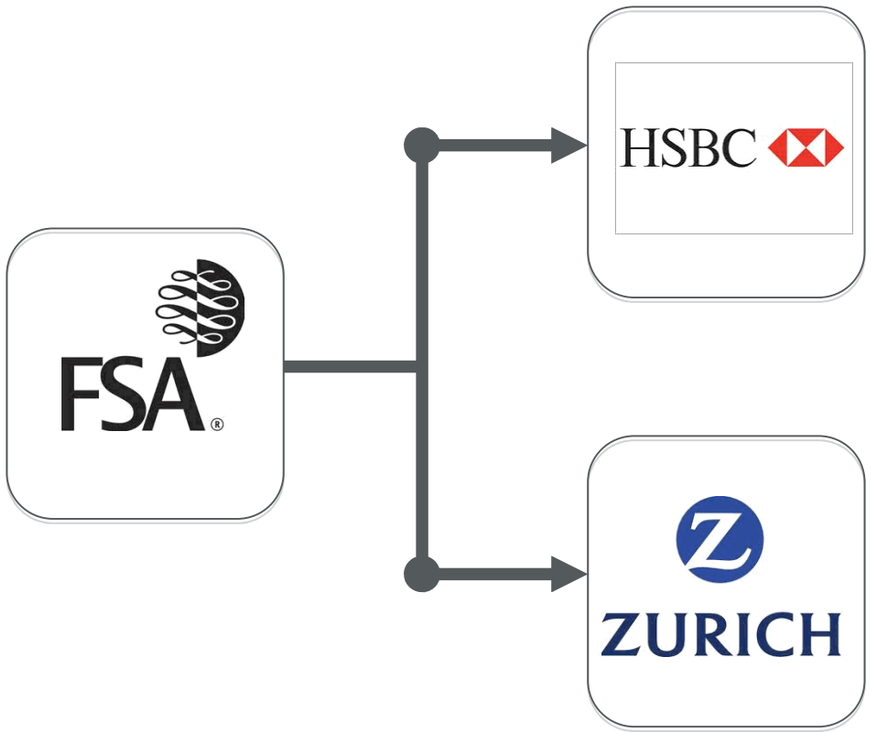
- Regulatory Liability: UK ICO Regulatory Fines

- Employment services company
- Theft of unencrypted data
- Personal information relating to 24,000 people
- 2010: £60,000 fine

- Surrey County Council
- Sensitive personal data sent to wrong people
- 2 further data breaches
- 2011: £120,000 fine
- Largest ICO fine to date

Cyber Losses

- Regulatory Liability: UK FSA Enforcement Action

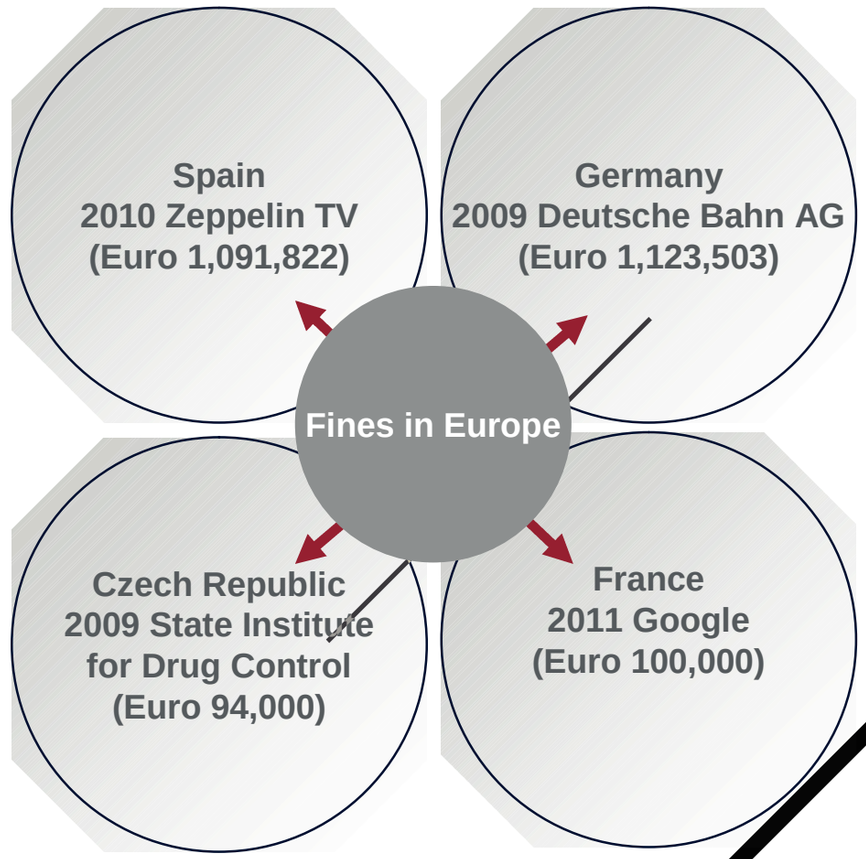


- 3 HSBC Companies
- Loss of Unencrypted Data sent to Third Parties
- Inadequate Training
- Ineffective Systems and Controls
- 2009: £3m FSA Fine

- Zurich Insurance Plc
- Outsourcing Agreement
- 46,000 Customer Details
- Loss of Back-up Tape
- Ineffective Systems and Controls
- 2010: £2.275 FSA Fine

Cyber Losses

- Regulatory Liability: EU examples

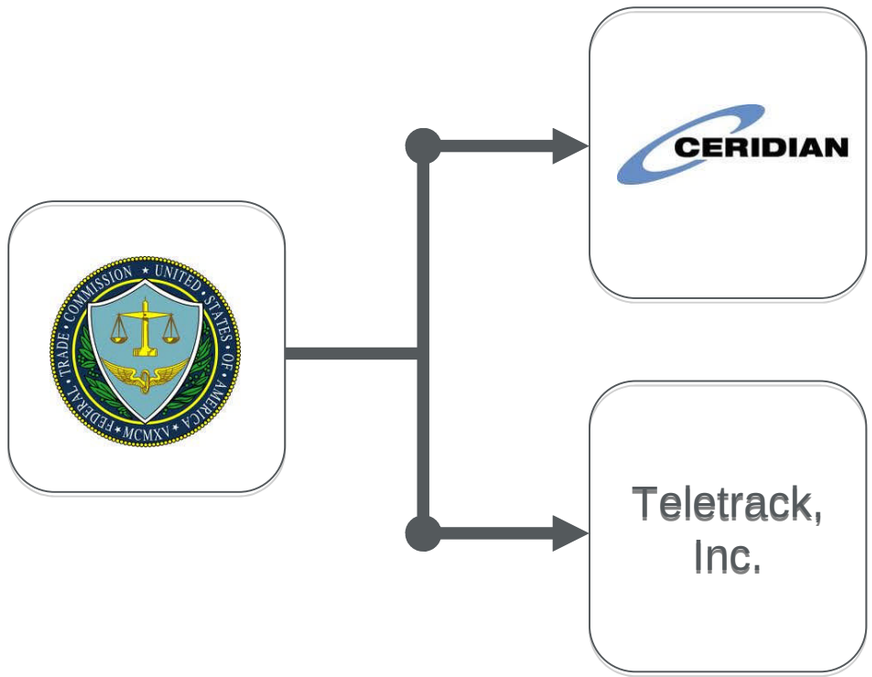


- Other
  - Criminal Sanctions
  - Imprisonment

EDWARDS WILDMAN

Cyber Losses

- Regulatory Liability: Recent US Enforcement Actions
  - Federal

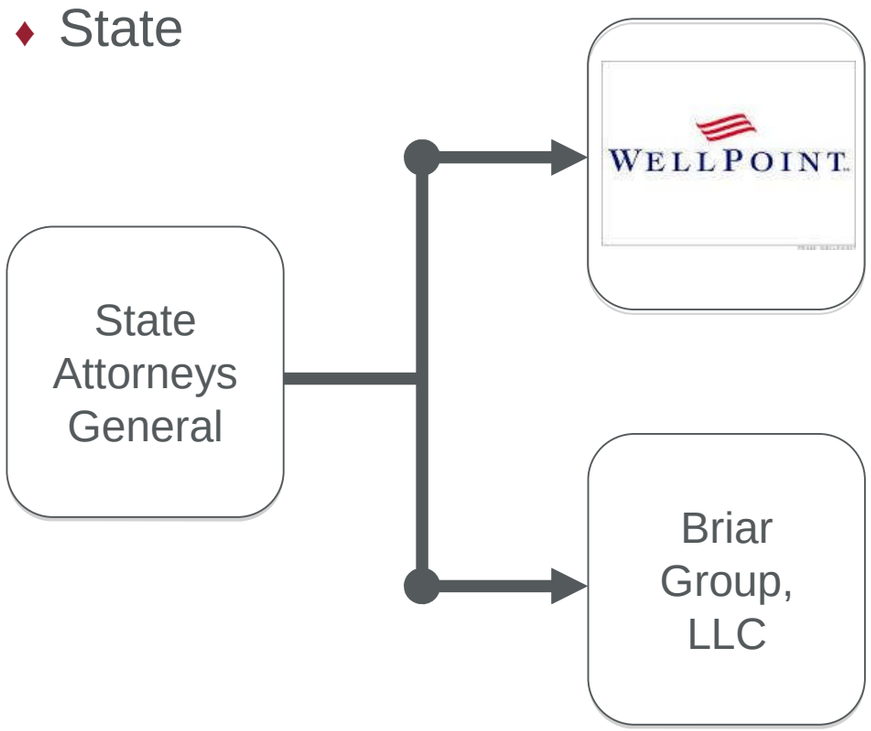


- Outsourcer of payroll and HR services
- Lost 28,000 customer employee records to SQL injection
- Claims regarding security were false and deceptive
- Settlement / 20 years of biennial independent audits

- Sale of credit reports to marketing firms
- Violation of FCRA
- $1.8 million fine
- Ongoing reporting requirements

Cyber Losses

- Regulatory Liability: Recent US Enforcement Actions
  - State

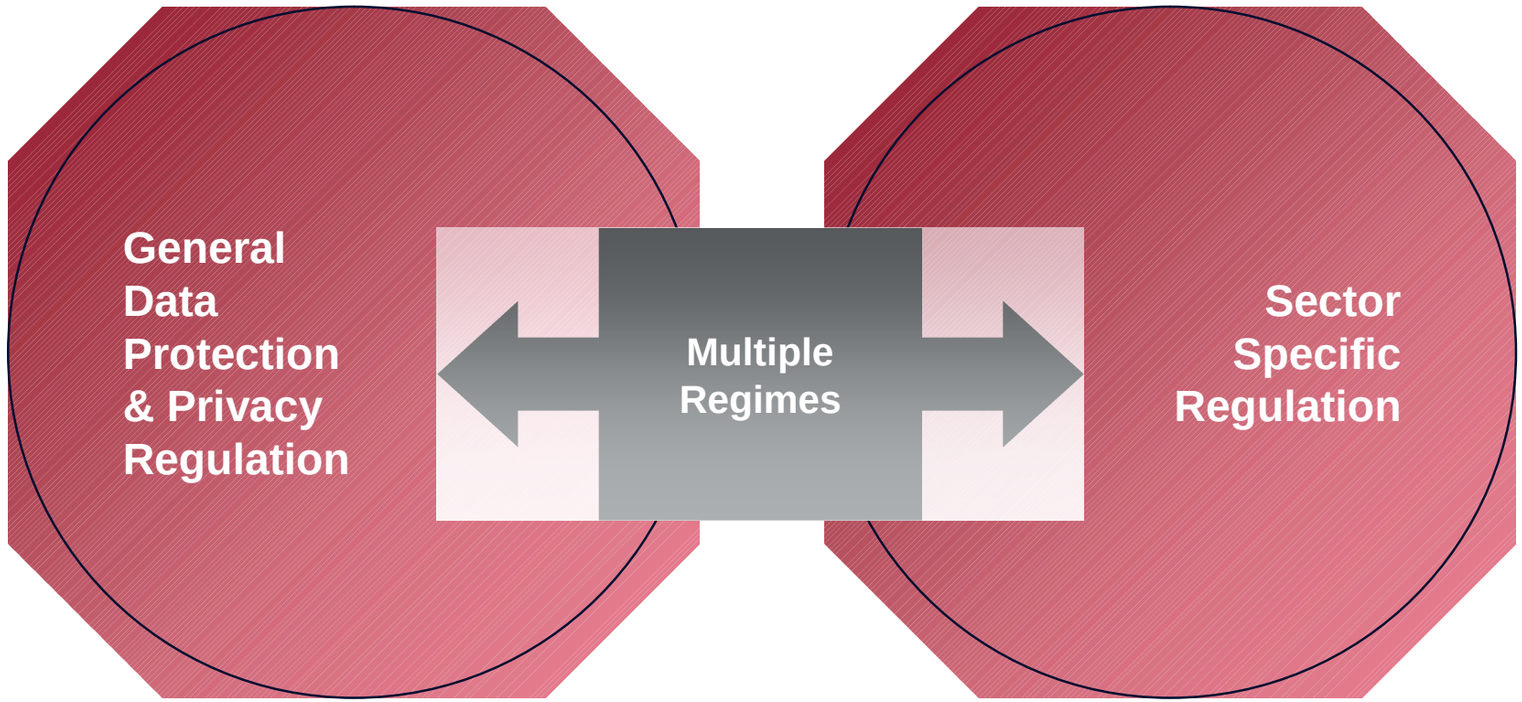


- Hospital Group
- 600,000 individual insurance applicants
- Health and financial information
- Exposed on website
- Indiana State Attorney General enforcement action
- Under authority of HIPAA/HITECH
- $100,000 fine and other charges and expenses

- Restaurant chain
- State enforcement action under MA consumer protection law pre-dating state data protection law
- $110,000 fine levied by MA

Legal and Regulatory Framework

- Regulatory Compliance: Global Sources of Requirements



Legal and Regulatory Framework

- Data Protection Regulation in the EU

Data Quality limitation of purpose and time; accuracy; relevance…	Filing Requirements
Justification for processing including consent	
Transparency	
Individual rights access, rectification & preventing processing	
Security	
Transborder data flow restrictions	

Legal and Regulatory Framework

- Data Protection Regulation: Security of Processing in the EU

Data Protection Directive (EU Directive 95/46/EC)

Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

Legal and Regulatory Framework

- Data Protection Regulation: Security of Processing in the EU

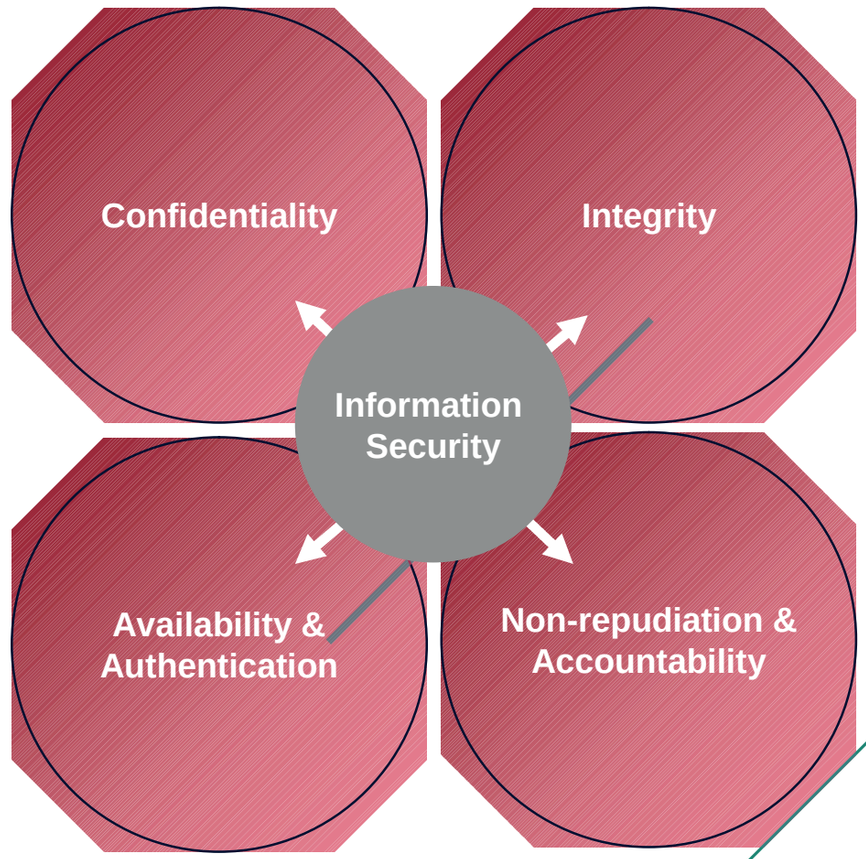
Data Protection Directive (EU Directive 95/46/EC)

The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that: (i) the processor shall act only on instructions from the controller, (ii) the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

Legal and Regulatory Framework

- Information Security



- Information
  - Financial Data
  - Personal Data
  - Client Data
  - Market Data
  - Content
- ISO/IEC 27001
- ISO/IEC 27002

EDWARDS WILDMAN

Legal and Regulatory Framework

- US Privacy & Data Protection Laws – General Themes
  - Generally, PI consists of an individual's name (full or first initial and last name) together with one of the following:
    - Social Security number
    - Driver's license or other state-issued ID
    - Financial account or credit card number with or without PIN
    - California, for example, includes certain health information
  - Types of protections include:
    - Limitation on what information can be collected and how it can be used
    - Requirements for physical and electronic security
    - Retention and disposal requirements
    - Requirements for vendor relationships

Legal and Regulatory Framework

- US
  - Privacy – Generally not as expansive as UK and EU, although changing
    - Federal Statutes
      - HIPAA and HITECH
      - Gramm-Leach-Bliley Act of 1999
      - Fair Credit Reporting Act
      - Children's Online Privacy Protection Act

Legal and Regulatory Framework

- US continued
  - States
    - California
      - First US privacy law
      - Song-Beverly Act restricting collection of addresses in connection with credit card transactions
    - Massachusetts
      - Leading US state privacy and data protection requirement
      - Broad and granular requirements
        - Requires company-wide assessment of risk
        - Specific encryption requirements
        - Vendor contract provisions
        - Collection, storage and disposal restrictions

Legal and Regulatory Framework

- Data Protection in the US
  - States (continued)

Nevada, Minnesota & Washington	PCI DSS incorporated into statute
Connecticut	Specific protection for Social Security numbers
New York	Document retention and destruction requirements

Legal and Regulatory Framework

- Sector Specific Regulation
  - EU
    - Financial Services
    - Communication Services
    - eCommerce Services
    - Healthcare Services
    - Gambling Services
  - US
    - Financial Services
    - Healthcare
    - eCommerce
    - Credit and Employment

Data Breach Notification

- US Data Breach Notification Requirements
  - Generally, more advanced and onerous than other countries
  - Generally, “breach” is defined to mean the
    - acquisition or misuse of,
    - or, in some cases, access to
    - PI
    - by an unauthorized person

    - Some states have a likelihood of harm threshold
      - Connecticut’s harm threshold requires consultation with appropriate federal, state and local law enforcement.

Data Breach Notification

- Data Breach Notification in the US
  - Federal

Gramm-Leach-Bliley	*HIPAA and HITECH*	*Bills Pending (see Developments and Trends)*

  - States

46 States

- All but 6 apply only to electronic data.
- Notification to individuals
- 15 require notice to state agencies.
- No remediation technically required, but expected.
- Different definitions make analysis expensive.

Data Breach Notification

- Data Breach Notification in the EU
  - Directive 2002/58/EC (Privacy and electronic communications)

    Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community.

  - Conditions
    - Personal Data Breach
    - Publicly Available Electronic Communications Service
    - Notification:
      - Competent National Authority '*without due delay*'
      - Data Subject '*where…likely to adversely affect*'
    - Exceptions

Data Breach Notification

- Data Breach Notification in the EU
  - Breach Notification Consultation (Closed 9 September 2011)
    - Circumstances
    - Procedures
    - Formats
  - Technical Implementation Measures

enisa European Network and Information Security Agency

Article 29 Working Party

European Data Protection Supervisor

  - Data Protection Directive Consultation

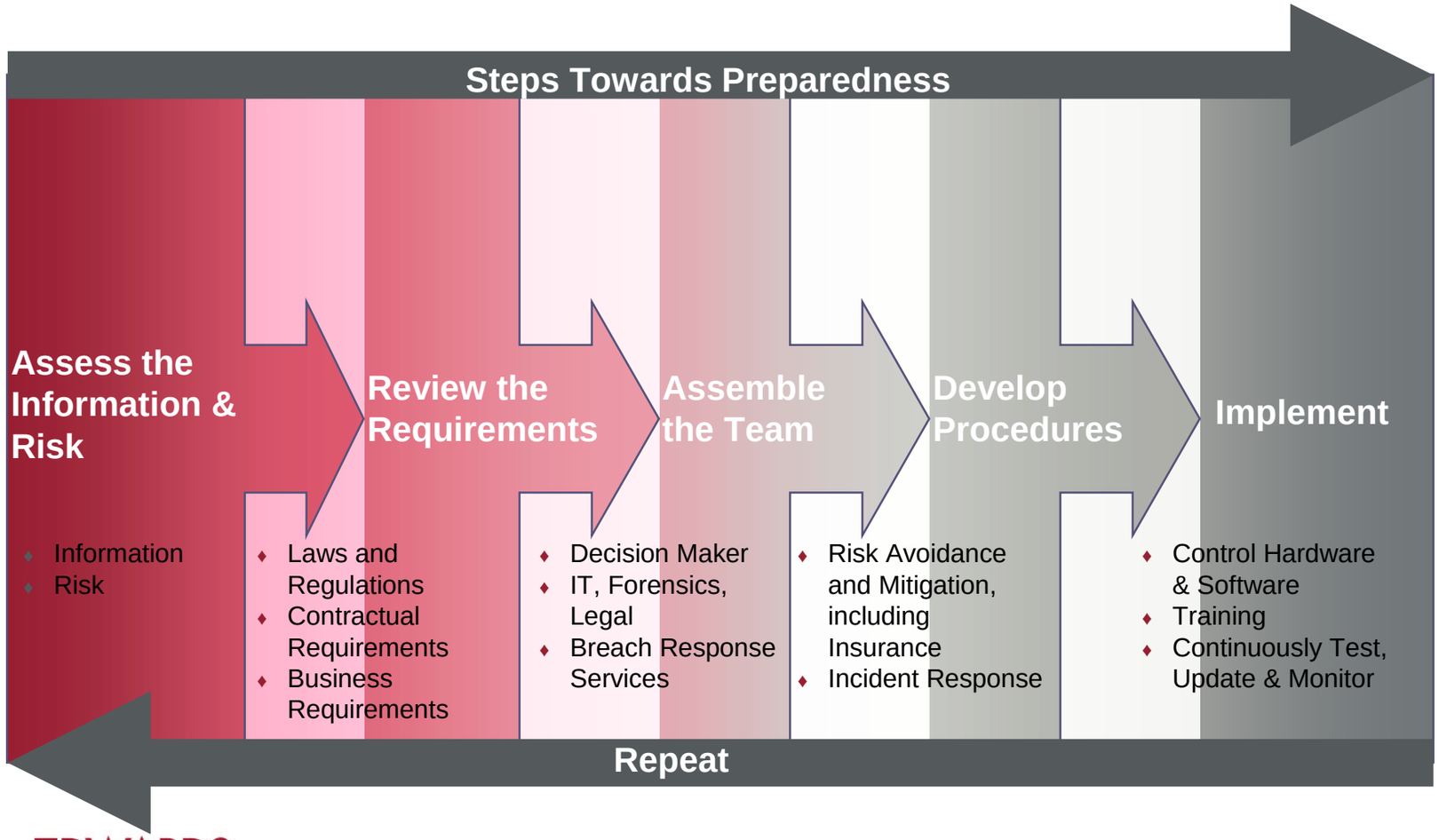
Data Breach Response

- Breach Preparedness

> "In preparing for battle, I have always found that plans are useless, but planning is indispensible."
>
> Dwight D. Eisenhower

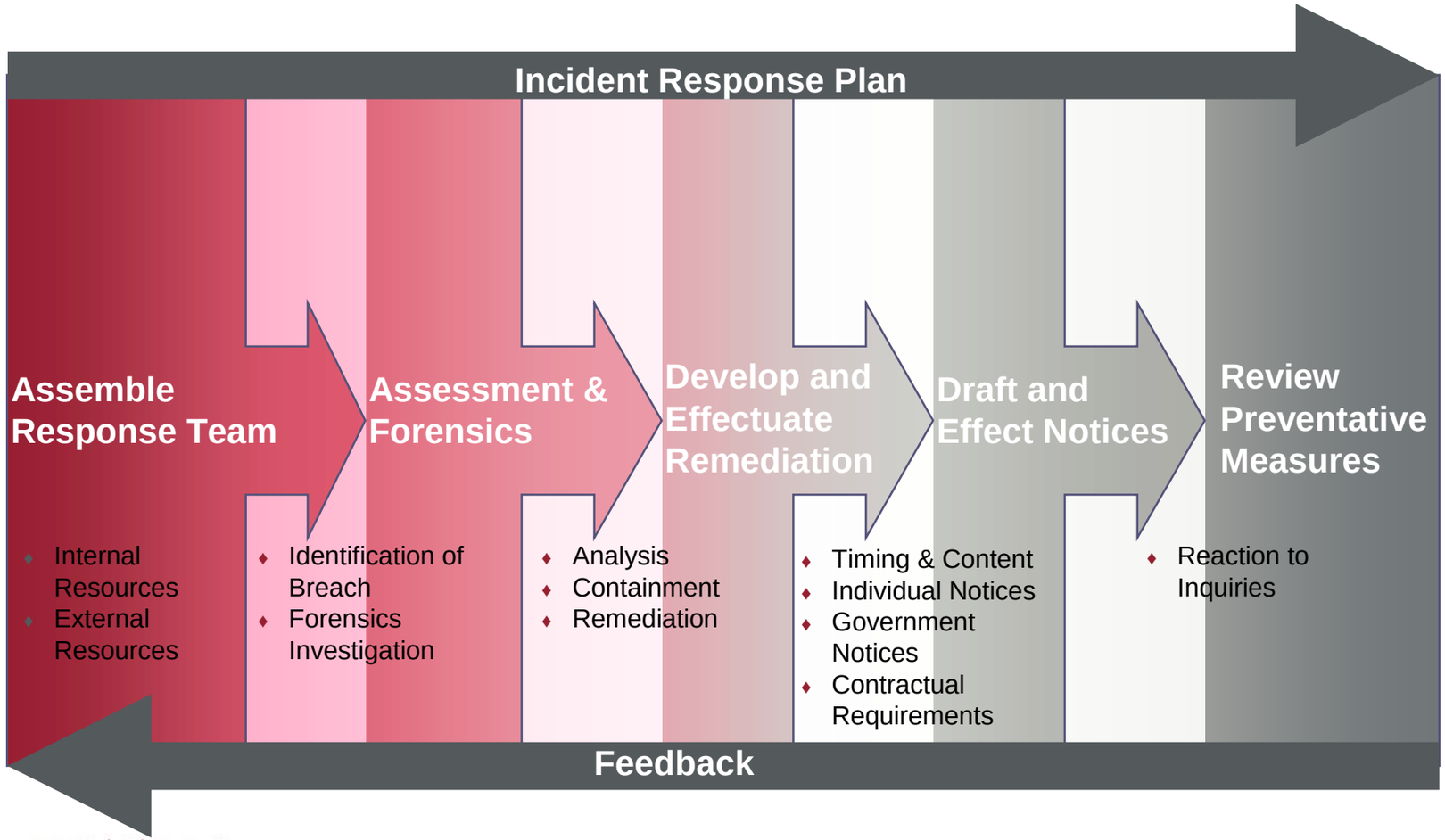
- Breach response is crisis management
- Planning is indeed indispensible.

Data Breach Response



EDWARDS WILDMAN

Data Breach Response



EDWARDS WILDMAN

Data Breach Response

- Incident Response Plan, continued
  - Other Considerations
  - Timeframes
  - Escalation Policies
  - Government, Media and Public Relations

Data Breach Response

- Global Complications

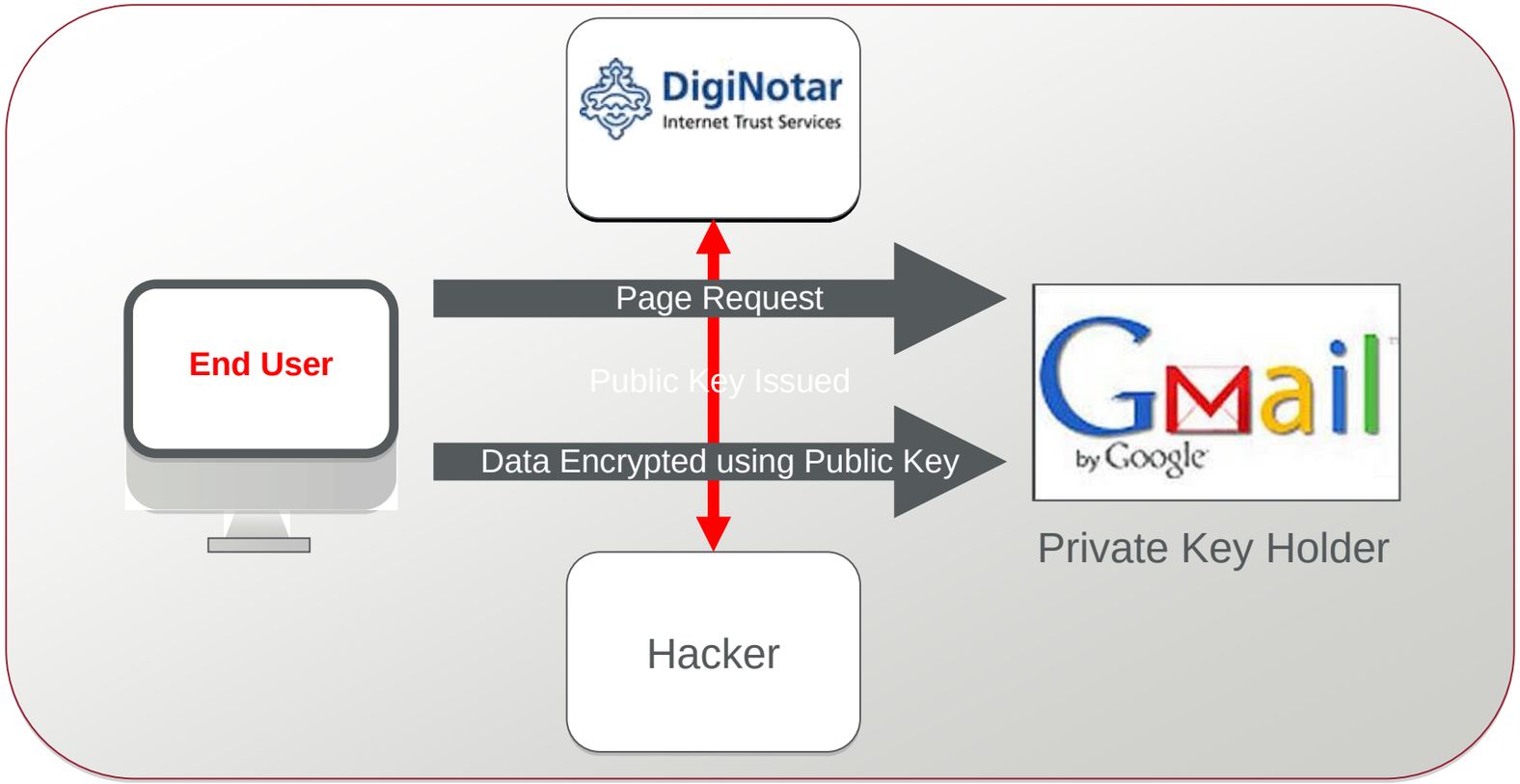
EDWARDS WILDMAN

Developments and Trends

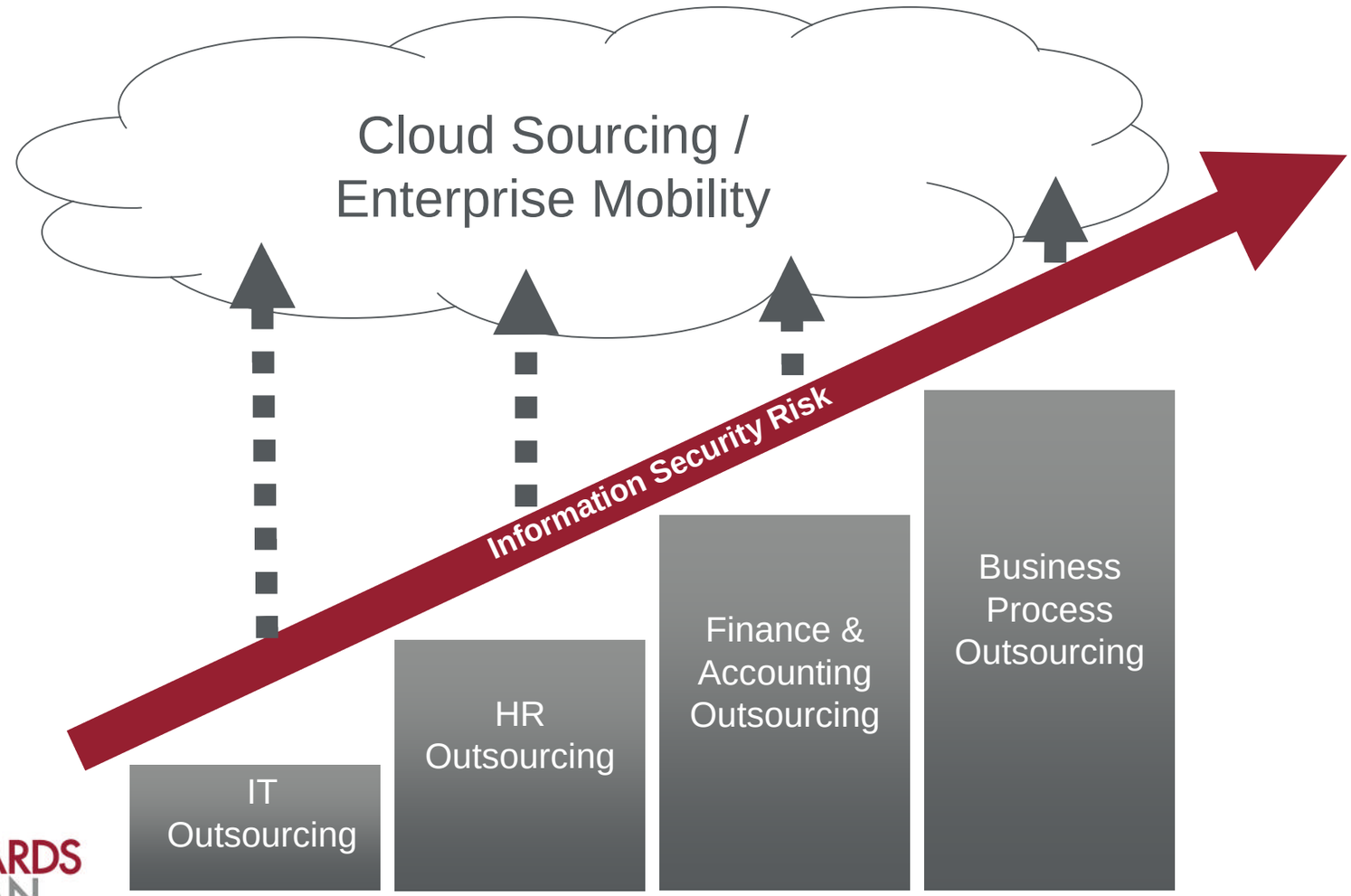
- Legislative Developments
  - EU
    - Electronic Privacy Directive
    - Data Protection Directive
    - Financial Services
    - Vendor Contracts
  - US
    - Proposed Federal Legislation on Breach Notification
    - Short notice requirements by regulatory authorities
    - Discrimination among affected individuals based on state requirements
    - Vendor Contracts

Developments and Trends

- Sophistication of Cyber Attacks



Developments and Trends



EDWARDS WILDMAN

Thank You & Questions

Theodore P. Augustinos
Partner
Edwards Wildman Palmer LLP
20 Church Street
Hartford
CT 06103
USA

+1 860 541 7710 (Direct)
taugustinos@edwardswildman.com

www.edwardswildman.com/taugustinos

Richard Graham
Partner
Edwards Wildman Palmer UK LLP
Dashwood
69 Old Broad Street
London
EC2M 1QS

+44 (0) 20 7556 4418 (Direct)
rgraham@edwardswildman.com

www.edwardswildman.com/rgraham

EDWARDS WILDMAN