Ninth National HIPAA Summit

The Leading Forum on Healthcare Privacy, Confidentiality, Data Security and HIPAA Compliance

Trends & Current Developments in Privacy for the CPO

September 12, 2004

P w C

Contact

Kim P. Gunter, J.D., LL.M.

Senior Consultant, Privacy Practice

(267) 330- 4026

Kim.P.Gunter@us.pwc.com

Agenda

Introduction & Background

Privacy Cross Industry Trends & Developments

PwC Governance Survey Results

What Others Are Doing . . .

Responsible Privacy Practices

Introduction & Background

Regulatory Risks, Heightened Enforcements & Financial Costs

- **New Laws.**
  - Since 1998, over 65 privacy laws in over 50 countries were passed in areas of financial privacy, data protection, telemarketing/fax, spam/web, and security breaches.
  - Since January 1, 2003, over 10 new privacy laws in the US were promulgated impacting financial services, pharmaceutical, health care, technology/media and virtually all organizations.
- **New Regulator Focus on Privacy & Data Protection.** Regulators are active globally, and asking tougher questions of privacy, data management, information security and control environments.
  - **Enforcements.** The FTC, FCC and state attorney generals all have all been aggressively inspecting and pursuing privacy breaches and lack or failure of safeguards.
  - **Expensive Class Actions.** The plaintiffs bar has begun using privacy as a new, fruitful area to pursue, in part, driven by a recent settlement of more than $60 million paid by a Fortune 500 retailer for allegedly inappropriately sharing customer information.

Breaches & Costs. Gartner projected that by 2006, 20-30% of Global 1000 will suffer exposure due to privacy mismanagement, and costs to recover from privacy mistakes will range from $5 -$20 million each.

Privacy & Business

Question: What keeps you up at night?*

CEOs and Boards of top e-Businesses

- Customer Loyalty
- Burn Rate / Profitability
- **Privacy**
- Sustainable Growth
- New Regulations
- Competition
- Staffing/Leadership

CEOs and Boards of Fortune 500s

- Shareholder Value
- Market Convergence
- **Privacy/Data Integrity**
- New Regulations
- Customer Loyalty
- Global Competition
- Technology Change

Privacy Impacts Bottom Line. A recent survey by Privacy & American Business of US consumers revealed that:

- 83% of US consumers will stop doing business if they hear or read a company is using information improperly;
- 91% of US Consumers would do more business with companies that have their privacy policies independently verified.

** Top 7 concerns for CEOs and Directors based on research by the Personalization Consortium*

The Privacy Paradox

Consumers:

- Consumers want a personalized experience and multi-channel availability
- But, they do not want to divulge personal information

Businesses:

- Businesses want to target & personalize to drive sales and build deeper, more valuable relationships
- But, that requires rich data profiles, and data collection raises privacy concerns

The Goal:

- Respectfully reach customers at the very time and place they need your product or service

Consequences of the Paradox . . .

consumers lie, complain and buy less

- Consumers lie
  - 67% of users admit providing false information
- They pressure legislatures
- Consumers shy away if they're unsure
  - 83% will stop doing business if they hear or read a company is using information improperly
  - 68% consider privacy before doing business
  - 58% would recommend companies who protect data
  - 91% would do more business with companies that have their privacy policies independently verified

Consumers Are Skeptical, Especially of Health Care

- **Consumers don't trust health care companies**
  - **Only 12% trust pharmaceutical companies with PHI**
  - Only 33% trust health plans & government programs to maintain confidentiality
  - 20% believe a health care provider, insurance plan, government agency or employer has improperly disclosed PHI
    - 50% say it resulted in personal embarrassment or harm
- **Consumers don't share**
  - 67% never share health information
  - 21% rarely share
  - 10% sometimes share
  - Only 2% often share health-related information (e.g., medical history or prescriptions) on the Internet
- **Healthcare must inspire trust -- 90% think it's very important that**
  - Health care providers and pharmacies establish effective privacy policies and do what they promise
  - Privacy policies be reviewed by third parties

For a consumer, “Privacy is What You Call It When You Do It Wrong”

- Privacy is an important means to build a “trusting” relationship, not just a compliance issue from Legal
- Turn privacy into a competitive advantage and a long-term customer value
- Learn from the mistakes of others
  - Hindsight is 20/20
  - Don't be a case study

Privacy Cross-Industry Trends & Developments

P w C

Privacy Cross-Industry Trends & Developments

- **New Laws; Marketing and Sales** – many new domestic and international privacy laws dramatically impact financial services and circumscribe the use of telemarketing, email, faxes, the web and wireless devices for business-to-business and business-to-consumer communications.
- **Security –** laws and new regulatory trends/enforcements affecting pharmaceutical companies and financial institutions require specific security administrative, technical and physical safeguards to protect sensitive information be put in place.
- **Globalization; Data Management –** the recent effectiveness of several EU and other international privacy directives and the political attention paid to data protection and outsourcing practices has heightened the desire of many organizations to focus on international employee, customer, and vendor, privacy & data management.
- **Governance, Risk & Compliance –** As privacy has become viewed as a cross-enterprise compliance issue impacting all business units, many companies are reconsidering how the privacy function within an organization is structured, staffed and funded to most effectively manage risks and ensure compliance.

The Last 2 Years in Privacy – Selected Enactments

Virtually every communications channel has or will be impacted:

- **E-Mail –** CAN-SPAM Act (effective 1/1/04); 2003 International legislation (e.g., EU, AU)
- **Web** - CA Online Privacy Law (effective 7/1/04)
- **Wireless –** TCPA; TRUSTe and DMA guidelines for wireless marketers
- **Telemarketing -** Telemarketing Sales Rule (DNC & changes effective 10/1/03;1/1/05)
- **Fax –** Telephone Consumer Protection Act (TCPA verifiable consent by 1/1/05; states)
- **Global –** Privacy and Electronic Communications Directive (2002/58/EC)

Data Protection Legislation

- California Information Practice Act (SB 1386; effective 7/1/03)
- California Personal Information: Disclosure to Direct Marketers Act (SB 27; effective 1/1/05)

Pharmaceutical and Health Care Industry Specific Privacy and Data Protection Legislation

- HIPAA Security Provisions (effective 4/05)
- Various State prohibitions on pharmaceutical sales and marketing practices (TX SB 11; CA AB 715)
- EU Clinical Research Directive (Directive 2001 / 20 / EC, implementation deadline 5/1/04)

Government Specific Privacy and Data Protection Legislation

- eGov Act (effective 2/03; PIAs required 12/04)

Pending Laws and Rules

- Jobs for America Act (Daschle/Kerry)
- U.S. Workers Protection Act (Dodd)
- Various US state proposed outsourcing laws (CA, NJ, others)
- US Notification of Risk to Personal Information Act (SB 1350)
- Interagency Guidance on Response Programs for Unauthorized Access to Customer Information
- Reporting on Cybersecurity by SEC registered corporations
- Congressional (House Committee on Technology, Information Policy); DHS
- Corporate Information Security Accountability Act of 2003

Foreign Legislation (4 years)

- Foreign Encryption Laws (U.S., Canada, France, Israel, Russia, China, etc.)
- EU Directive 95/46/EC - The Data Protection Directive (1995)
- Germany Federal Data Protection Law (1997)
- Switzerland Federal Law on Data Protection (2000)
- Canada Personal Information Protection & Electronics Documents Act (2000)
- Australia Privacy Amendment (Private Sector) Act (2000)
- United Kingdom Financial Services Authority – Systems & Controls (2002)
- Japan Personal Data Protection Law (2003)
- Ireland Data Protection Act (1998 revised 2003)

Heightened Enforcement & Brand Peril

Illustrative Enforcements, Penalties & Legal Actions

FTC investigated drug industry advertising practices/privacy violations – targeted promotional letters sent by pharmacies to customers and paid for by pharma.

FTC - Web & Email – Needed safeguards to prevent unauthorized/unintentional disclosure of sensitive personal information collected from Prozac.com.

FTC – Web/Information Mgmt – Must implement, test and monitor safeguards to control potential risks identified in a risk assessment.

Data Management – $60+ million class action settlement for improper data sharing

FCC & State AGs – Do Not Call -- Enforcements, in part for revenue.

State AGs – Massive Vendor Data Leakage – multiple clients.

State AGs – Email Database Growth – E-append program mismanagement.

Private Action – Email – First of floodgate of actions under CAN-SPAM by IASPs.

Class Action – Marketing Practices -- Eli Lilly secured signed blank letters from doctors whose patient had taken Prozac. Walgreens mailed free trials.

Class Action – 3rd-Party Vendor - Weld v. CVS -- Wrongful disclosure of medical information by CVS to direct-marketing company in patient-compliance program.

OCR/State AGs – HIPAA – Thousands of complaints; set to commence actions.

Liability Case Studies

- **FTC Settlement with Eli Lilly**
- **Private Rights of Actions**
- **Predicted HIPAA Risk Areas**

Eli Lilly Settles FTC Charges Concerning Security Breach

- Unauthorized and unintentional disclosure of sensitive personal information collected from consumers through its Prozac.com and Lilly.com Web sites
- Lilly to implement an information security program to protect consumers' privacy

"Eli Lilly and Company respects the privacy of visitors to its Web sites, and we feel it is important to maintain our guests' privacy as they take advantage of this resource."

"Our Web sites have security measures in place, including the use of industry standard secure socket layer encryption (SSL), to protect the confidentiality of any of Your Information that you volunteer; however, to take advantage of this your browser must support encryption protection (found in Internet Explorer release 3.0 and above). These security measures also help us to honor your choices for the use of Your Information."

Eli Lilly Email – We Are All Only One Email Away . . .

From: Mail_usmail-welcome@lilly.com

Sent: Wednesday June 27, 2001 8:37 PM

To: [redacted]@ aol.com, [redacted]@hotmail.com, [redacted]@yahoo.com, [redacted]@juno.com, [redacted]@earthlink.com, [redacted]@lilly.com, [redacted]@webtv.net, [redacted]@hotmail.com [redacted]@gateway.net, [redacted]@home.com, [redacted]@dotnow.com, etc.

- Subject: Medi-Messenger
- Dear Medi-Messenger User:
- We're listening! This week Eli Lilly and Company relaunched Prozac.com with a new navigation and feel. Based upon feedback from consumers like you, we have discontinued our Medi-Messenger e-mail reminder service. We are appreciative of your comments, and hope this does not cause any inconvenience to those of you who were using this feature.

Eli Lilly settlement

- FTC complaint alleges:
  - Lilly's claim of privacy and confidentiality deceptive because company failed to maintain or implement internal measures appropriate under the circumstances to protect sensitive consumer information

- According to the FTC, Eli Lilly failed to:
  - provide appropriate training for employees
  - provide appropriate oversight and assistance
  - implement appropriate checks and controls on the process

- FTC Order:
  - Bars misrepresentations
  - Requires Lilly to establish and maintain an information security program

Demystifying an Information Security Program

- Information Security Program
  - designate appropriate personnel to coordinate and oversee the program
  - identify reasonably foreseeable risks and address these risks in each relevant area of its operations
  - conduct an annual written review by qualified persons
  - adjust the program in light of any recommendations from reviews, findings from ongoing monitoring, or material changes
- Recommendations:
  - Make sure you know what information your company collects, how it is stored, and how it is used, and write your policy accordingly
  - Use a team approach, including representatives from legal, marketing, IT, and Web design to: i) Determine current information practices; ii) Assess what laws may apply, and iii) Develop and draft a clear privacy policy
  - Educate your employees, develop training materials

"Litigation 101"

Sensitivity of the information

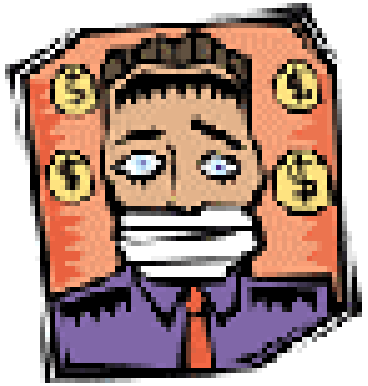
leads to emotionally-charged

plaintiffs . . .

which leads to

high-stakes deterrence:

$$$$$$$$$$$$$$$$$$$$



… And then came along HIPAA!!

Avoiding Litigation and Trouble

The Top HIPAA Threats

(1) *Business Associates* **-- Medical data abuses or breaches by business associates**

(2) *Broken Promises* **-- Failure to follow one's own privacy policies and procedures**

- *E.g., Marketing Rules*

(3) *Security* **-- Inadvertent mass disclosure due to poor security**

Risk Area 1 -- Business Associates

Does HIPAA "Directly" Apply to You?

- Covered Entities
  - Healthcare providers who transmit individually-identifiable health information in electronic form
  - Health plans (including self-funded health plans)
  - Healthcare clearinghouses
- Business Associates -- entities performing activities "on behalf of" covered entities "Provides legal, actuarial, accounting, consulting, data aggregation . . . management, administrative, accreditation, or financial services to or for such covered entity . . . involv[ing] the disclosure of individually identifiable health information from such covered entity . . . or from another BA."
- Hybrid Entities

Risk Area 1 – Obligations of/Breaches by Business Associates

Covered entities – to an extent, are their brother's keeper

- Must obtain satisfactory assurances that the B.A. will appropriately safeguard the information
- No automatic liability for violation by B.A., but C.E. can't avoid responsibility by intentionally ignoring problems with B.A.

Pre-HIPAA Example: Weld v. CVS

- Alleged wrongful disclosure of medical information by CVS to direct-marketing company in patient-compliance program.
- CVS and Elensys Care Services Inc. sent refill reminders and drug ads to CVS pharmacy customers.
- CVS scanned databases for drug company criteria. Mailings sent on CVS letterhead; paid for by the drug manufacturers.

Risk Area 2 –
Failure to Follow One's Privacy Policy/Procedures

HIPAA Requirements:

- HIPAA requires covered entities to adopt policies and procedures governing the protection of patient privacy.
- HIPAA also requires Notice of Privacy Practices be given and patient's to have right to request restrictions on use and disclosure of their PHI.

Violations of a privacy policy likely to result in state law claims for:

(i) negligence, (ii) breach of contract or (iii) misrepresentation

- *Aetna* – Health insurance claim forms from Aetna blew out of a truck on the way to a recycling center and scattered on I-84 in East Hartford during the evening rush hour. The forms should have been shredded under company policy.
- *Arkansas Dept. of Human Services (DHS)* – Confidential Medicaid records were disclosed during the sale of surplus equipment twice in 6 months violating document destruction policy.
  - 10/01 - DHS's sale of surplus computer storage drives with Medicaid records.
  - 4/02 - DHS sold a file cabinet with Medicaid files inside.

Kentucky police told it's legal to name injured

- Kentucky attorney general ruled that HIPAA does not give police the legal authority to withhold from reports the names of people injured in accidents.

Official says records leak violated federal rules

- Leaked patient records include information about seven patients recently treated by firefighter-medics.
  - The records detail instances of substandard care administered by firefighter-medics
    - Open records laws
      - If not a CE – do not have to follow HIPAA
      - If a CE & disclosure is mandated, may comply with law
      - If a CE & disclosure is permitted, then not required by law, not permissible

No Charges against doctor who refused to draw blood

- Doctor refused to take blood sample for blood-alcohol level from a homicide suspect without man's consent in Minneapolis where suspect refused to voluntarily provide sample

Risk Area 2 – Marketing Under HIPAA'S Privacy Rule

HIPAA Requires:

- Communication about a product or service that encourages recipients to purchase or use it - Must disclose remuneration to the covered entity from a third party
- Patient authorization is required for use or disclosure of PHI for marketing, unless an exception is available

Exceptions:

- Face-to-face encounters
- Promotional gift of nominal value
- Communications describing health benefits
- Communications to further treatment, for case management or care coordination, or to recommend alternative treatments or providers Prescriptions and referrals; Disease management and wellness programs; Prescription reminders; Appointment notifications
- Note: Under these exceptions, covered entity may market health-related products and services on behalf of third parties

Risk Area 2 – Hindsight is 20/20

Walgreens

- Unsolicited samples of Prozac were distributed, some in a hand-addressed manila envelope from Walgreens drugstore
- Eli Lilly secured signed blank letters from doctors whose patient had taken Prozac (even if not currently taking it)
- Walgreens mailed a one-month free trial of Prozac Weekly with a "Dear Patient" form letter -- "Congratulations on being one step closer to full recovery"

- Action
  - A woman recipient filed a class-action lawsuit stating that Walgreens, a local hospital, three doctors, and Prozac maker Eli Lilly misused her patient information and medical records and invaded her privacy
  - Woman said she once took Prozac many, many years ago, but had a bad side effect and does not take currently; moreover, although she lives in and received the sample in Florida, original prescription was filled at a Walgreens in New England

But what about today?

Privacy Rights Group Sues Albertsons for Illegally Selling Pharmacy Customers' Information

The Privacy Rights Clearinghouse

- Charging Albertsons, 2nd largest supermarket chain & 5th largest drugstore retailer in US, with violating the privacy rights of thousands customers by illegally selling their confidential prescription information to drug companies.
- Aventis, Shering-Plough, AstraZeneca, TAP Pharmaceutical Products, Eli Lilly, Novartis, Wyeth, Proctor & Gamble, Teva Pharmaceutical, GlaxoSmithKline, Merck, Allergan, Bristol-Meyers Squibb, Pfizer, Galderma, and Otsuka America Pharmaceuticals.
- **California** (other states) "reminder" communications are: 1) deceptive and false - conceal the true motive of raising increased revenue for the drug companies and pharmacies involved, and are not just a friendly reminder to refill a prescription; 2) communications violate California laws that specifically safeguard medical confidentiality absent written authorization from the customer; 3) practices ultimately violate state privacy laws by disregarding a citizen's right to just be left alone.

Risk Area 3 -- Security -- It's 10 o'clock, do you know where your data is?

- HIPAA Security standard requires reasonable and appropriate administrative, technical, and physical safeguards to:
  - ensure the integrity & confidentiality of information;
  - protect against any reasonably anticipated
    - threats or hazards to the security or integrity of the information; and
    - unauthorized uses or disclosures of the information; and
  - otherwise ensure compliance by officers and employees.

Risk Area 3 – Pre-HIPPA Security Breach Examples

- *National Enquirer:* "Singer Tammy Wynette needs liver transplant."
  - Information incorrect, and obtained illegally. Settled out of court.
  - Pittsburgh University Medical Center employee who faxed singer's medical records to tabloid for $2,610 pleaded guilty to wire fraud and sentenced to six months in prison.

- *University of Montana*: Hundreds of psychological records of 62 children and teenagers were accidentally posted on UM web site for 8 days.

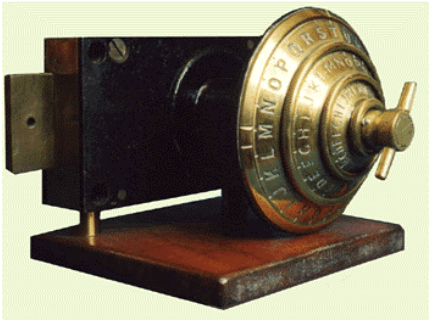
- *Medlantic Healthcare Group:* Part-time, unauthorized employee accessed and discussed with co-workers a patient's HIV status. $250,000 in damages.

- *Eli Lilly & Company.*

Risk Area 3 – Pre-HIPPA Security Breach Examples

Goals:

- Protecting a Trusted Brand
- Managing Risks
- Building Long-Term Value



Means:

- Managing new and complex legislative and regulatory requirements
- Addressing increased customer and governmental scrutiny
- Designing and implementing personal information management practices that:
  - differentiate the organization from its competitors
  - Enable new business processes, marketing channels and relationship-building techniques

Edit View Favorites Tools Help

http://www.usdoj.gov/usao/waw/press_room/2004/aug/gibson.htm

Web Search Rank: 2,430

UNITED STATES ATTORNEY'S OFFICE
Western District of Washington

PRESS ROOM

August 19, 2004

SEATTLE MAN PLEADS GUILTY IN FIRST EVER CONVICTION FOR HIPAA RULES VIOLATION

RICHARD W. GIBSON, age 42, of SeaTac, Washington pleaded guilty today in federal court in Seattle to wrongful disclosure of individually identifiable health information for economic gain. This is the first criminal conviction in the United States under the health information privacy provisions of the Health Insurance Portability and Accountability Act

admitted that he obtained a cancer patient's name, date of birth and social security number while GIBSON was employed at the Seattle Cancer Care Alliance, and that he disclosed that information to get four credit cards in the patient's name. GIBSON also admitted that he used several of those cards to rack up more than $9,000 in debt in the patient's name. GIBSON admitted he used the cards to purchase various items, including video games, home improvement supplies, apparel, jewelry, porcelain figurines, groceries and gasoline for his personal use.

The Government and GIBSON agreed as part of the Plea Agreement that GIBSON should be sentenced to a term of 10 to 16 months. Under these terms, the Court could order that the term be served either wholly

SEATTLE MAN PLEADS GUILTY IN FIRST EVER CONVICTION FOR HIPAA RULES VIOLATION

GIBSON admitted that he obtained a cancer patient's name, date of birth and social security number while GIBSON was employed at the Seattle Cancer Care Alliance, and that he disclosed that information to get four credit cards in the patient's name. GIBSON also admitted that he used several of those cards to rack up more than $9,000 in debt in the patient's name. GIBSON admitted he used the cards to purchase various items, including video games, home improvement supplies, apparel, jewelry, porcelain figurines, groceries and gasoline for his personal use. GIBSON was fired shortly after the identity theft was discovered.

Internet

Identity Theft

- **FTC Complaints:**
  - 2000: 31,000
  - 2001: 86,000
  - 2002: 162,000
  - 2003: 214,000
  - Top consumer fraud complaint in 2002
  - 30% growth predicted going forward
  - Estimated 9.9 million victims in 2002
- **Average impact:**
  - $1500
  - 175 hours of clean up
  - credit disruptions
- Cost to consumers = $5 billion
- Cost to industry = $48 billion
- 42% of complaints involve credit card fraud

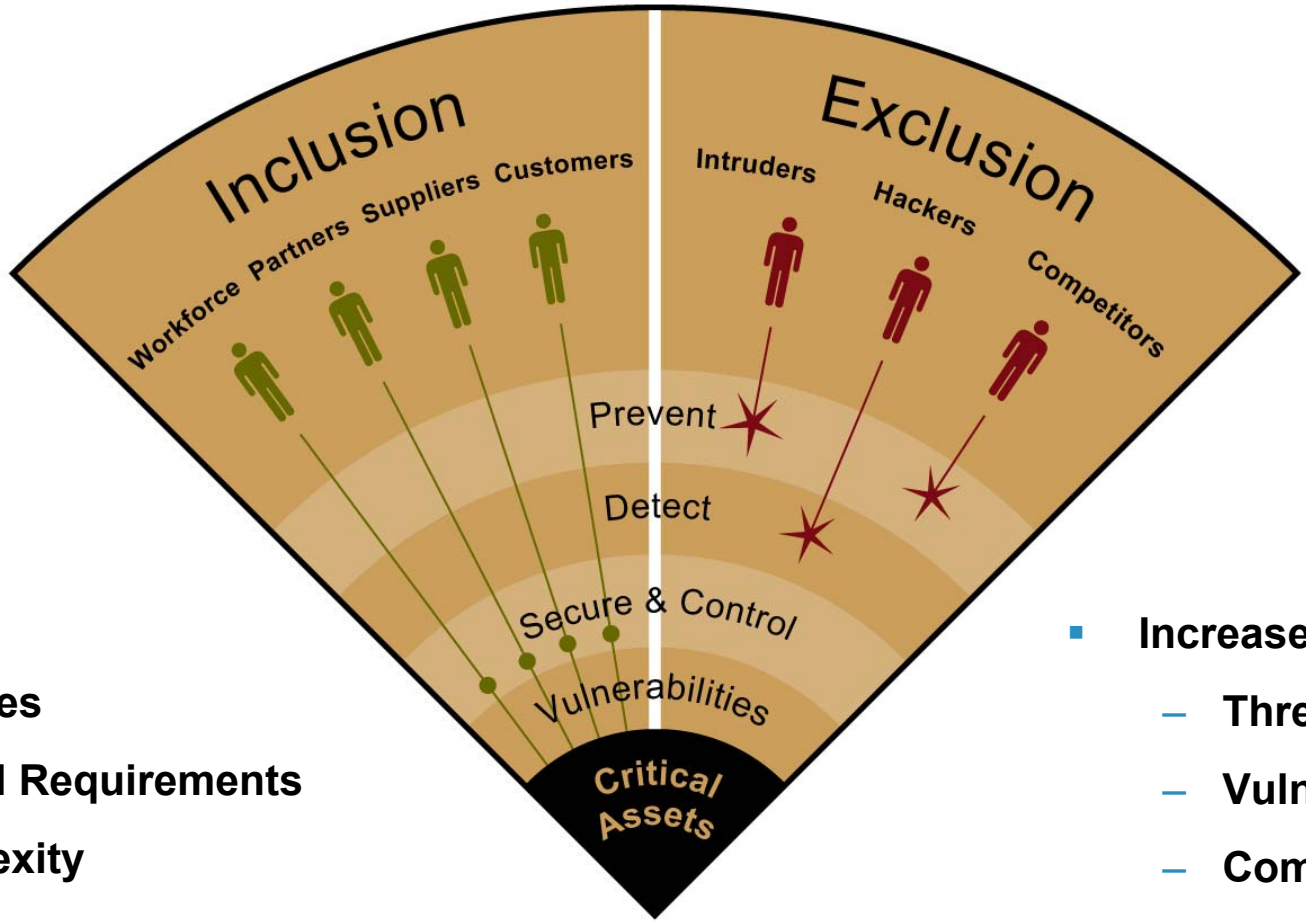
Identity theft coverage now available

United States v. Richard Gibson

- Charge: Wrongful Disclosure of Individually Identifiable Health Information
- Elements of Offense:
  - Disclosed to another person IIHI relating to an individual
  - Made the disclosure knowingly;
  - Made disclosure for non-permitted purposes;
  - Made disclosures with intent to use IIHI for personal gain.
- Penalty
  - Imprisonment of up to 10 years
  - Fine of up to $200,000
  - Supervision of up to 3 years
  - Probation of up to 5 years
  - Penalty Assessment of $100 to be paid at or before sentencing

But who's the covered entity?

Security -- Challenges of Inclusion and Exclusion



- **Increased:**
  - **Identities**
  - **Control Requirements**
  - **Complexity**

- **Increased:**
  - **Threats**
  - **Vulnerabilities**
  - **Complexity**

The Global Picture

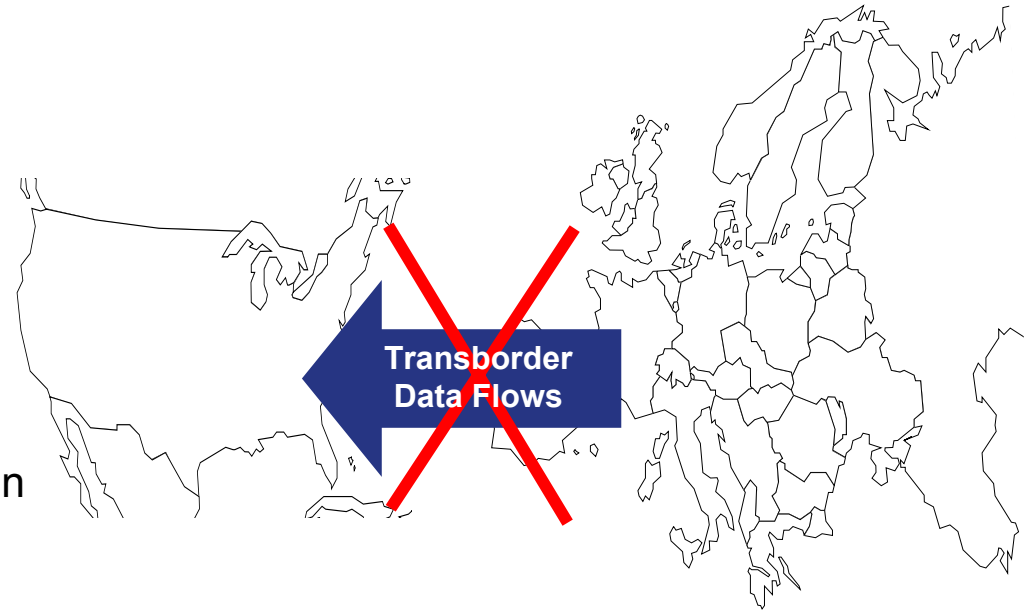
Sample of Data Protection Laws Around the World

- **The EU Data Protection Directive & comparable privacy legislation by 25 member states**
  - Based on -- OECD Organisation for Economic Cooperation and Development 7 principles
  - Notice, Choice, Onward Transfer, Security, Data Integrity, Access, Enforcement
- Foreign Encryption Laws (U.S., Canada, France, Israel, Russia, China, etc.)
- Switzerland - Federal Act on Data Protection (1992)
- Hungary - Protection of Personal Data and Disclosure of Data of Public Interest (1992)
- Canada - Personal Information Protection and Electronic Documents Act (2000)
- Argentina - Personal Data Protection Act (2000)
- Chile - Law for the Protection of Private Life (1999)
- Australia - Privacy Amendment (Private Sector) Act (2000)
- Hong Kong - The Personal Data (Privacy) Ordinance (1996)
- New Zealand - Federal Privacy Act (1993)
- Japan Personal Data Protection Law (2003)
- Ireland Data Protection Act (1998 revised 2003)
- Czech Republic – Act on Protection of Personal Data (2000)
- and more…

Recent privacy legislation (Australia, Hong Kong, Canada) trending toward EU-style privacy regulation and away from U.S. sectoral/data elements-based models

EU Data Protection Directive
Main Requirements

- Information processed lawfully & fairly
- Legitimate, specified and explicit data processing
- Information kept accurate and up to date
- Individual rights to access their information
- Confidentiality & security of information



KEY IMPLICATION -
Restricts the transfer of personal information to 3rd countries that do not have "adequate" protection.

The US *does <u>not</u>* meet this "adequacy" requirement

How will EU data be legally accessed, transferred and warehoused in the U.S.?

EU Privacy Enforcement Actions

- May 2001 - Spanish government fined Microsoft for improperly transferring employee data from Spain to a web server located in the U.S. Microsoft was able to have fines reduced from several hundred thousand dollars to about $57,000
- April 2001 - Madrid court ruled against NCR for dismissing an employee on the basis of information obtained when the employee's computer was remotely accessed from the U.S. Besides violating the employee's privacy rights, the court found that the company had breached legal protections for union activities.
- April 2001 - Four Spanish directors of Deutsche Bank faced imprisonment over Company's unlawful interception of employee e-mail. A worker fired by the bank on the basis of information contained in his e-mail had previously won a case overturning the dismissal, and was given the right to seek the prison sentences.
- June 1997 – Telefonica paid $660,000 to the Spanish government to settle cases of data misuse because they provided information from their subscriber database to banks, direct marketing companies and Reader's Digest.
- May 1995 - Swedish DPA instructed American Airlines to delete all health and medical details about Swedish passengers after each flight, unless "explicit consent" could be obtained. AA was also restricted from transferring customer information from Sweden to its SABRE reservation system in the United States. American Airlines lost the first round of its lawsuit challenging the law - the court also ruled that the U.S. didn't have adequate privacy protection.
- Sweden reportedly prohibited the transfer of a credit registry database from Dun & Bradstreet's Swedish affiliate back to the D&B U.S. affiliate on the grounds that the registry contained financial information on Swedish citizens. According to reports, only after joining Safe Harbor did D&B guarantee uninterrupted data flow between its affiliated entities.

Globalization

- **Global Data Management –** the recent effectiveness of several EU and other international privacy directives and the political attention paid to data protection and outsourcing practices has heightened the desire of many organizations to focus on international employee, customer, and vendor, privacy & data management.

- **More Companies are considering international data transfer and Safe Harbor (or exceptions and alternatives), for several types of data:**

➢ **The environment for conducting clinical trials is changing – Globalization & Increasing Outsourcing to CROs and Others**
  - The industry faces continued increasing pressure to manage costs, including compliance costs, and safely accelerate clinical trial completion to maximize patent value and exclusivity.
  - Increased delegation of study design and execution to outsourced service providers (i.e., CROs & SMOs).
  - Increased globalization of research conduct, especially given dearth of study subjects.
  - Data protection and integrity concerns must be mitigated as new technologies are adopted (electronic data collection (EDC), electronic submissions/validation, adverse event reporting).

➢ **Unique privacy issues involved in the employer/employee relationship:**
  - Performance reviews, evaluation data - is this personal information as defined by law?
  - Employee choice over information handling - how much is too much?
  - Obtaining employee consent for use of data
  - Use of Social Security Number or other national identifiers
  - Access to health-related information through benefit plans, onsite medical facilities
  - Increased scrutiny over surveillance of employees in the workplace and employee email, Internet use, hard drives

Joining the Safe Harbor

- **Companies Include:**
  - Disney Consumer Products, Microsoft, General Motors, Bacardi, PepsiCo, Polo Ralph Lauren, Publishers Clearing House
- **Safe Harbor Benefits**
  - All 25 Member States of the EU will be bound by EU Commission's finding of adequacy;
  - Uninterrupted data flows & waiver of country data transfer pre-approval requirements;
  - Claims brought by EU citizens against US companies will be heard in the US subject to limited exceptions.

The safe harbor framework offers a simpler and cheaper means of complying with the adequacy requirements of the Directive.

- **Safe Harbor Drawbacks**
  - Failure to comply with the Safe Harbor requirements could expose an organization to federal civil and criminal liability;
  - Safe Harbor companies must annually certify verification of ongoing compliance.
- **Key Factor to Success**
  - Ongoing safe harbor compliance costs vary widely in part based on the soundness of the safe harbor infrastructure put in place originally. Transparency and sustainability are critical features to consider and install to ensure an effective compliance process exists in years and beyond.

Other U.S. Responses to EU Data Directive

- Model Contracts
  - do not require public registration
  - governed by individual Member State law
  - more restrictive around purpose
- Ad Hoc or Processor Contracts
  - require DPA approval, including additional purpose
  - individually negotiated by country / exporter
- Consent
  - requires “unambiguous” consent from employees / individuals
  - explicit consent for sensitive data, and data transfers outside EU
- Binding Corporate Rules
  - alternative to other mechanisms allows for more appropriate rules based on organization structure
  - allows coordinated DPA approval

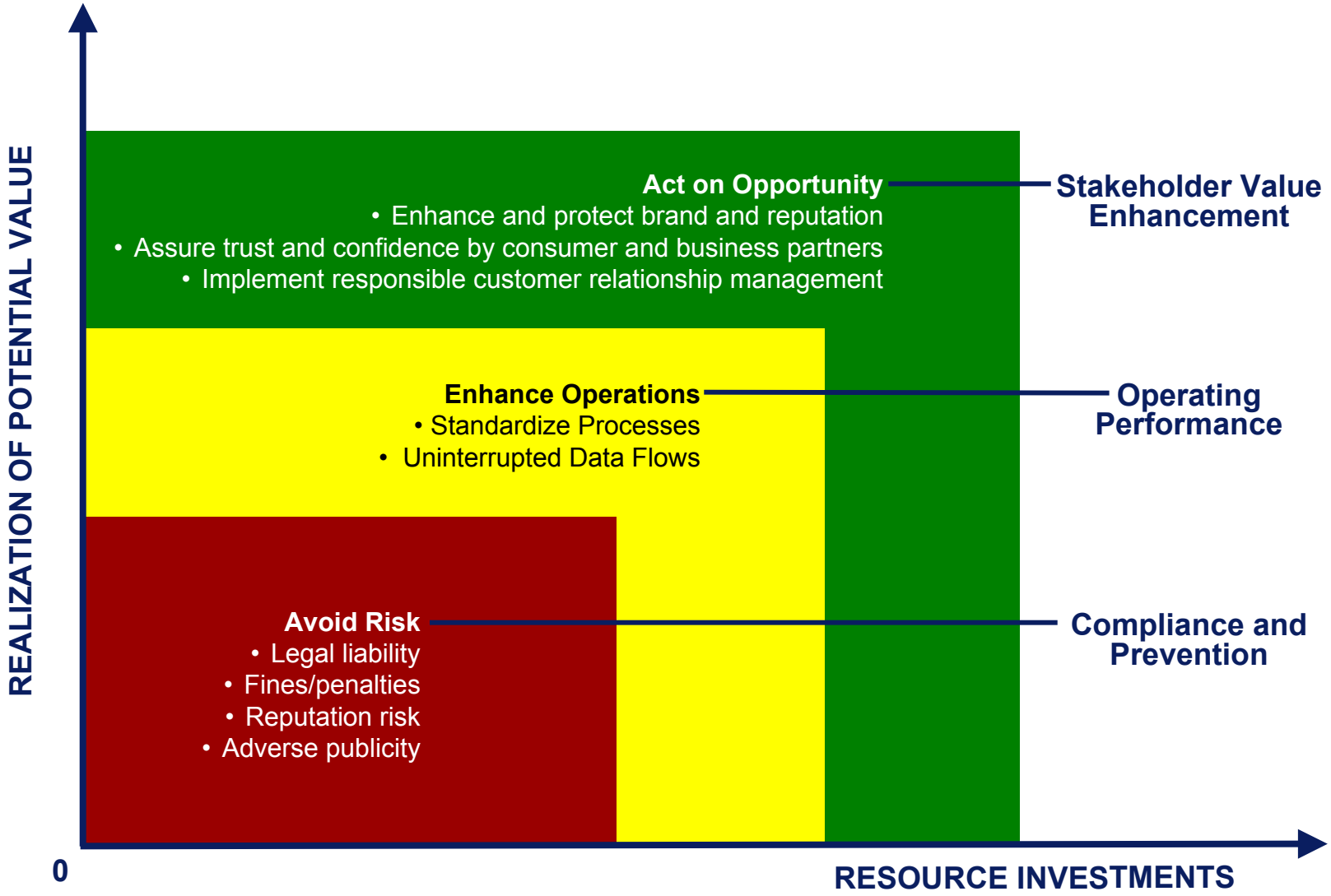
Difficult Data Management Issues

Common Issues Requiring New Models & Enterprise-Wide Solutions

- Enterprise Risk-Based Privacy Management Framework
- Data Inventory, Flow Mapping & Risk Assessment
- Enterprise-Wide/Global Privacy Principles, Policies, Controls, Resources & Training
- Cross-Channel, Centralized, Enterprise-Wide Preference Management & CRM Strategies
- Enterprise-Wide Compliance Assessment, Monitoring/Testing, Auditing & Benchmarking
- 3rd Party Sharing, Outsourcing and Vendor Management (Assessment/Monitoring & Contracting)
- Privacy Impact Assessment Process
- Data Tagging and Tracking (Auditing/Forensic Uses)
- Need for a Data Tsar--US Version of EU Data Controller
- Authentication and Identity Management
- Privacy Governance/Infrastructure and Relationship to the Business, Legal/Risk Management, and Technical and Physical Security

- **Enterprise and global** approaches sought
- **New models** promoting privacy, security, integrity, values-based culture and appropriate checks and balances
- People, process and technology **strategically aligned** to achieve enterprise privacy governance, risk & compliance management objectives
- **Leveraging technology** to manage complexity
- Investigate these trend to **drive more efficient and better controlled business processes** (i.e., performance improvement).

Privacy Strategy Spectrum



PwC Governance Survey Results

P w C

1. CPO Position

- ***Maturation of the Privacy Officer Position***
  - 83% of respondents indicated they hold the Chief Privacy Officer or equivalent position
    - The other titles included Chief Compliance Officer, Integrity Assurance and Information Protection.
    - The P&AB 10/2001 survey of privacy professionals noted 61% of respondents held a title of Chief Privacy Officer or an equivalent.
    - In contrast, the 2003 CIO / PwC survey of IT professionals indicated only 27% of financial services companies and 18% of non-financial services companies employed a Chief Privacy Officer, Data Protection Officer or similar.

2. Reporting Structures

- ***Varying structures exist based on business model and culture:***
  - Legal 56%, Compliance 22%, Government Affairs 9% with other structures being split evenly.
- ***Greater Alignment with Information Security and the Business***
  - At least one-quarter discussed the idea of reorganizing the privacy function to better coordinate with information security function through either direct reporting, via cross-functional committees or indirect reporting between the two functions.
  - A number of CPOs acknowledged the need for closer/better relations with business units.
- ***Dual Reporting is an emerging trend***
  - 27% had an existing dual reporting line that included various combinations of Legal/ Compliance/Risk Management/CIO and CFO.

3. Top Priorities Going Forward

Privacy	Security
Training	Training
Local and Global Regulatory Compliance	Risk / Vulnerability Assessments
Vetting and Monitoring Third Party Vendors	Identity Management

4. Privacy Office & Budget

Growth in Privacy FTE Headcount (and Consultants)

	CPO Survey (2003)	P&AB (2001)
Count	**FTE**	**FTE**
None	17%	7%
1	11%	37%
2-4	28%	40%
5-9	33%	16%
10+	11%	0%

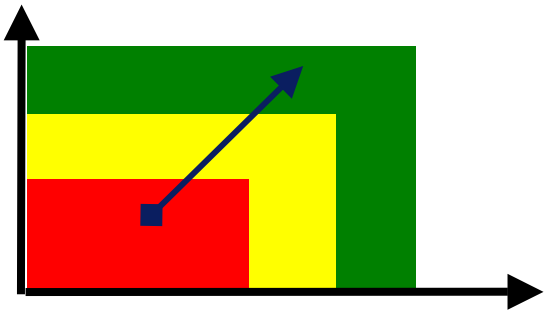
Annual Project Budgets

Budget Range	Privacy
No Response	23%
0 – $ 500,000	11%
$ 500,000 – 1 million	22%
$ 1 – 5 million	33%
$ 5 – 10 million	11%
$10 – 500 million	0%

What Others are Doing . . .

What Others are Doing…

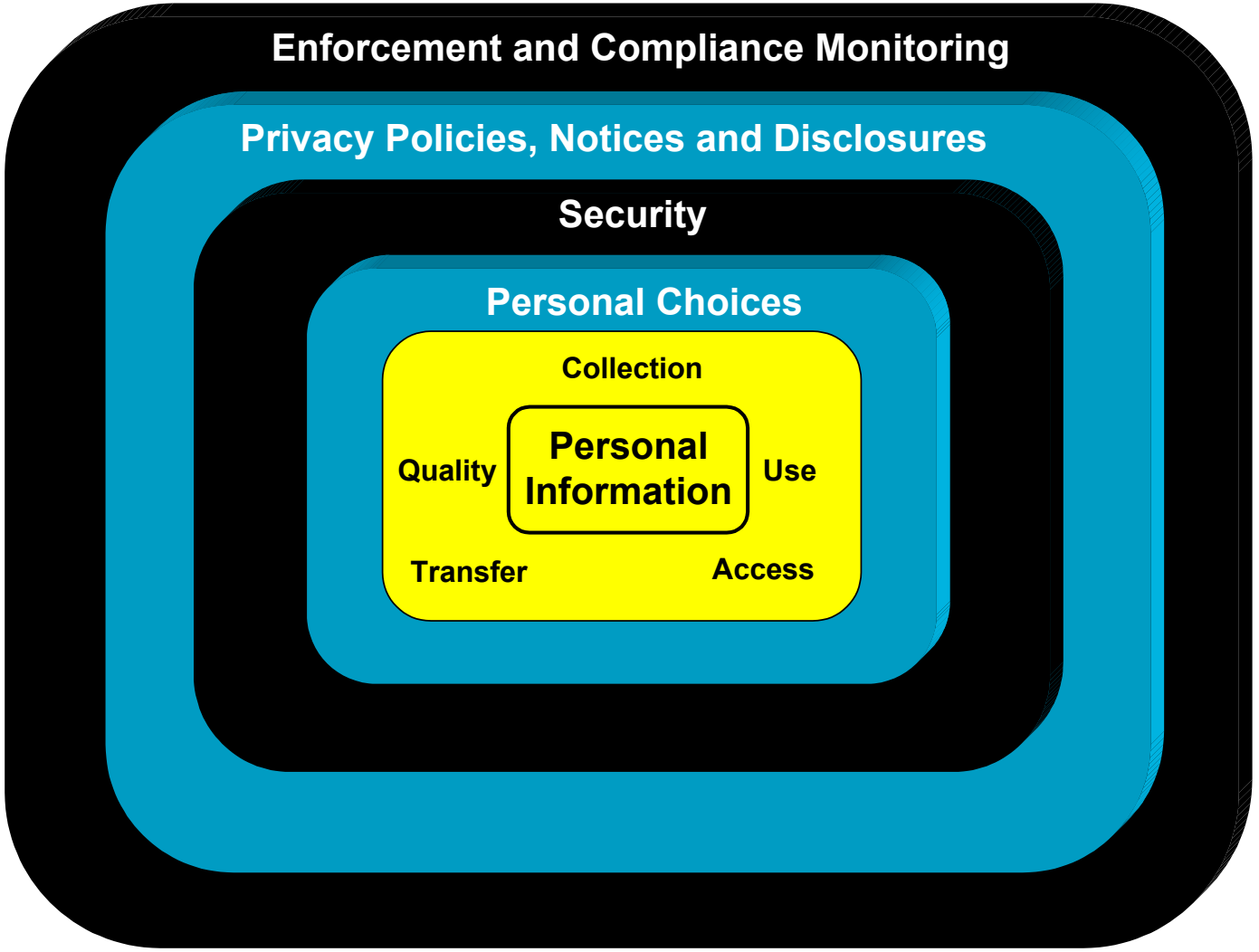
- Reconsidering and/or Assessing
  - Sales & Marketing Communications
  - Clinical Privacy Compliance
  - Global Context -- EU Safe Harbor, Model Contracts
  - 3rd Party Vendor Assessments
  - Employee Privacy Policy & Data Management
  - Privacy Risk Scorecards (Risk Based Overview with Best Practices Benchmarked)
- Building an Effective and Efficient Compliance Framework
  - Data Mapping, Diagramming Flows and Identifying Risk Trigger Points
  - Risk Assessment and gap analysis reporting
  - Building compliance and accountability into business units and shared services (e.g., IT, HR)
  - Compliance monitoring and audit
- Other Strategies
  - Leverage tactical issues to invest strategic issues
  - Building internal privacy assessment and monitoring functions
  - Implement Enterprise-Wide Risk Management Framework
    - Privacy & General Governance Study



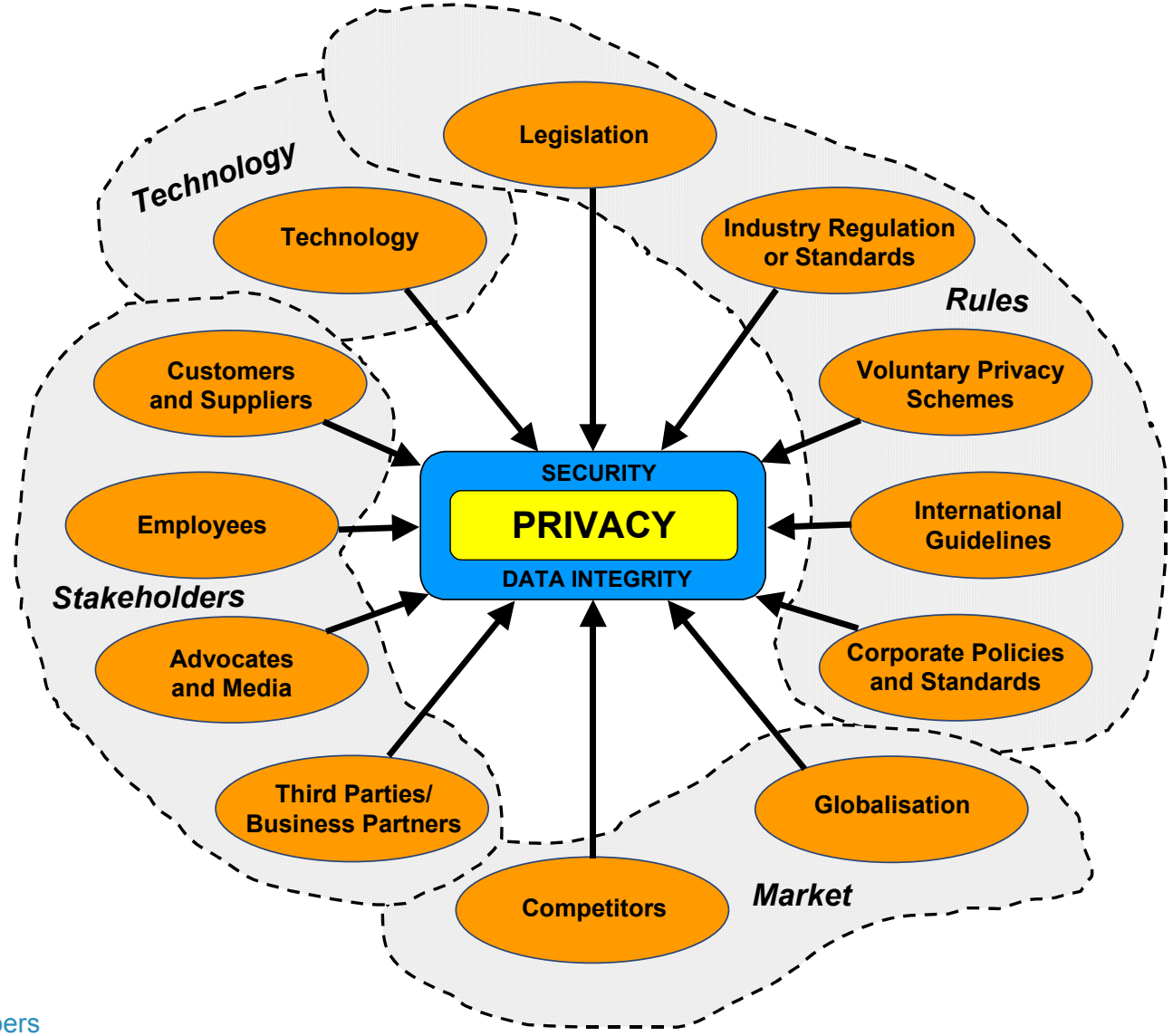
Responsible Privacy Practices

P w C

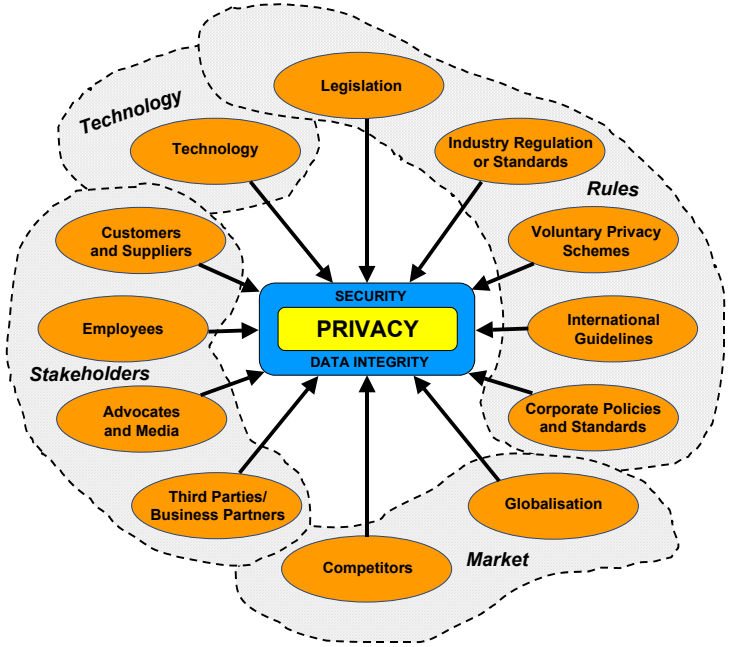
Many Elements to Privacy Compliance



Some Privacy Compliance Drivers



Some Privacy Compliance Drivers



Goals:

∗Protecting a Trusted Brand

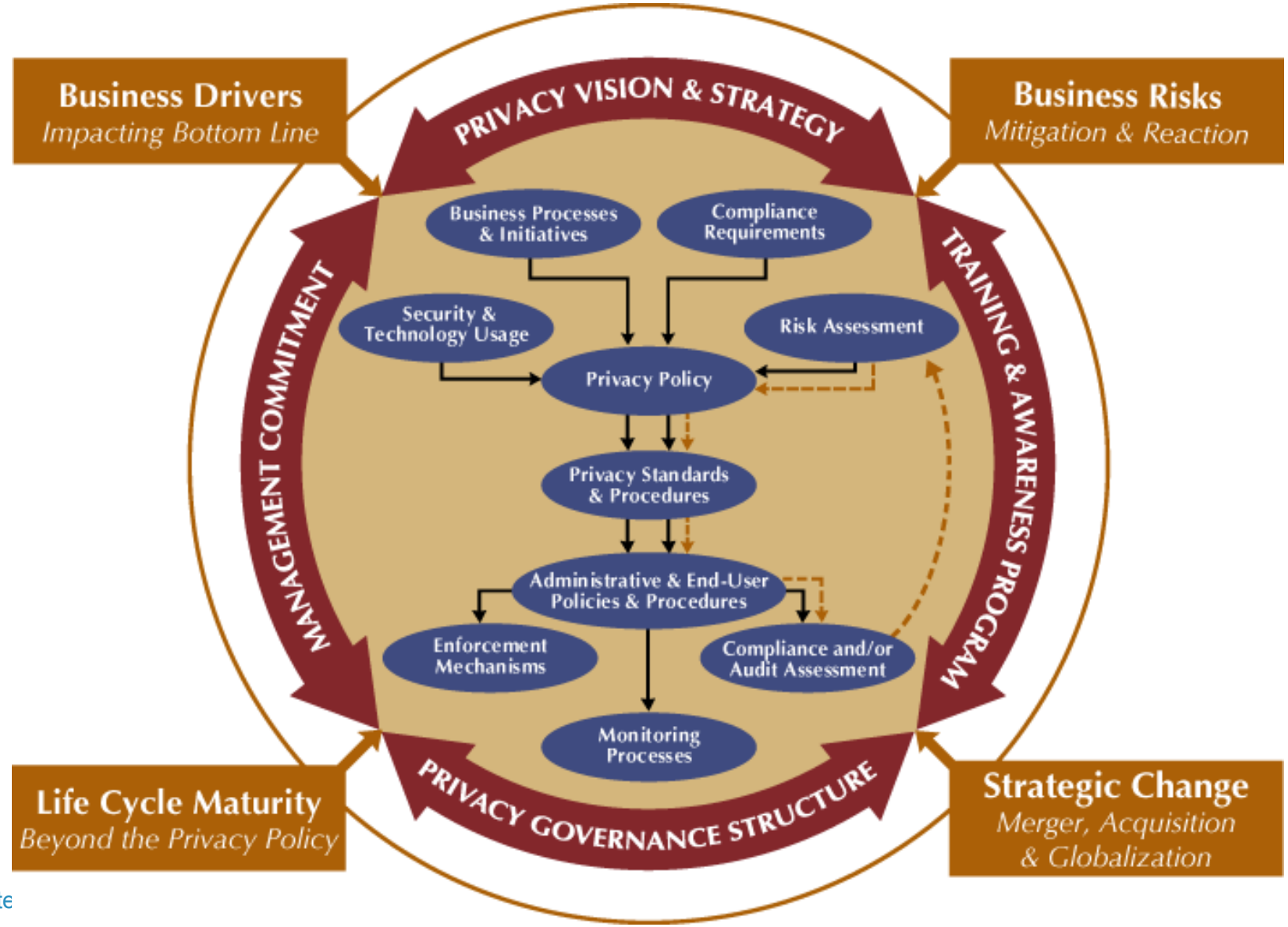
∗Managing Risks

∗Building Long-Term Value

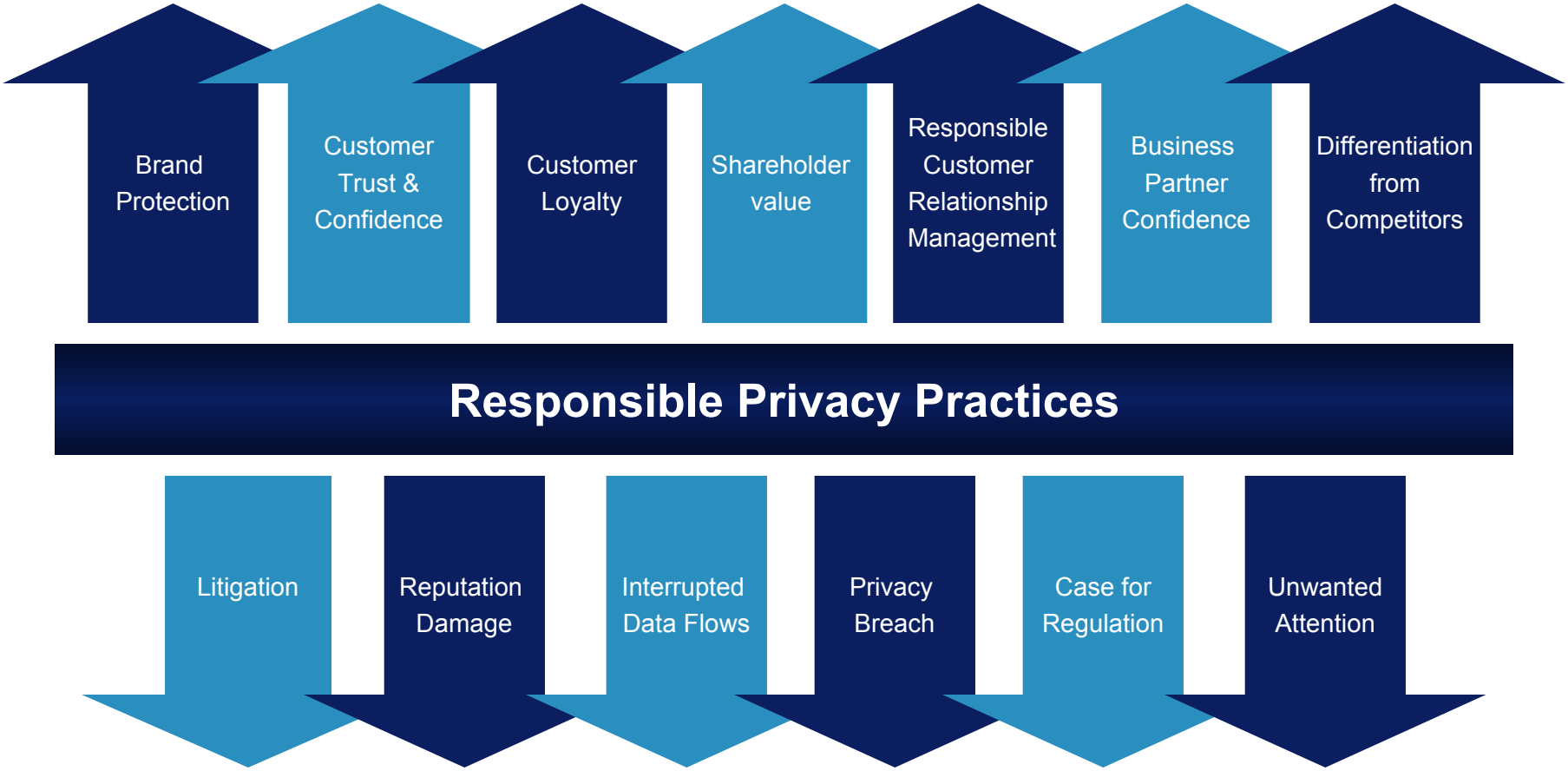
The drivers will vary dramatically for each organization and the different components that need to be analysed in detail include:

- Rules - legislation, regulation, guidance, industry standards/best practices, corporate policies across different jurisdictions
- Markets - globalisation, competitors
- Stakeholders - customers and suppliers, advocates and media, third party/business partners, employees
- Technology - the use of the Internet and sophisticated data capture, storage and security technologies

A Framework for Privacy Compliance



Benefits of Good Privacy Practices



Questions?

Kim P. Gunter, J.D., LL.M.
Senior Consultant, Privacy Practice
(267) 330- 4026
Kim.P.Gunter@us.pwc.com

PwC – The Leader in Privacy

PricewaterhouseCoopers has an extensive privacy consulting practice (Forrester, Market Overview: Privacy Management Technologies, February, 2003)

PricewaterhouseCoopers is ranked as the leading professional services firm providing information security and data privacy services to Global 2000 organizations. IDC, The Shifting Landscape: U.S. Information Security Services, 2003.

IDC, the premier global market intelligence and advisory firm in the information technology and telecommunications industries ranked PwC as an "Outperformer" with respect to their service offerings and growth potential, according to the IDC report, The Shifting Landscape: U.S. Information Security Services, 2003.

P w C