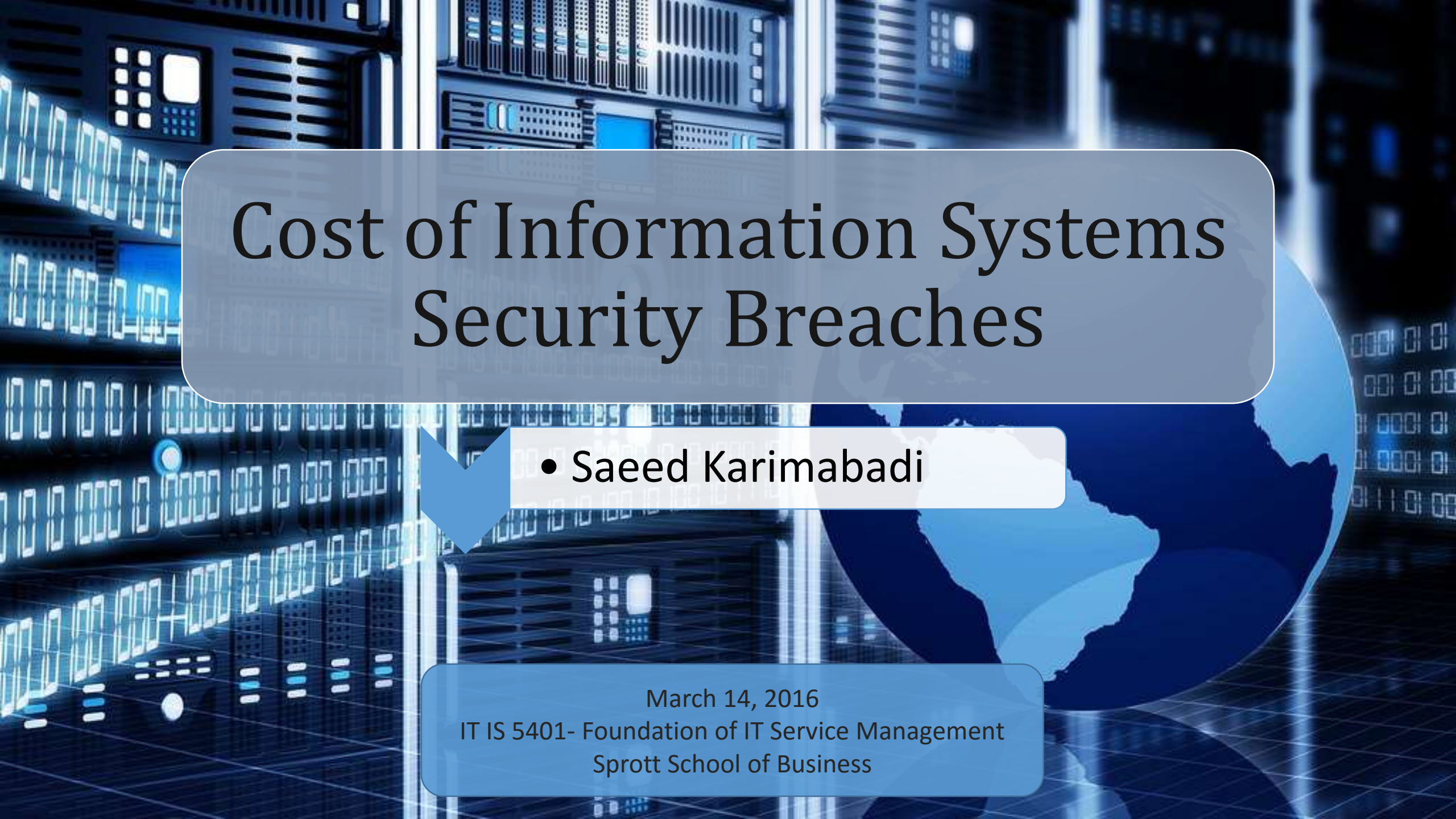


Cost of Information Systems Security Breaches

- Saeed Karimabadi

March 14, 2016

IT IS 5401- Foundation of IT Service Management

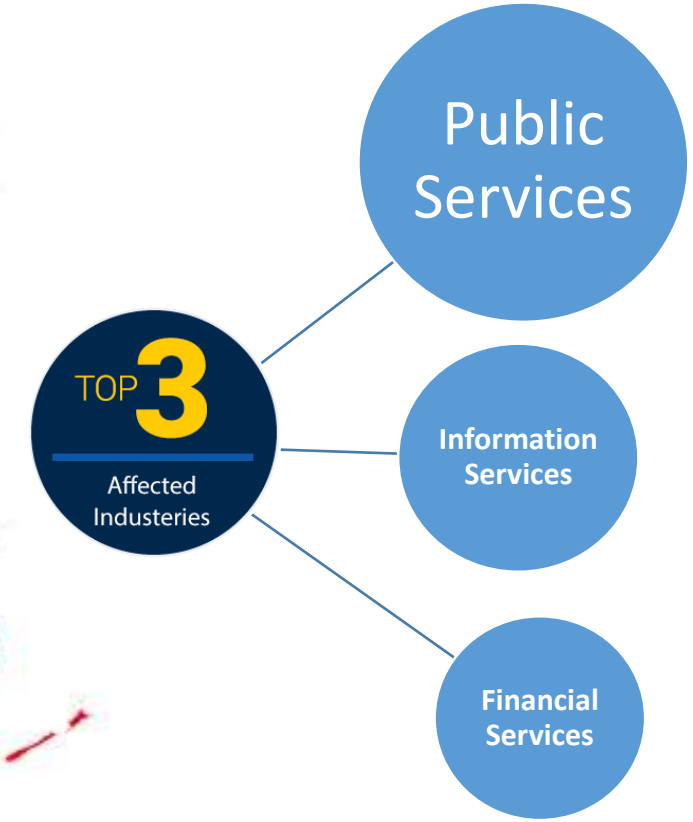
Sprott School of Business

Average Cost of a Security Breach

Average Total Cost of a data breach	2014: $3.52 Million	2014: $3.52 Million
Average Cost of each Stolen record:	2014: $145 per record	2015: $154 per record

- IBM report on Cost of Security Breach , May 2015

Data Breach Victim Demographics - 2015



- Data from Verizon's 2015 Data Breach Investigations Report

Data breaches cost per capita and GDP

Data breaches cost the most in the US and Germany and the lowest in Brazil and India.

The average per capita cost of data breach:	US : $217	Germany : $211	Brazil : $78	India : $56

Organizations Data Security

Brazil and France:

Least Secure Organizations

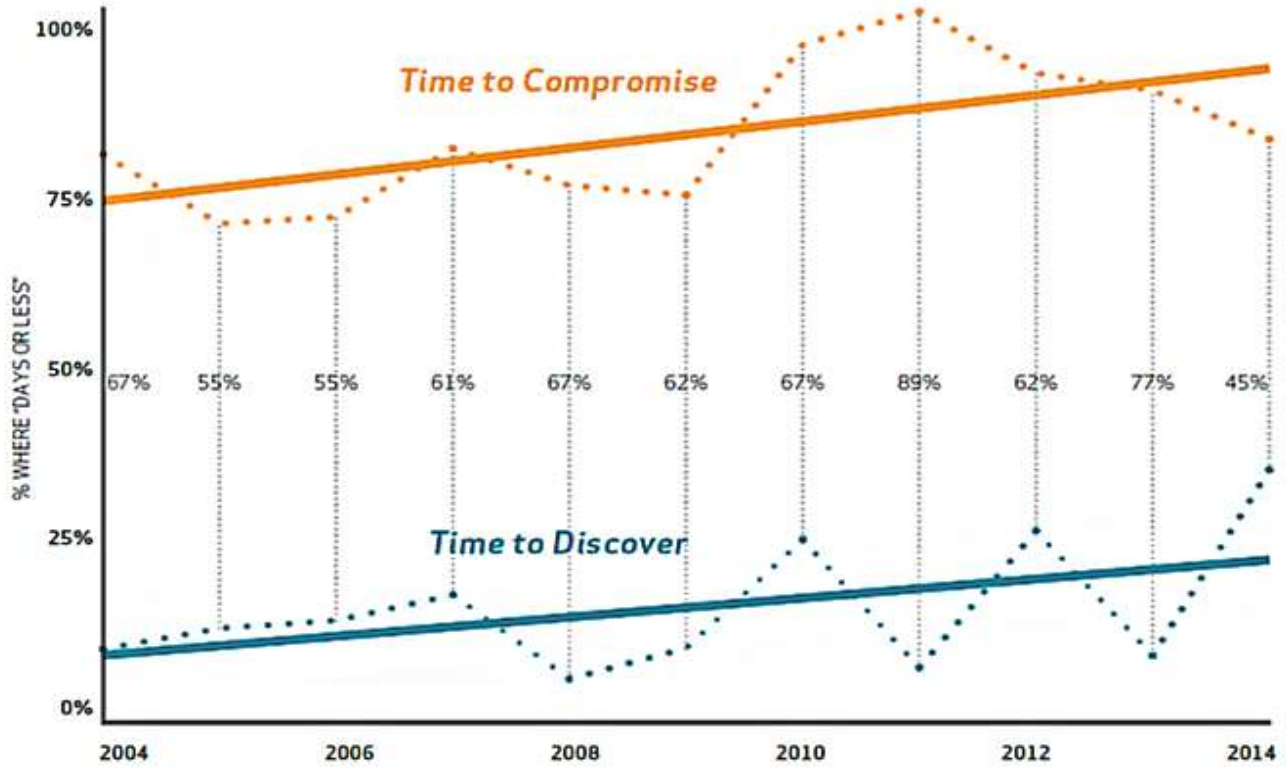
- Organizations in Brazil and France are more likely to have a data breach

Germany and Canada:

Most Safe Organizations

- Organizations in Germany and Canada are least likely to have a breach.

Breach Discovery – Primary Challenge



- Data from Verizon's 2015 Data Breach Investigations Report

60%

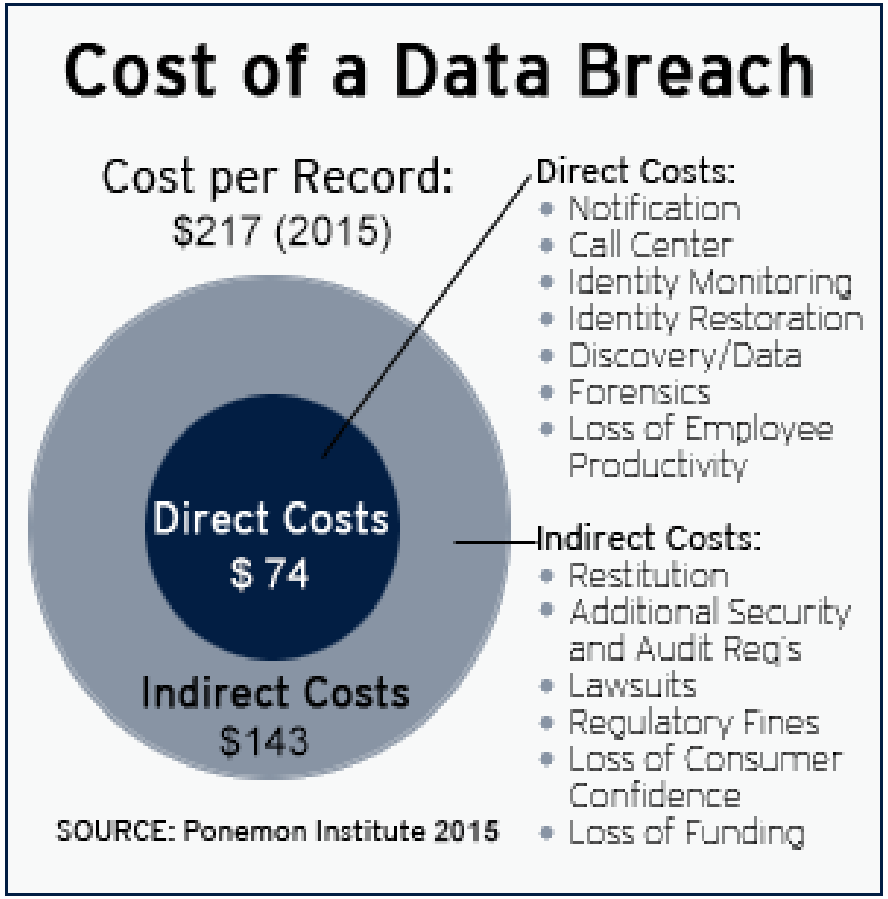
IN 60% OF CASES, ATTACKERS ARE ABLE TO COMPROMISE AN ORGANIZATION WITHIN MINUTES.

- It contrasts how often attackers are able to compromise a victim in days or less (orange line) with how often defenders detect compromises within that same time frame (teal line).
- Indicating a growing "detection deficit" between attackers and defenders.

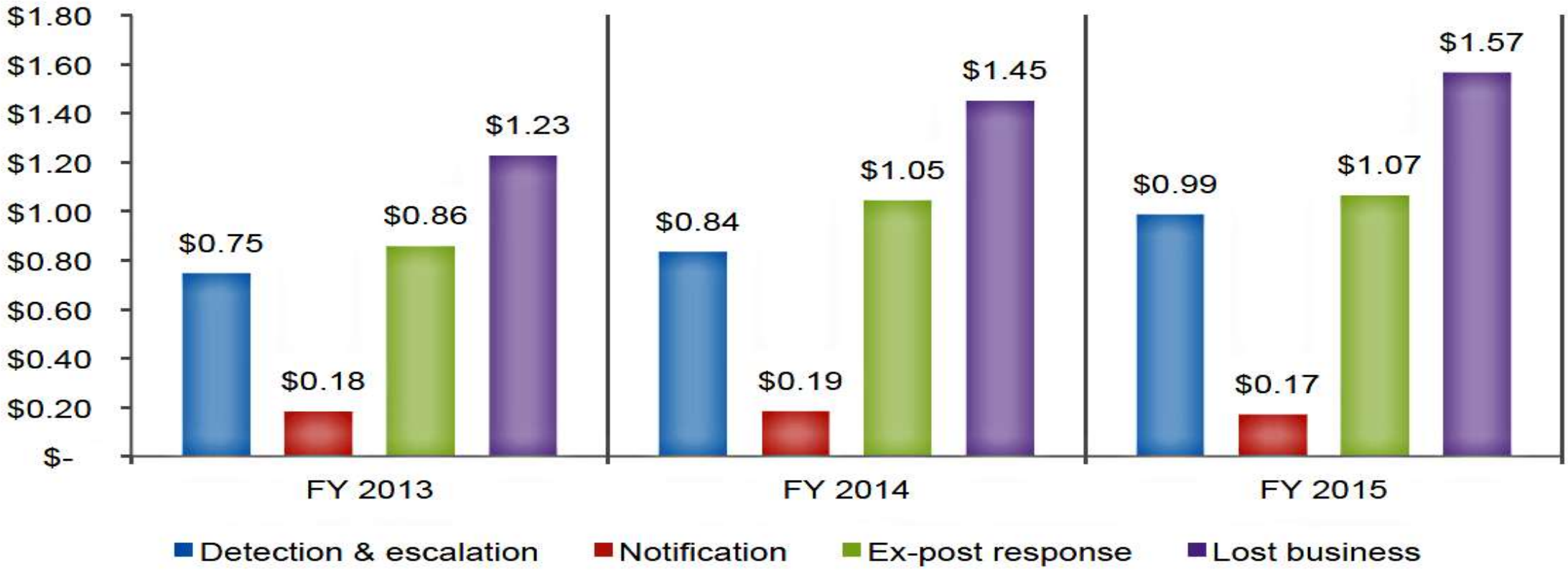
Possible Outcome of a Security Breach

- **Damaged Intellectual Property:** Blue prints, designs
- **Revenue Lost:** Downtime
- **Theft:** Bank Information, Transfer codes
- **Vandalism:** False or discrediting information
- **Loss of customers :** Lose customers trust
- **Damage to business reputation**
- **Compliance obligations**
- **Government investigations**
- **Civil litigation**

Key Costs to A Data Breach



Cost Components



Hidden Costs

Increasing Cost of Data Breach

Attacks Frequencies	• Cyber attacks have increased in frequency and in the cost to remediate the consequences.
Lost Business Cost	• The consequences of lost business are having a greater impact on the cost of data breach.
Detection Cost	• Data breach costs associated with detection and escalation increased.

Recent Major Data Breaches

JP Morgan Chase data breach 2014

- Largest bank in the United States
- World's sixth largest bank by total assets.
- Over 83 million accounts
- 76 million households (approximately two out of three households in the US)
- 7 million small businesses.
- JPMorgan spend $250 million on computer security every year.

CHASE

Sony PlayStation Security Breach 2011

PlayStation Network security breach will cost Sony much more than money

Hacking of 77 million users' data is expected to cost the company tens of millions and puts a wrench in Sony's goal of networking across entertainment devices and content.

Sony Pictures Hack 2014

100 terabytes of data was stolen containing:

- Personal information about Sony Pictures' employees and their family
- E-mails between employees
- Information about executive salaries
- Copies of unreleased Sony films

System availability denied, degraded

Lawsuits

Brand damage

Damage:

$1.25 billion from

- Lost business
- Various compensation costs
- New investments

Staples Data Breach 2014

Stolen Data

- Cardholders names, card numbers, expiration dates and card verification codes of 1.16 million customer credit and debit cards used at 119 Stapled locations in 35 American states

Long Breach Discovery

- This data was stolen over a period of up to Six months.

Consequences

- Caused the resignation of the company's CEO during mid-2014
- The attack cost financial institution $200 million
- Profit fell 46 percent in fourth quarter of 2013

Adobe Data Breach 2013

Stolen Data

- 38 million passwords, 3 million credit card records and source code to several programs.

Quick response

- Being a Silicon Valley-based tech company, was clearly ready to contain the damage even though its security measures had failed.

eBay Cyber Attack 2014

- Stolen Data
  - Personal Data of 233 million registered account
- Poor Response to Crisis
  - The company failed to send out a mass email in a timely manner to customers
  - It waited two weeks instead of one to notify investors and customers.

Reduce Cost of Data Breach

Executive Level Involvement

Executives opinion:

- 79 percent believe that executive level involvement is necessary.

Executive Involvement

- 70 percent believe board level oversight is critical.

Board Level oversight

As evidence, CEO Jamie Dimon personally informed shareholders following the JPMorgan Chase data breach that by the end of 2014 the bank will invest $250 million and have a staff of 1,000 committed to IT security

How to Reduce The Cost

Board Involvement	• Board involvement and the purchase of insurance can reduce the cost of a data breach.
Loss of Customers	• The loss of customers increases the cost of data breach.
Notification Cost	• Notification costs remain low, but costs associated with lost business steadily increase
Time to Identify The Breach	• Time to identify and contain a data breach affects the cost.
Business Continuity	• Business continuity management plays an important role in reducing the cost of data breach.

Information Security Basics: The CIA Triad

- Confidentiality, integrity and availability, also known as the **CIA triad**, is a model designed to guide policies for information security within an organization.

- Balances the competing requirements of confidentiality, integrity and availability with equal emphasis on each.

What To Have In Place Prior To A Compromise

- Create an action plan on what to do if you are breached.
- Practice that plan periodically.
- Have a list of all relevant contacts, emails, numbers, etc.
- Potential agreement with forensic firms already prepared.
- Identify all third parties that touch, store or transmit card data on your behalf.
- Be familiar with your vendor agreements to understand your/their responsibilities in regards to PCI compliance and breach notification.

What To Do If Compromised

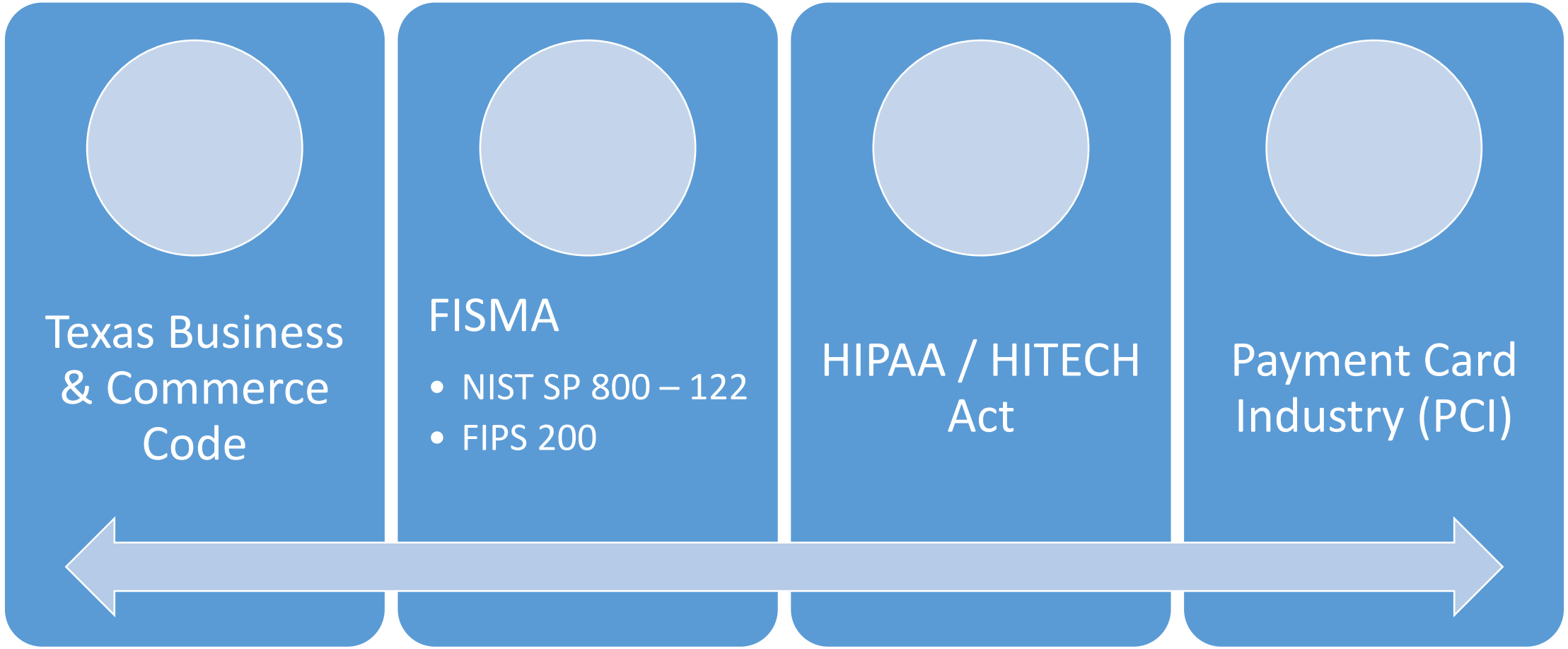
1. Notify the incident internally
2. Assemble a response team
3. Investigate the incident
4. Determine whether the incident constitutes a reportable breach
5. Contain the breach and mitigate harm, to the extent possible
6. Notify affected persons, Law enforcement, Government and Media
7. Respond to inquiries
8. Improve processes to avoid future data breaches





Data Security Regulations

Regulatory compliance & state codes



Texas Business and Commerce Code

- Sec. 521.052 BUSINESS DUTY TO PROTECT SENSITIVE PERSONAL INFORMATION.

(a) A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.

- Sec. 521.053 NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED

"…shall disclose any breach of system security, after discovering or receiving notification of the breach, to any resident of this state whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made as quickly as possible,…"

Payment Card Industry (

- **Anyone who stores, process, or transmits credit card data must be PCI compliant**
- **Common PCI validation requirements**
  - Report on Compliance (ROC)
  - Self-Assessment Questionnaire (SAQ)
  - Letter of Attestation
  - Quarterly PCI scans
- **Sample PCI Data Security Standards Requirements**
  - Annual Penetration Testing (DSS 11.3)
  - Security Awareness Training (DSS 12.6)
  - Quarterly PCI scans (DSS 11.2)