Symantec™

2011 Annual Study: U.S. Cost of a Data Breach

March 2012

Ponemon Institute and Symantec Research

- Seventh year Ponemon has conducted this benchmark study
- Examines the following topics:
  - Average costs from a breach (direct and indirect)
  - Potential legal costs
  - Costs of lost customers and brand damage
  - Key trends
  - Preventive measures taken after a breach
- Results are not based upon hypothetical responses

Methodology

49 U.S.-based organizations
actual data breach experiences

400 individuals interviewed
responsible for IT, compliance, infosec
with knowledge of data breach costs

14 industry sectors

0 catastrophic data breaches
incidents >100,000 compromised
records not included

Data breaches continue to have serious financial consequences

Average organizational cost per data breach

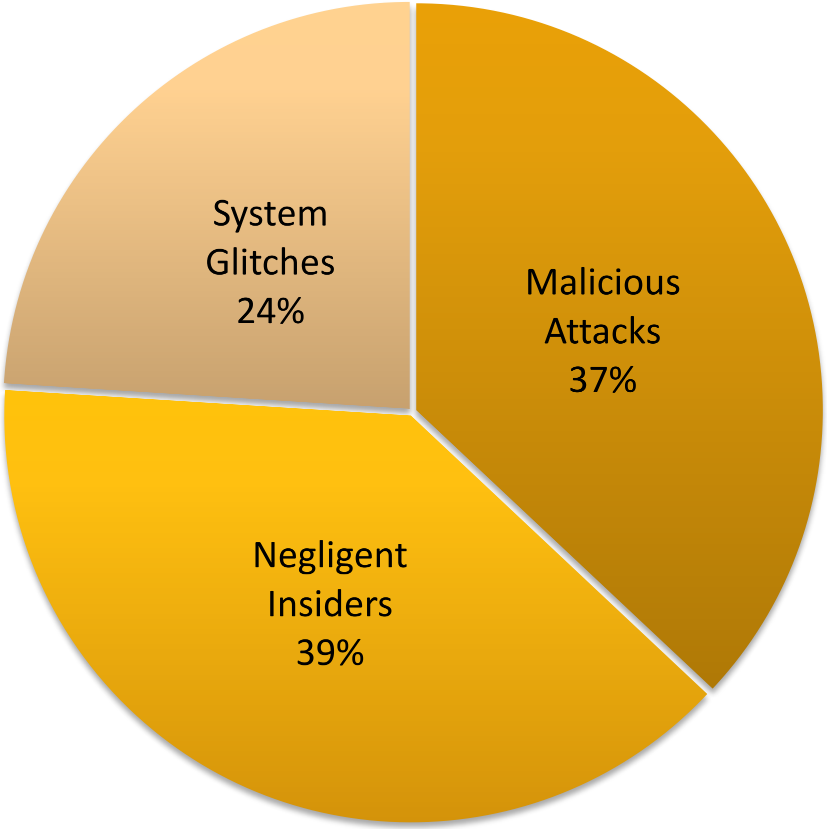
$5.5 million

Cost per compromised record

$194

Malicious attacks most costly, more frequent

Major Causes of Data Breach

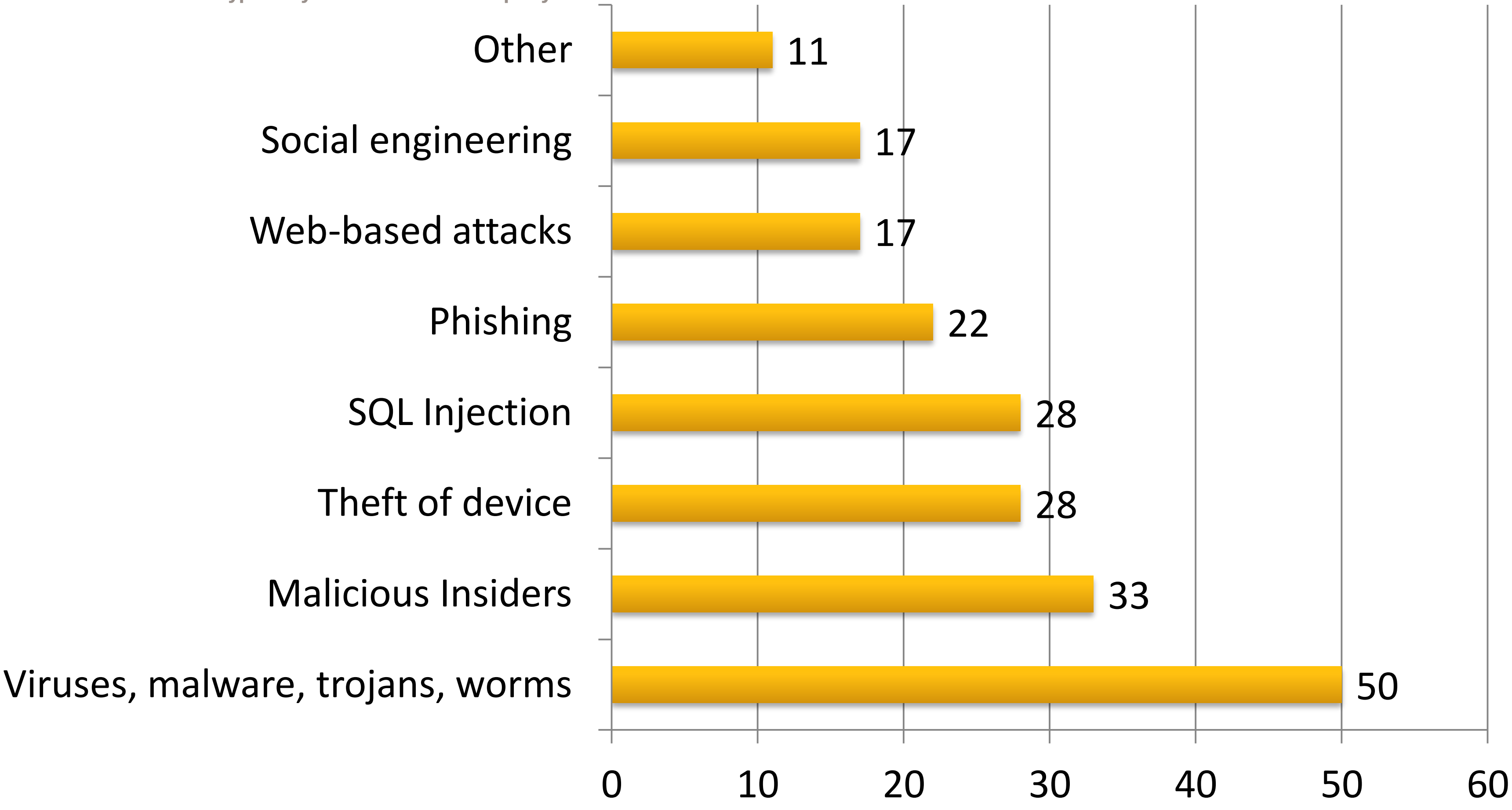


- *For the first time,* malicious attacks cause > one-third
  - 37% of cases involved malicious attacks
  - Up 6 points from 2010
- Malicious attacks average $222 per record
  - Highest of all breach types
  - $48 more per record than negligent insiders

Malicious insiders should not be underestimated

Breakdown of Malicious Attacks

More than one attack type may exist for each company



More customers remain loyal

- *For the first time*, fewer customers abandon companies after a data breach
  - Average abnormal churn decreased to 3.2% in 2011
  - Down 18% from 3.9% in 2010
- The more churn, the higher the cost of data breach
- Certain industries are more susceptible to churn
- Lost business costs in 2011 decline to $3.01 million

Taking steps to keep customers loyal and repair damage to reputation and brand can help reduce the cost of a data breach.

Customer Churn

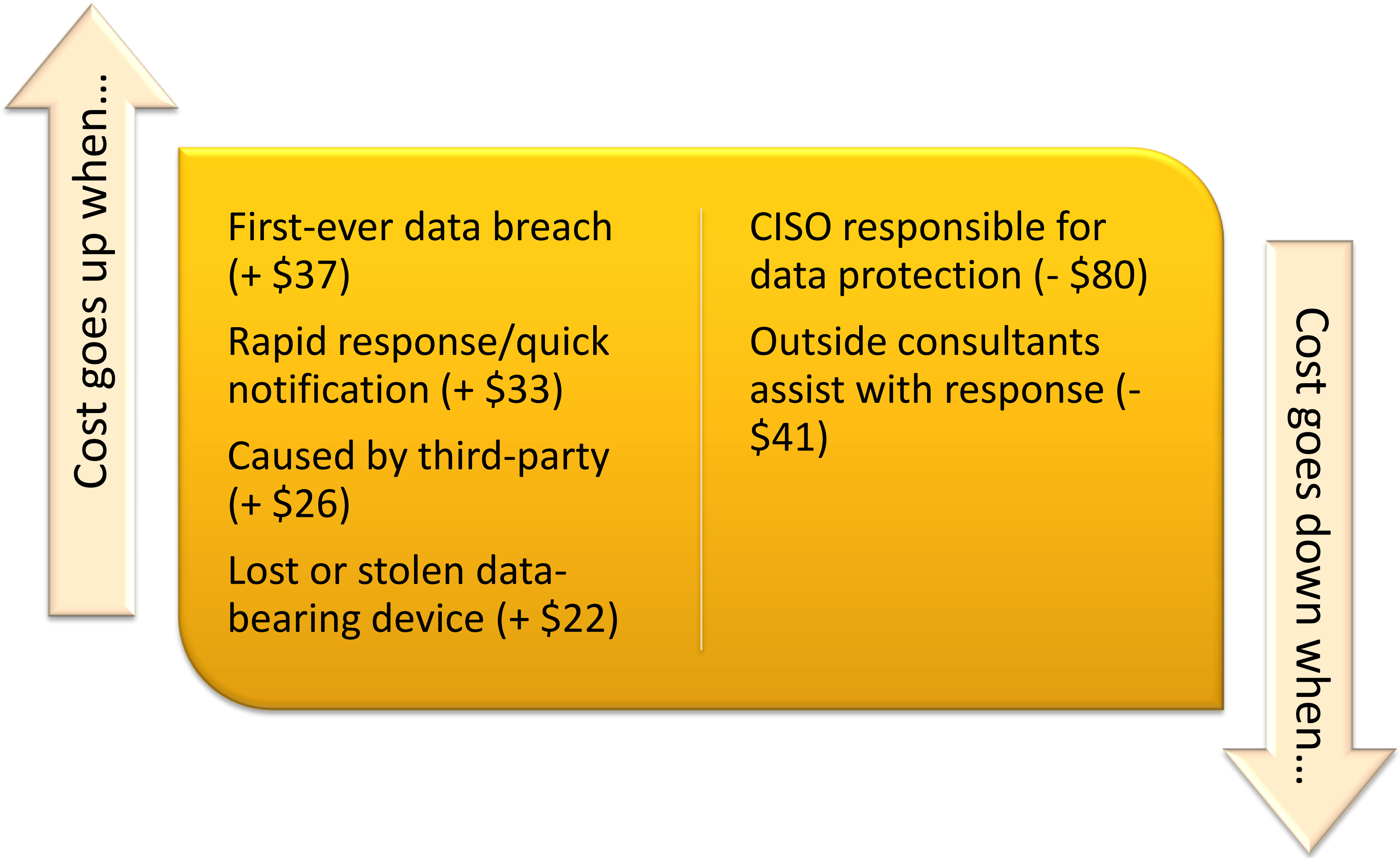
18%

Detection + escalation costs lower, notification higher

- Organizations more efficient in investigating data breaches
  - Average detection and escalation cost declined to $428,330
  - Down 6% from its high of $455,304 in 2010
- Notification costs increased slightly to $561,495
  - Up 10% from $511,454 in 2010
  - Increase in laws and regulations governing data breach notification is a factor

Suggests that organizations had the appropriate processes and technologies to respond to and resolve data breach incidents.

Six factors that raise / reduce cost of a data breach



Cost goes up when…

First-ever data breach (+ $37)

Rapid response/quick notification (+ $33)

Caused by third-party (+ $26)

Lost or stolen data-bearing device (+ $22)

CISO responsible for data protection (- $80)

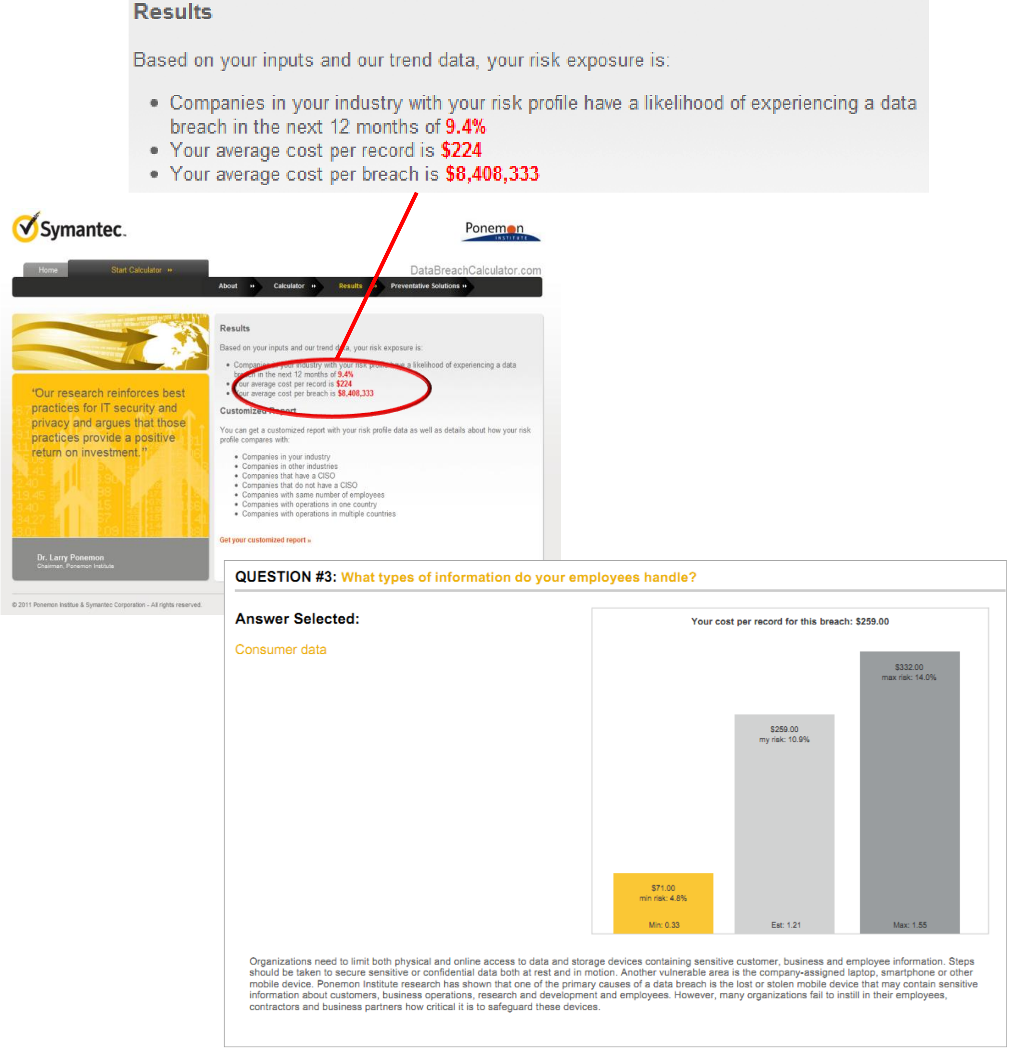
Outside consultants assist with response (- $41)

Cost goes down when…

Best Practices to Avoid Major Causes of Data Breach

- Assess risks by identifying and classifying confidential information
- Educate employees on information protection policies and procedures, then hold them accountable
- Implement an integrated security solution that includes reputation-based security, proactive threat protection, firewall and intrusion prevention in order to keep malware off endpoints
- Deploy data loss prevention technologies which enable policy compliance and enforcement
- Proactively encrypt laptops to minimize consequences of a lost device
- Implement two factor authentication
- Integrate information protection practices into businesses processes

Data Breach Risk Calculator



Results

Based on your inputs and our trend data, your risk exposure is:

- Companies in your industry with your risk profile have a likelihood of experiencing a data breach in the next 12 months of 9.4%
- Your average cost per record is $224
- Your average cost per breach is $8,408,333

"Our research reinforces best practices for IT security and privacy and argues that those practices provide a positive return on investment."

Dr. Larry Ponemon
Chairman, Ponemon Institute

Results

Based on your inputs and our trend data, your risk exposure is:

- Companies in your industry with your risk profile have a likelihood of experiencing a data breach in the next 12 months of 9.4%
- Your average cost per record is $224
- Your average cost per breach is $8,408,333

Customized Report

You can get a customized report with your risk profile data as well as details about how your risk profile compares with:

- Companies in your industry
- Companies in other industries
- Companies that have a CISO
- Companies that do not have a CISO
- Companies with same number of employees
- Companies with operations in one country
- Companies with operations in multiple countries

Get your customized report »

QUESTION #3: What types of information do your employees handle?

Answer Selected:

Consumer data

Your cost per record for this breach: $259.00

Organizations need to limit both physical and online access to data and storage devices containing sensitive customer, business and employee information. Steps should be taken to secure sensitive or confidential data both at rest and in motion. Another vulnerable area is the company-assigned laptop, smartphone or other mobile device. Ponemon Institute research has shown that one of the primary causes of a data breach is the lost or stolen mobile device that may contain sensitive information about customers, business operations, research and development and employees. However, many organizations fail to instill in their employees, contractors and business partners how critical it is to safeguard these devices.

- Enables organizations to estimate how a data breach could impact their company
- Uses seven years of trend data from this study
- It can calculate:
  - The likelihood that the company will experience a data breach in the next 12 months
  - The cost per record in the event of a data breach at the company
  - The overall cost of a data breach at the company
- www.databreachcalculator.com

In Summary

- Key Findings:
  - For the first time, data breach costs have declined
  - Customers less likely to leave after at data breach
  - Lost business costs declines sharply
  - Well-meaning insiders and malicious attacks are the main causes of data breaches, with more than one-third of incidents involving malicious or criminal attacks
  - Detection and escalation costs declined while notification costs increased
  - Specific attributes increase the cost of a data breach
  - Certain factors reduce the cost of a data breach
- Data breaches continue to have serious financial consequences for organizations
- Organizations are taking security threats more seriously while simultaneously facing an increased number of them
- Organizations are becoming better at managing the costs to respond to and resolve data breach incidents

Thank you!

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.