

PAYMENTS & PRIVACY

DEVELOPMENTS FOR THE RETAIL INDUSTRY

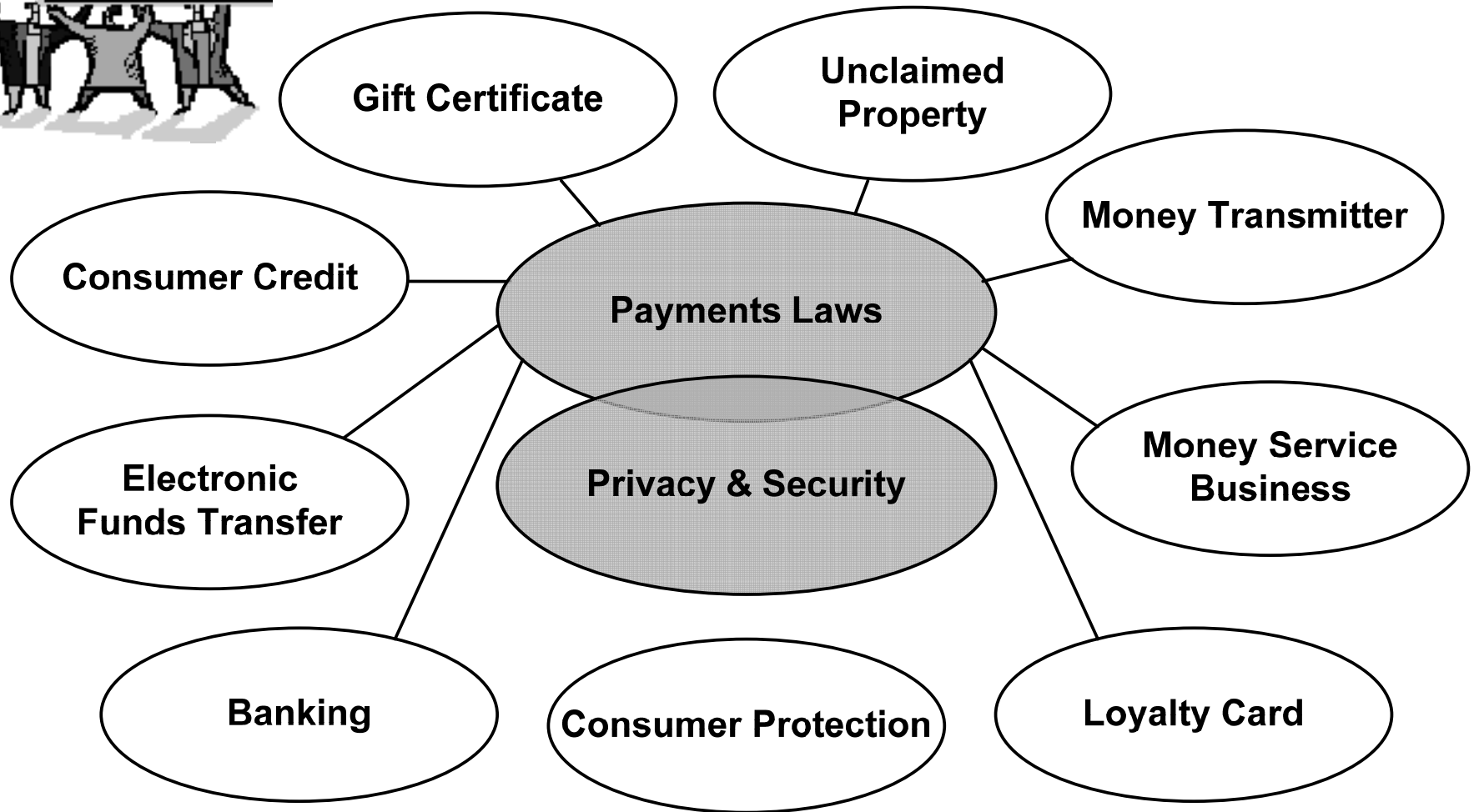
J. Dax Hansen
Thomas C. Bell

02.26.08

Payments & Privacy: Two Separate Topics That Also Come Together

- Payment Card Industry (PCI) Data Security Standard
- Retailer Breach Liability Laws
- State Security Breach Notice Laws
- Joint Customers Under Co-Brand, Private Label, Rebate Card Deals
- Loyalty Card Laws

Part I: Payments



Nuts and Bolts – Spotting Payments Issues



- Your interests and risk profiles are different from other players in the payments eco system
- Open loop vs. closed loop
- Follow the money—avoid "deposit taking," issuance of "payment instruments" and "money transmission"
- Expiration dates and "breakage"
- Fees
- Paid vs. promotional
- Adequacy of disclosures
- Crime and fraud
- Exclusivity, noncompetition and other onerous provisions

Development and Trends

1. New Laws: e.g., in 2007 new GC and UP laws enacted in: AR, CA, FL, IL, MN, MT, NV, NM, NC, OR, UT
2. Convergence and new technologies jeopardize GC unclaimed property planning (mobile/NFC, dual purpose cards, pressure to register)
3. Rebate cards and Faigman v. ATT&T Mobility LLC
4. Evolution of "Points" programs from loyalty to resemble GCs and open loop payment instruments
5. Alternative method payments, including mobile

Part 2: Privacy & Data Security

Since January 2005 over 218 million data records of U.S. residents have been exposed due to security breaches.

Source: Privacy Rights Clearinghouse, www.privacyrights.org

What are the costs?

- Ponemon Institute's 2007 Annual Study:
U.S. Cost of a Data Breach
 - pgp.com/downloads/research_reports/index.html

Data breach costs continue to increase: For 2007, per-record compromised costs continued to increase, growing more than 9 percent since 2006 and more than 42 percent since 2005.

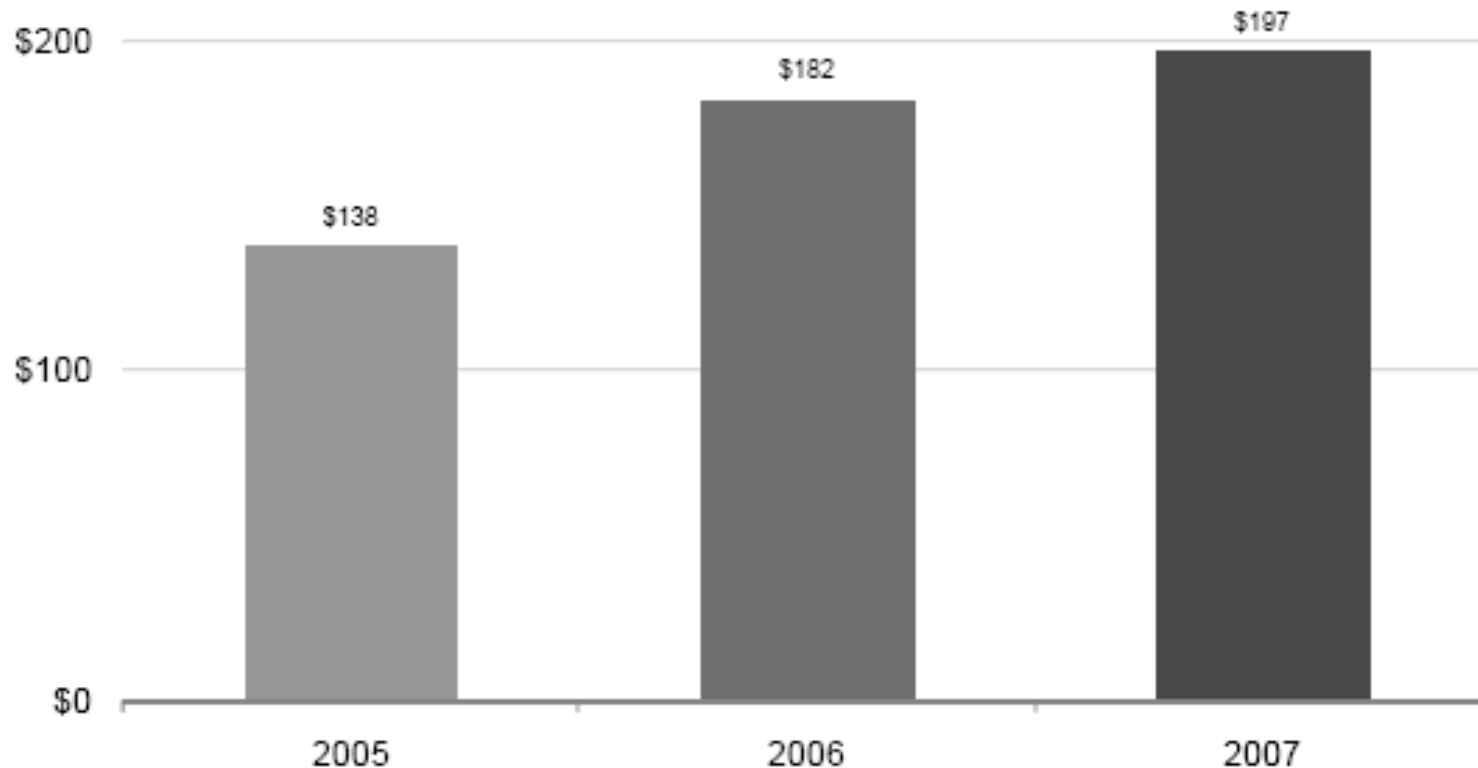


Figure 1: Average per-record cost of a data breach, 2005–2007

Source: Poneman Institute, 2007 Annual Study: U.S. Cost of a Data Breach.

Activity cost category	2005	2006	2007	Trend
Investigation & forensics	6%	6%	6%	→
Audit & consulting services	6%	8%	7%	↘
Outbound contact costs	11%	8%	4%	↘
Inbound contact costs	11%	9%	5%	↘
Public relations/communications	0%	1%	3%	↗
Legal defense	4%	6%	8%	↗
Security consultants	2%	3%	2%	↘
Free or discounted services	4%	2%	1%	↘
Credit monitoring services	3%	3%	1%	↘
Lost business (due to churn)	49%	46%	56%	↗
Customer acquisition	5%	8%	9%	↗

Table 2: Percent of breach costs by activity cost category, 2005–2007

Note: The cost of lost business includes both lost business due to churn and increased customer acquisition costs.

Source: Poneman Institute, 2007 Annual Study: U.S. Cost of a Data Breach.

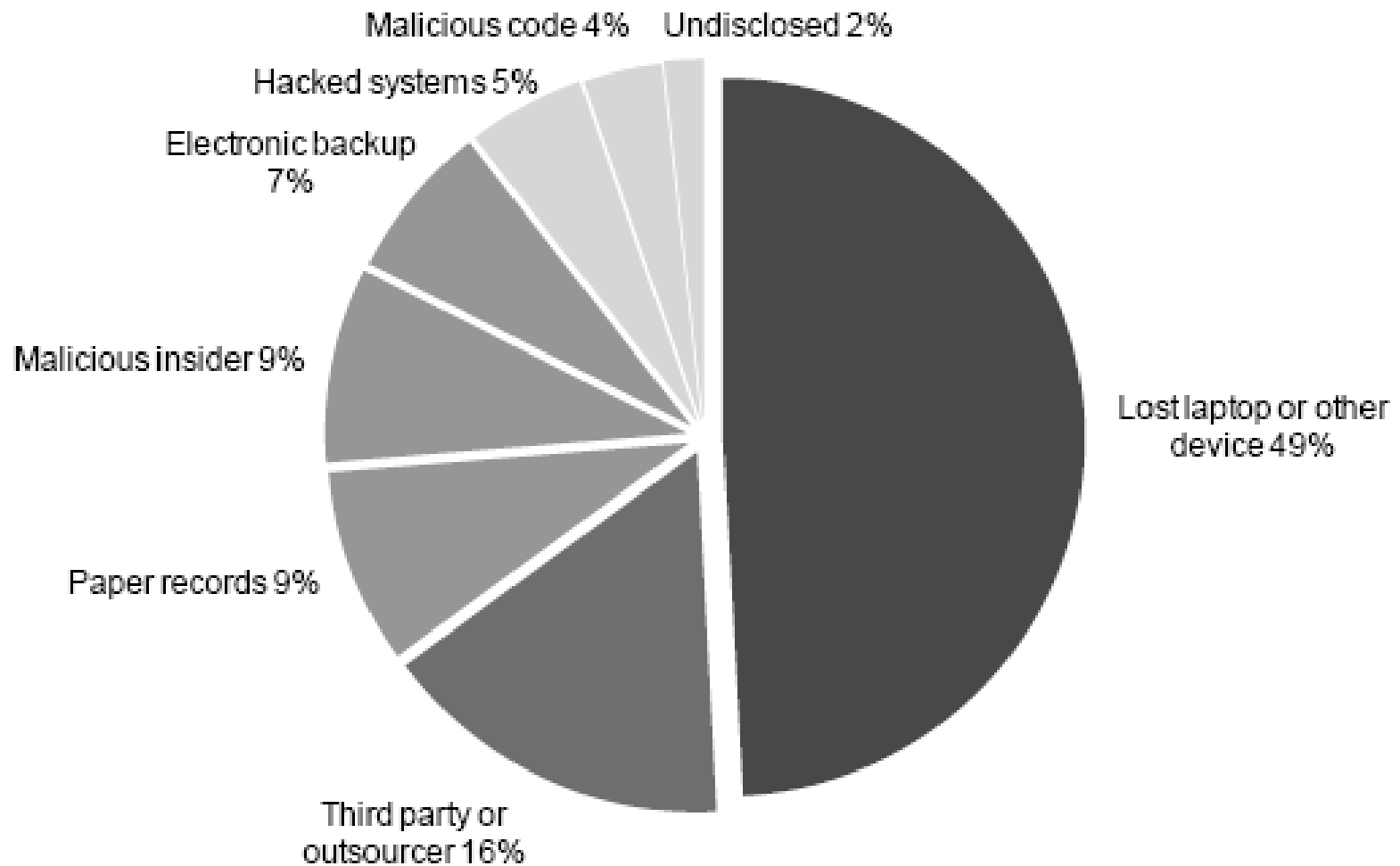


Figure 3: Primary cause of a data breach

Source: Poneman Institute, 2007 Annual Study: U.S. Cost of a Data Breach.

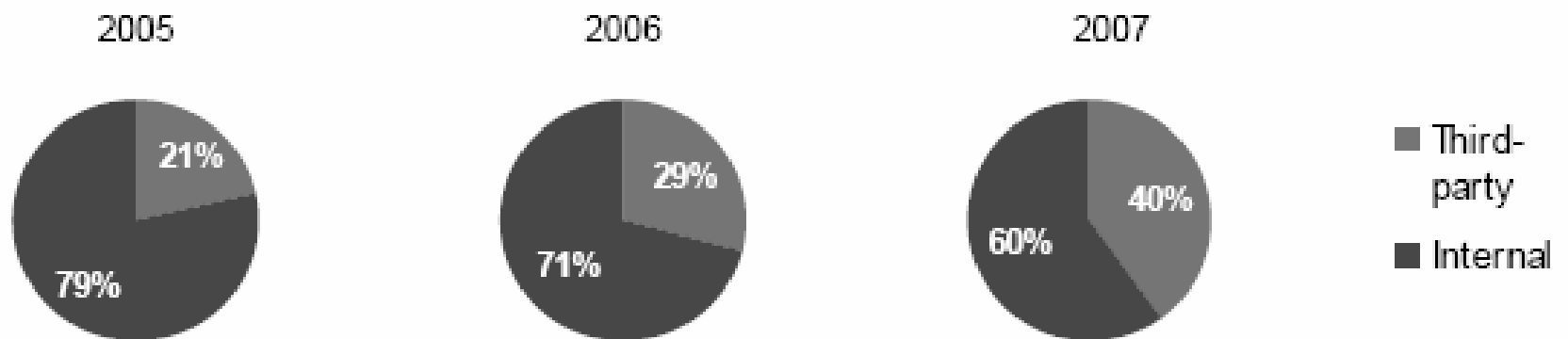


Figure 4: Third-party share of data breaches, 2005–2007

Source: Poneman Institute, 2007 Annual Study: U.S. Cost of a Data Breach.

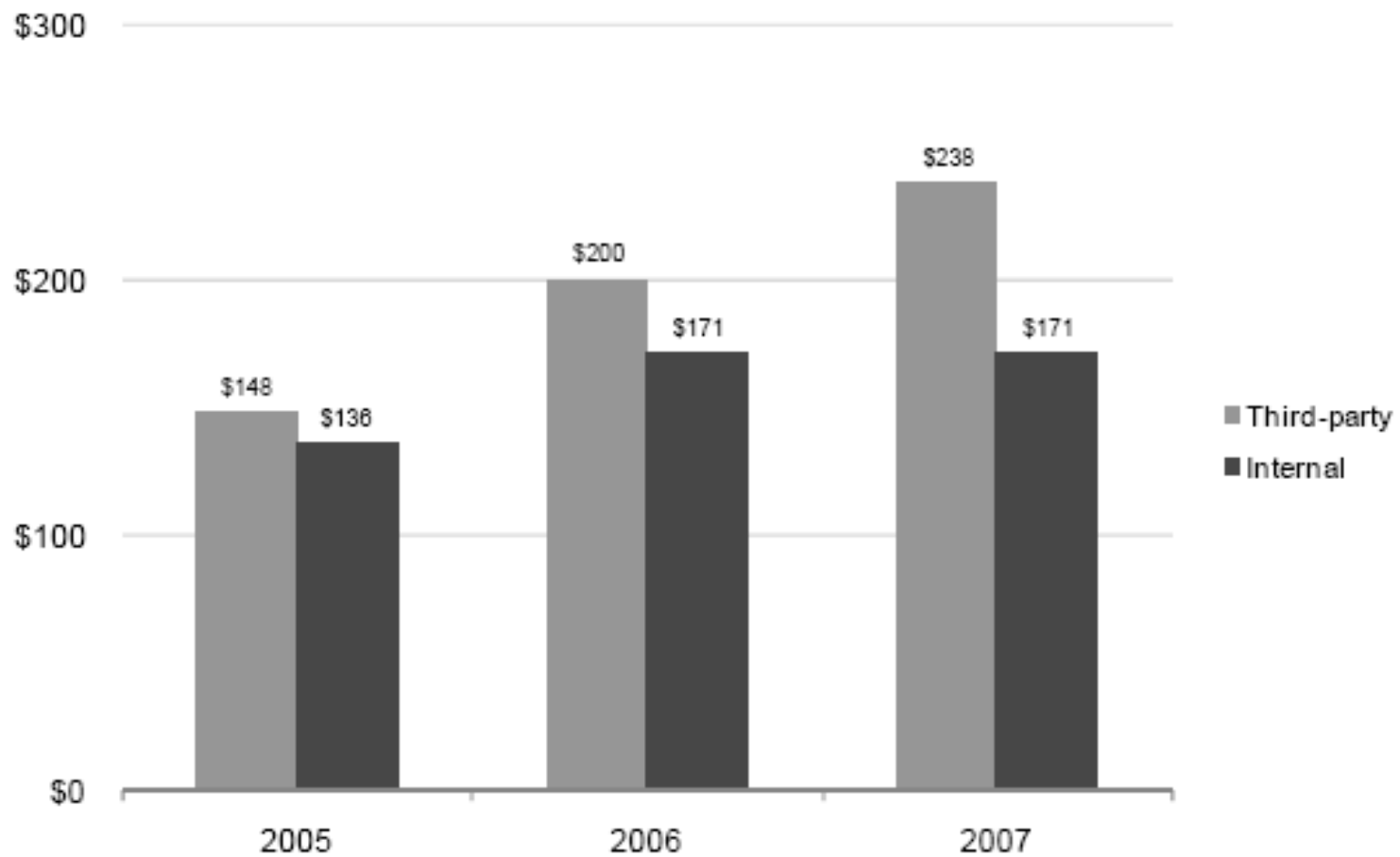


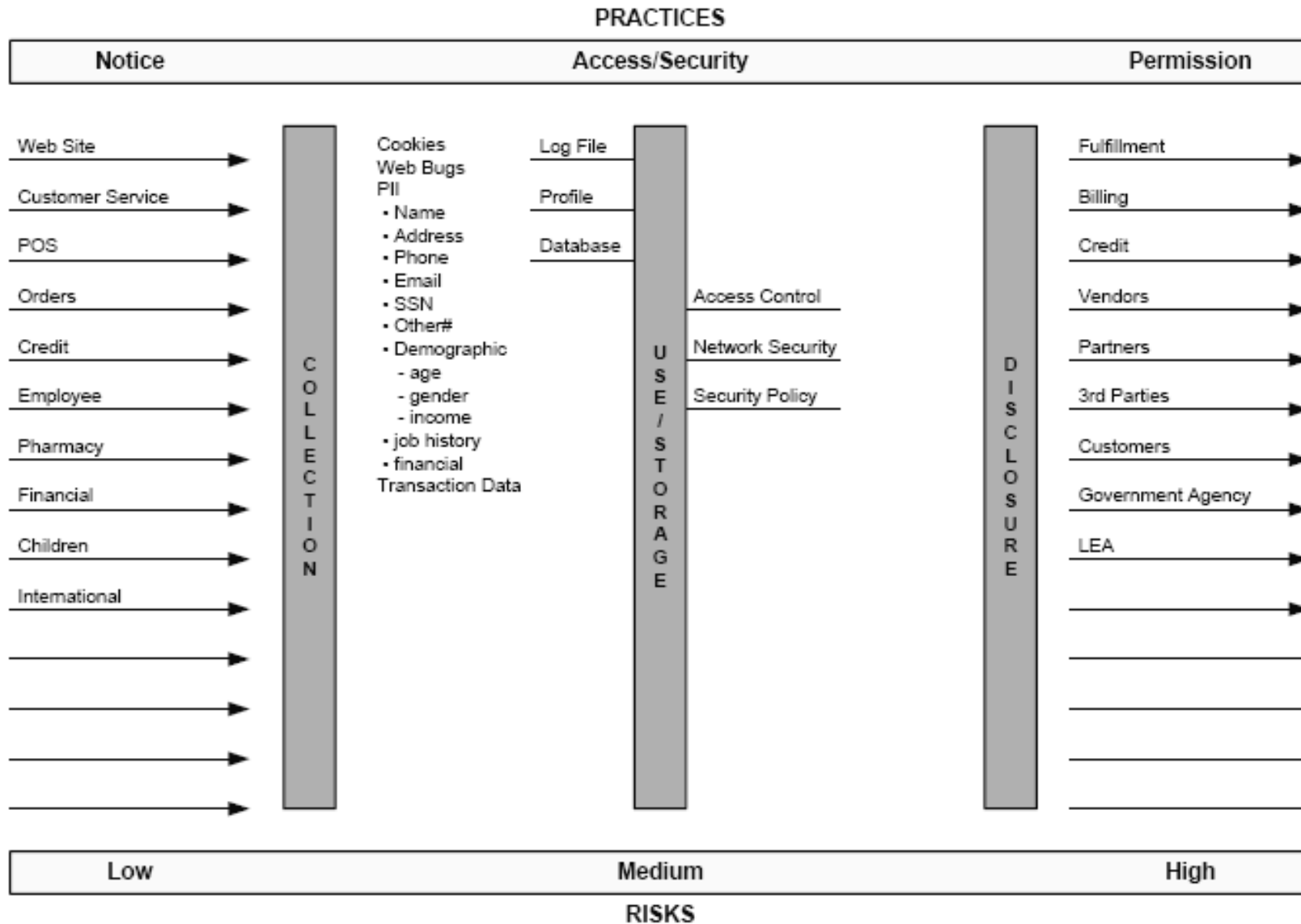
Figure 5: Third-party data breach costs, 2005–2007

Source: Poneman Institute, 2007 Annual Study: U.S. Cost of a Data Breach.

What is the legal landscape?

- Regulatory and payment rules (FTC, Breach notice laws, ECPA, PCI, GLB, etc.)
- Privacy policy
- Privacy framework—what is happening in the organization?

Privacy Framework



Retail Cases: Some Lessons Learned

- Protections are not just privacy policy based: BJ's
- Merchants and Financial Institutions are not on the same side: TJ Maxx

Preparation

- Breach response plan (hand out)
- Contract strategies

Minimum contract strategies for third party sources of risk: data hosts, processors, advertisers, marketing partners, storage companies, etc.

- Define and deal with "personal information"
- Due diligence
 - past audits
 - past breaches
 - ongoing audits

Minimum contract strategies (cont.)

- Notice:
 - Vendor shall immediately notify Retailer of any actual, probable or reasonably suspected breach of security of the Vendor Systems and of any other actual, probable or reasonably suspected unauthorized access to or acquisition, use, loss, destruction, compromise or disclosure of any Confidential Information of Retailer, including without limitation any Personal Information (each, a "Security Breach").

Minimum contract strategies (cont.)

- Cooperation
 - In any notification to Retailer required under this Addendum, Vendor shall **designate a single individual** employed by Vendor who must be available to Retailer 24-hours per day, 7-days per week as a contact regarding Vendor's obligations under this Addendum. Vendor shall (a) assist Retailer in investigating, remedying and taking any other action Retailer deems necessary regarding any Security Breach and any dispute, inquiry or claim that concerns the Security Breach; and (b) shall provide Retailer with assurance satisfactory to Retailer that such Security Breach or potential Security Breach will not recur. Unless prohibited by an applicable statute or court order, Vendor shall also **notify Retailer of any third-party legal process** relating to any Security Breach, including, but not limited to, any legal process initiated by any governmental entity (foreign or domestic).

Minimum contract strategies (cont.)

- Standard of Care
 - Vendor is **fully responsible** for any authorized or unauthorized collection, storage, disclosure and use of, and access to, Personal Information.
 - Vendor shall implement and maintain administrative, physical and technical safeguards ("Safeguards") **that prevent** any collection, use or disclosure of, or access to, Personal Information that this Agreement does not expressly authorize, including, without limitation, an information security program that meets the highest standards of best industry practice to safeguard Personal Information.

Minimum contract strategies (cont.)

- Indemnity
 - Vendor will defend and indemnify Retailer, its parent, subsidiaries and affiliates, and each of their respective officers, shareholders, directors and employees from and against any third party claims, losses, liabilities and expenses (including, without limitation, reasonable attorneys' fees and expenses) that relate to **any failure to comply** with any obligation enumerated in this (1) Agreement relating to Personal Information, or (2) this Addendum.
 - Which costs are covered?

Minimum contract strategies (cont.)

- Limitation on Liability
 - Vendors typically seek to exclude indirect and consequential damages. These damages are, however, precisely the type of damages that Retailer might incur from the disclosure, theft or destruction of data.
 - Therefore, seek to carve out (i) all damages arising from breaches of this Addendum and (ii) all indemnification obligations (or, if absolutely cannot get (ii), all indemnification obligations arising out of breaches of confidentiality or security provisions--i.e., all breaches of this Addendum).
 - Similarly, carve out (i) all damages arising from breaches of this Addendum and (ii) all indemnification obligations (or, if absolutely cannot get (ii), all indemnification obligations arising out of breaches of confidentiality or security provisions—i.e., all breaches of this Addendum) from the overall cap on damages.

New Developments

- "Rebate" Cards
- Loyalty Programs
- eCommerce Partners:
whose customer is it?

Questions?

