Cyber risk insurance: What’s the big deal?

Oliver Brew - LIU

Lauri Floresca – Woodruff Sawyer

Mickey Estey – RT Specialty

Winston Krone – Kivu Consulting

Tom Kang - ACE

Liberty International Underwriters.

Topics

- Brief history
- Market drivers
- Threat landscape
- The insurance process
- Breach Response
- Real-life claims situations
- Future gazing

Insurance history lesson

- 1997: First ‘internet liability’ policy written
- 1999: Y2K catalyst to focus on technology risk
- 1999 – 2002: Dot-com bubble - first phase growth
- 2003: CA 1386 (first notification law)
- 2005 – 2010: Breaches on the rise and increasing regulation
  - 2007: TJX breach
  - 2009: Heartland Payment Systems
- 2013: HIPAA final rule
- Compared to auto insurance…?

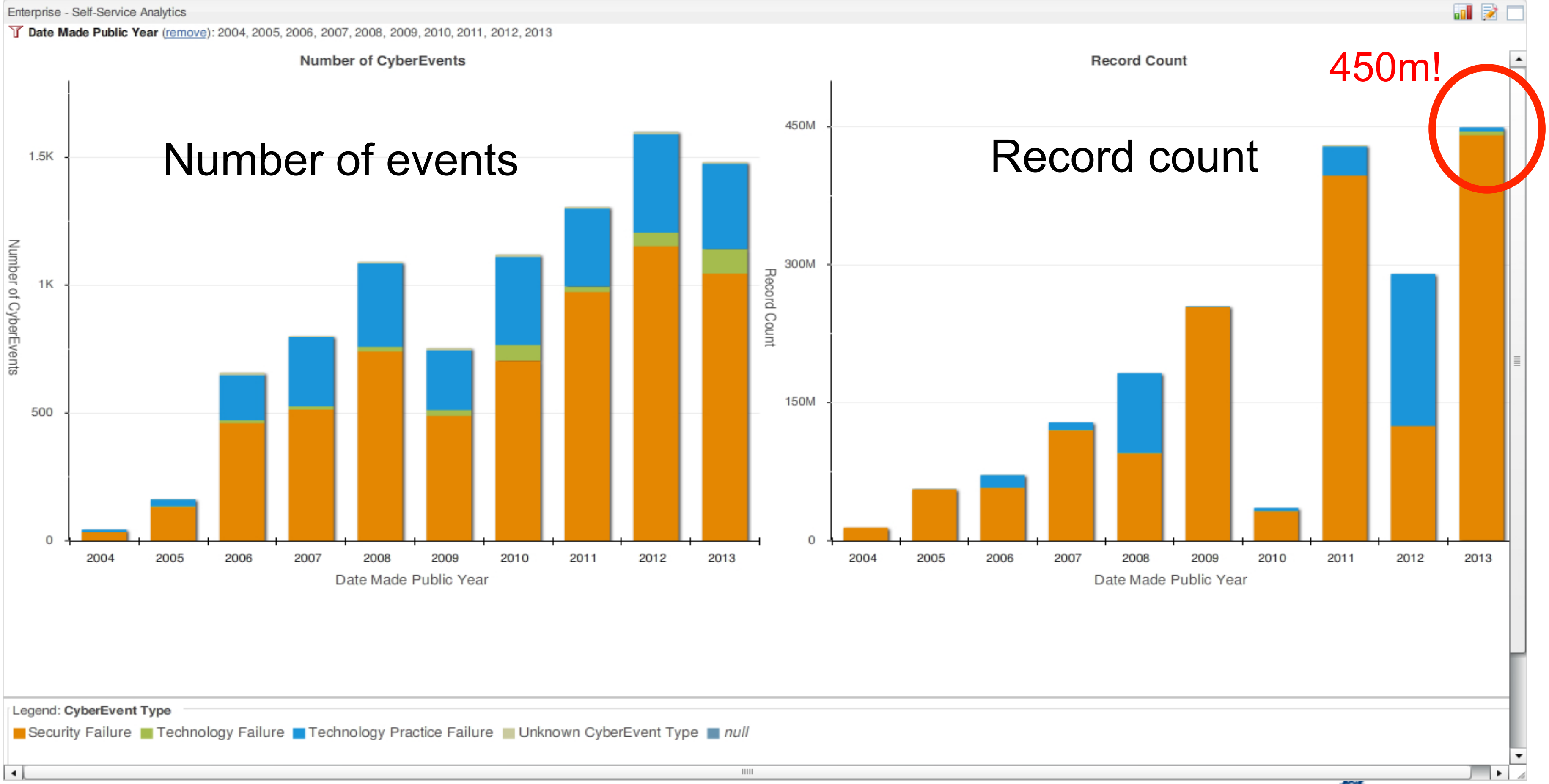
Liberty International Underwriters.

Why the market is taking off

- Data breaches are not going away
- Continued legislation and litigation
- Active regulators flexing muscles
- Boards recognizing it is the “right thing to do”
  - SEC Guidance October 2011
- Increasing contractual obligations for specific privacy / security coverage

Data breach history

Total Cyber Events and Records Breached* (2004 – 2013)



Enterprise - Self-Service Analytics

Date Made Public Year (remove): 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013

Number of events

Record count

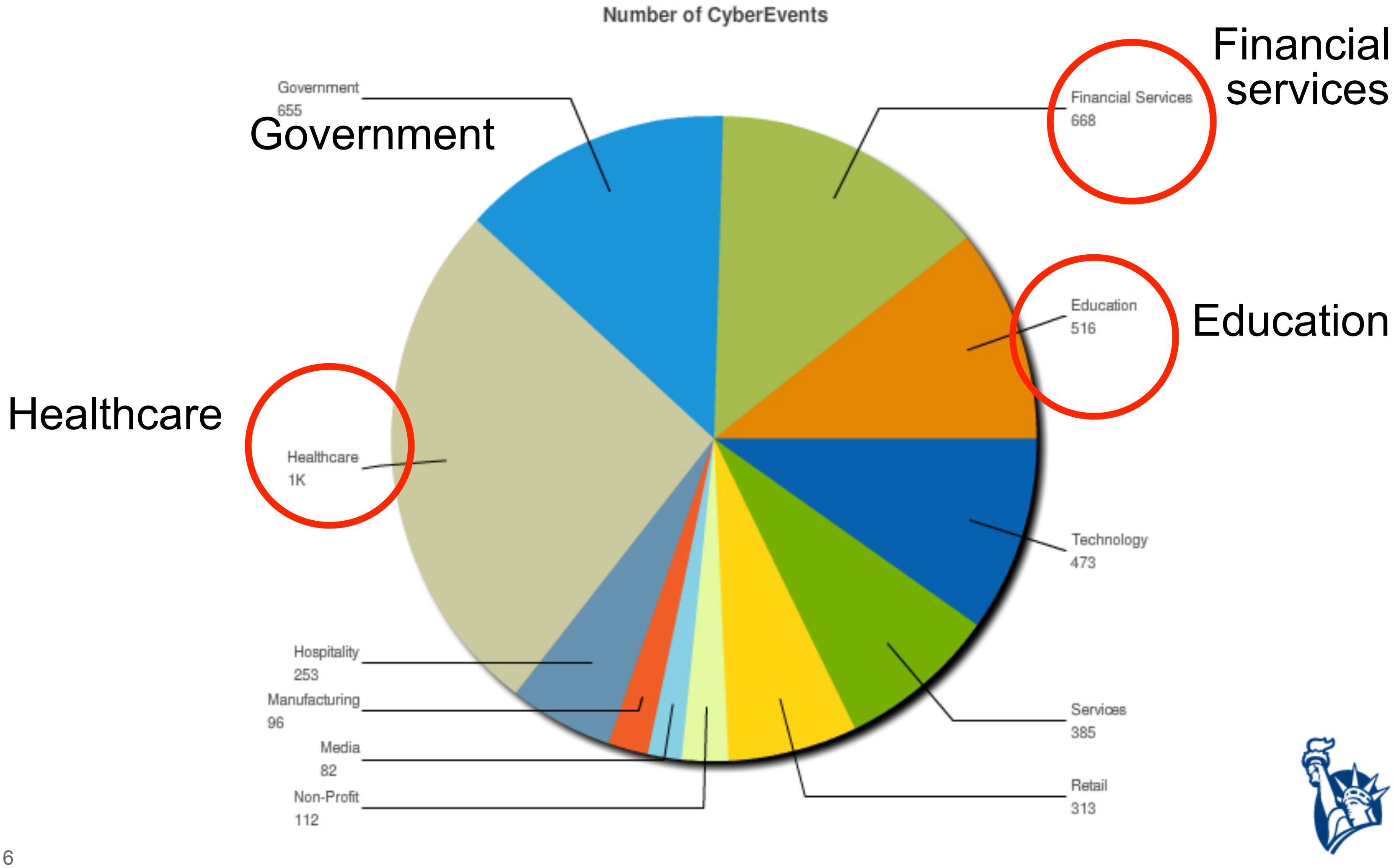
450m!

*Only Depicting Events with losses >30K Records

Liberty International Underwriters.

Range of industries impacted

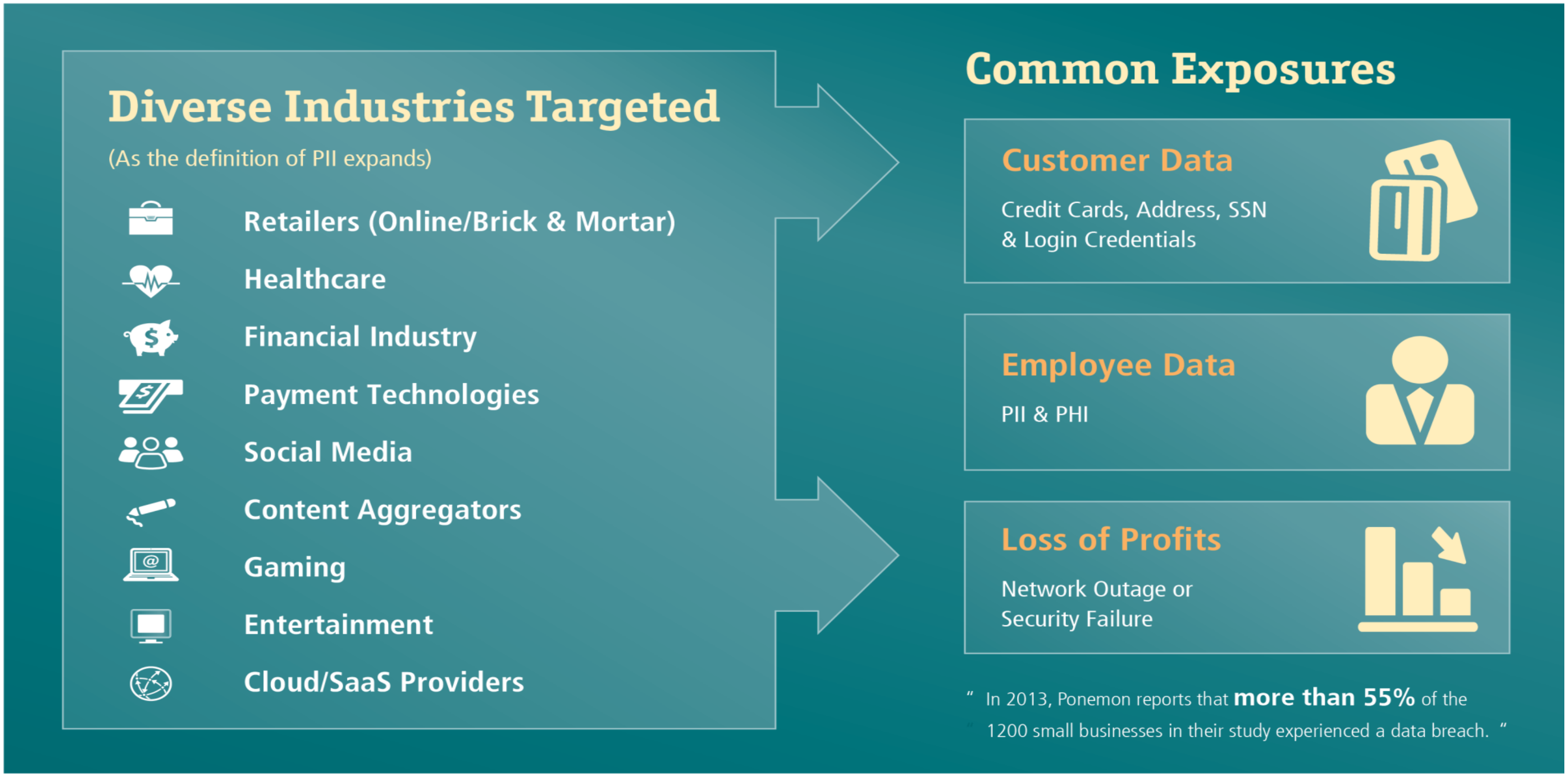
Cyber Events By Industry (2009 – 2014) *US Companies only



All companies have cyber risk

There are two types of companies:

Those that have had a security breach, and those that don’t know they’ve had a breach.



Diverse Industries Targeted

(As the definition of PII expands)

- Retailers (Online/Brick & Mortar)
- Healthcare
- Financial Industry
- Payment Technologies
- Social Media
- Content Aggregators
- Gaming
- Entertainment
- Cloud/SaaS Providers

Common Exposures

Customer Data

Credit Cards, Address, SSN
& Login Credentials

Employee Data

PII & PHI

Loss of Profits

Network Outage or
Security Failure

“ In 2013, Ponemon reports that **more than 55%** of the 1200 small businesses in their study experienced a data breach. ”

Common cyber exposure misconceptions

" We use a third party payment processor, so we've transferred that exposure. "

- A data breach can occur while your customers' data is in transit, not just while it is sitting at the payment process.
- Even if it happens at the payment processor, you are still responsible under privacy breach laws.
- Even if it is your payment processors' fault, they have likely limited their liability so your chance of recourse is slim.

" We don't store any credit cards or PII on our network. "

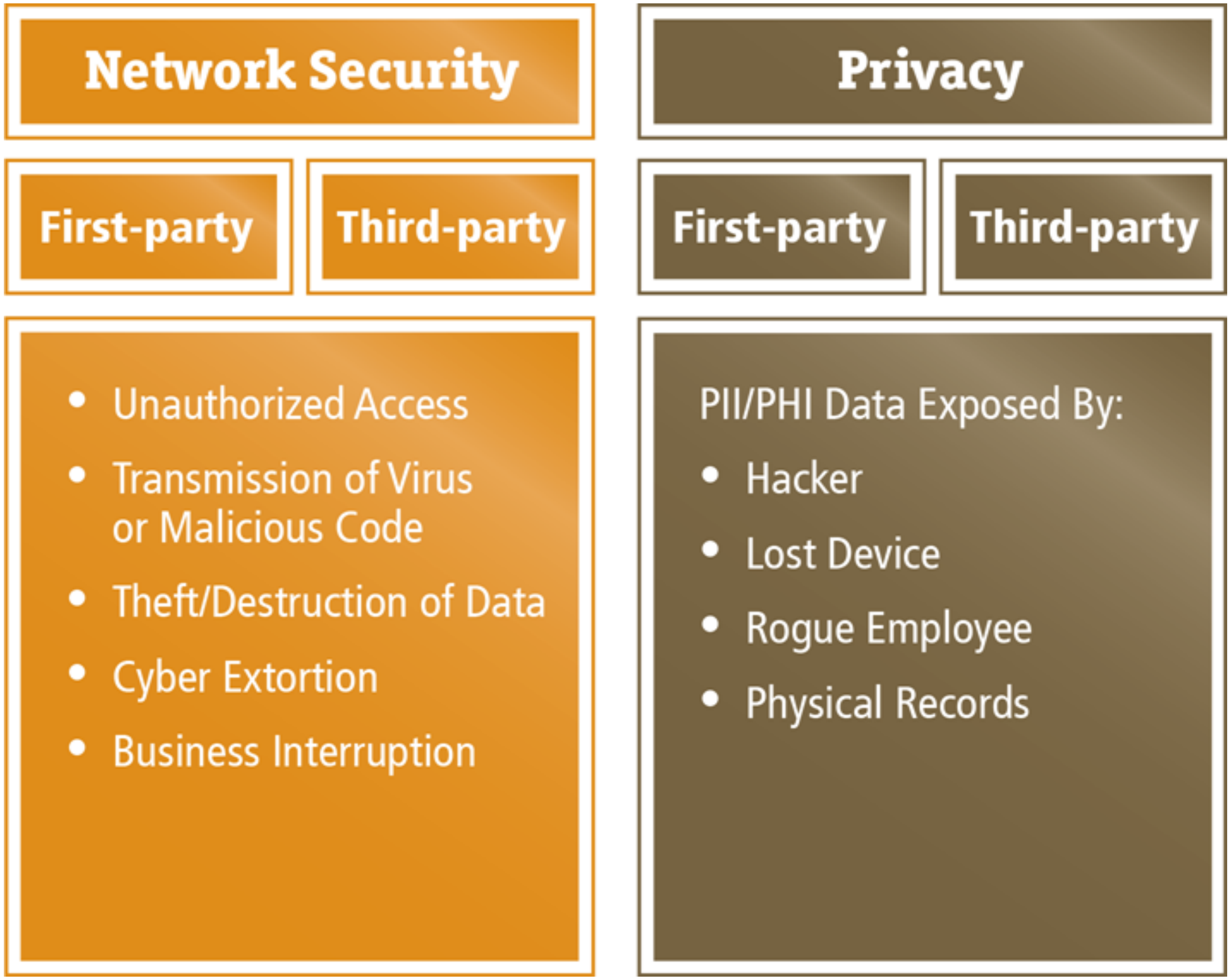
- In some cases hackers have been able to intercept data in real time, "skimming" credit card, data, passwords and other sensitive information.

" We have upgraded our security by transferring our data to a cloud provider. "

- This is often true—major cloud providers have the resources and scale to invest in much higher security than most business. And yet, no security is foolproof.
- The aggregation of data in the cloud may prove to be an attractive target for high-tech criminals.
- The same caveats apply as for outsourced payment processing (above).

Liberty International Underwriters.

Cyber Liability Exposure Overview



Network Security

First-party

Third-party

- Unauthorized Access
- Transmission of Virus or Malicious Code
- Theft/Destruction of Data
- Cyber Extortion
- Business Interruption

Privacy

First-party

Third-party

PII/PHI Data Exposed By:

- Hacker
- Lost Device
- Rogue Employee
- Physical Records

Liberty International Underwriters.

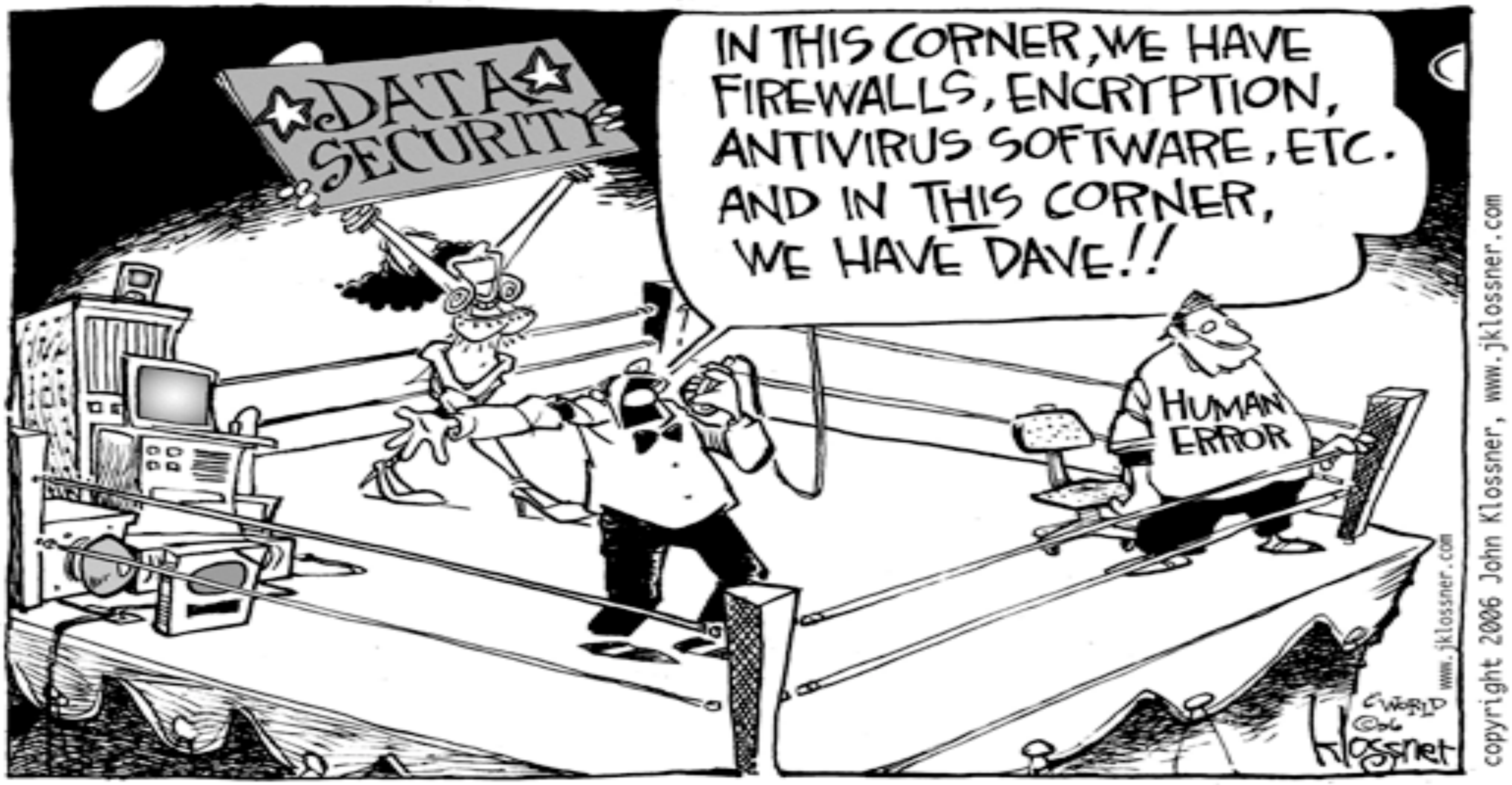
The market today

- **Capacity Available: $200M-$300M in total**
  - 20-30 insurers serving different segments of the market
  - Less availability of Business Interruption coverage (especially contingent)
- **Target breach impacting carrier appetites for large risks**
  - High excess pricing (above 50M) increased substantially.
- **First party sub-limits increasing**
  - Carriers will generally offer 50% to 100% of their total limit
  - Programs can be structured to drop down over 1st party limits to build capacity

Threat landscape

- Internal threats: employee risk (malicious / inadvertent)
- External threats
- Regulatory regime
- Litigation on the increase

The Weakest Link


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
©WORLD ©06
klossner
www.jklossner.com
copyright 2006 John Klossner, www.jklossner.com

Hacking: the glamorous threat

- Hacktivism - Anonymous
- Organized financial crime
- “Just because I can”
- State sponsored…?

Ever-increasing regulatory oversight

- HIPAA / HITECH
  - Notice within 60 days when PHI is breached
  - Requires notice to Secretary of HHS
  - Allows State AGs to bring civil actions for HIPAA violations
- FTC
  - Section 5 authority
- Industry specific regulators:
  - PCI DSS: Cardbrands (visa, MC, Amex)
- 47 State notification laws
  - Affirmative laws

Preparing for the insurance process

- Bring stakeholders together
- Gap analysis
- Benchmarking against various compliance standards
  - PCI DSS, ISO27001, HIPAA, NIST, SSAE16…
- Complete application
- Review quotations
- Bind cover and sleep easy

Underwriting factors

- Industry
- Size of company
- Type and volume of data
- Risk management
  - People
  - Process
  - Technology
- Incident response
- Claims

Current hot button issues for insurers

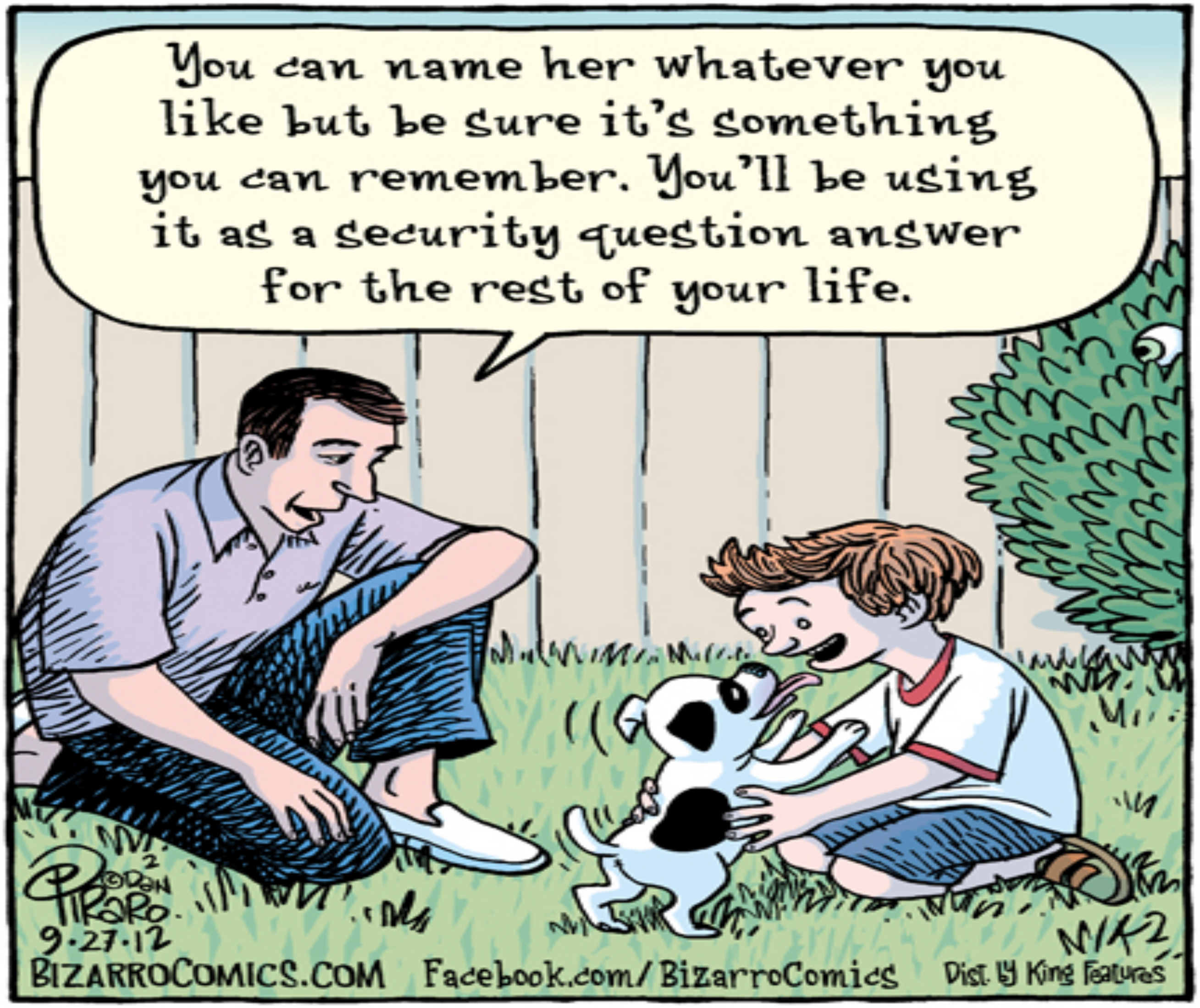
- Data/Confidential Info – Types/How much?/location
- Encryption (Safe harbor) – At rest, in motion, backup, mobile devices
- POS Systems & Software – Patches/updates/controls
- Use of cloud vendors – who and what services (payroll, payments, services, etc.)
- Vendor Controls – Due Diligence/ Contracts/Data shared/Access control
- Network Access – How and who accesses your network remotely?
- Subsidiary acquisitions – Due diligence, conversion process
- Compensating controls – What else are you doing?

Liberty International Underwriters.

Safeguard controls

- ***People***: proper security budget and vigilance
- ***Processes***: ISO27002, HITECH ready; employee education and training; written management processes; breach response plan
- ***Technology***: firewalls; intrusion detection software; hardened and patched servers (tested); encryption of PII

Employee awareness


You can name her whatever you like but be sure it's something you can remember. You'll be using it as a security question answer for the rest of your life.
©Dan Piraro 9.27.12
BIZARROCOMICS.COM
Facebook.com/BizarroComics
Dist. by King Features

Liberty International Underwriters.

Risk management strategies

- “But we spend money on IT security”

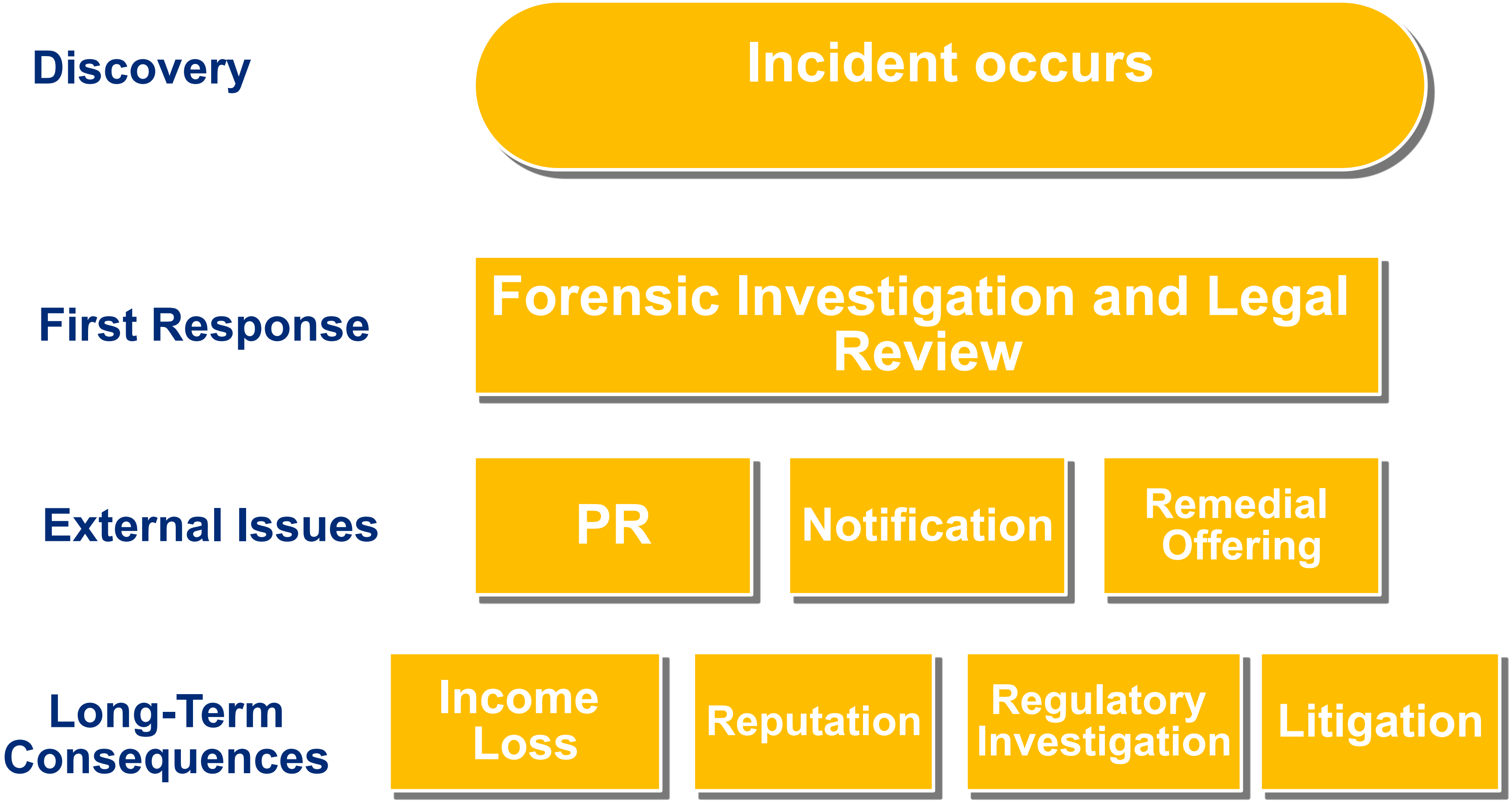
Insurance 🚫 vs IT security spending

- There is always residual risk, as long as people are involved

Breach Response

- Claims handling – not just lawyers
- Data breach first responder
  - Hand holding / consultative
- Specialist services:
  - Forensics
  - Breach notification services
  - Call centres
  - Crisis management
- A well-handled breach does not mean a crisis

Simplified Data Breach Timeline



Discovery

Incident occurs

First Response

Forensic Investigation and Legal Review

External Issues

PR

Notification

Remedial Offering

Long-Term Consequences

Income Loss

Reputation

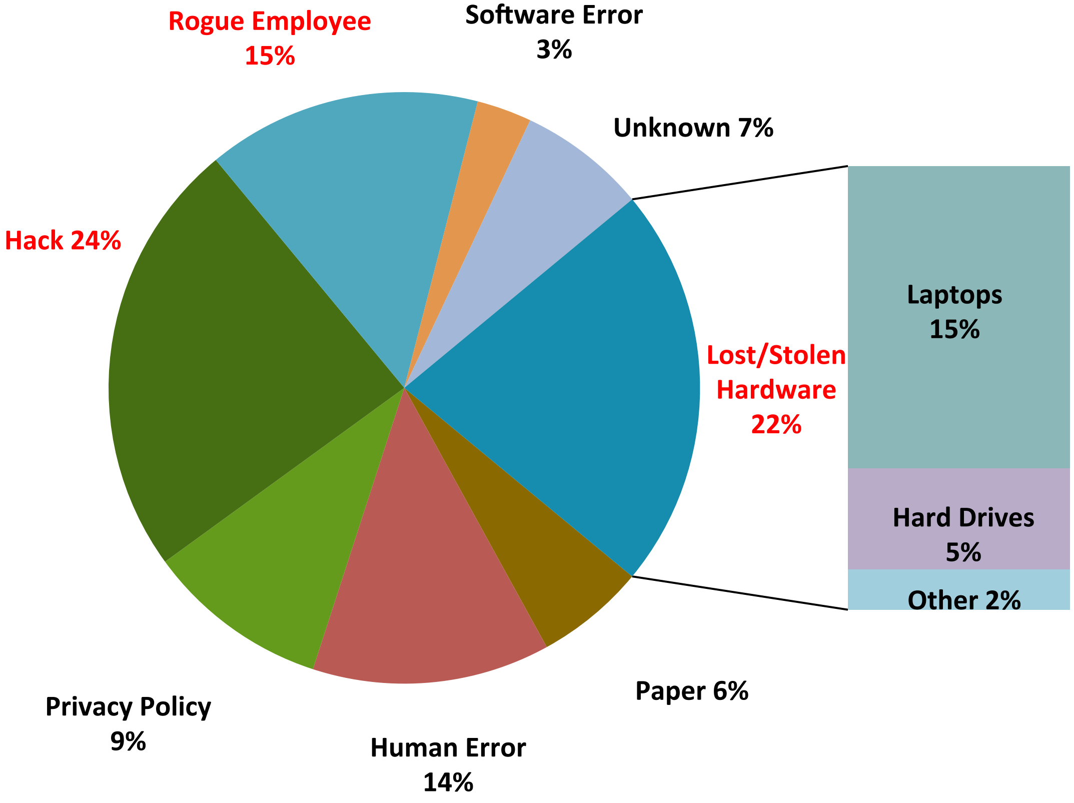
Regulatory Investigation

Litigation

What Should Happen When a Breach Occurs?

- Don’t panic
- Action incident response plan
  - Team
  - Is it a privacy matter?
- Handle regulators / laws
- Tell insurers / lawyers (privilege) and keep informed
- Fastest response not always most appropriate
- Protect evidence / data trails
- Debrief / lessons learned

Claims and Industry Trends (ACE Data)



Industry Breakout

- Healthcare – 31%
- Technology – 14%
- Professional Services – 12%
- Retail – 10%
- Financial Institutions – 8%

Targeted Attacks for PI:

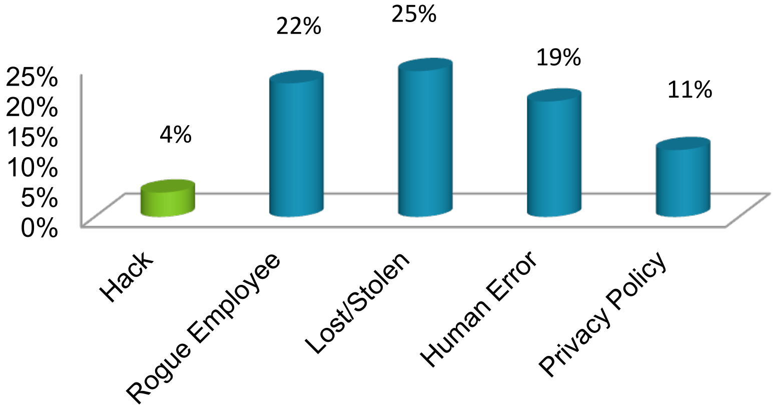
- Lost/Stolen Devices
  - 2008 – 41%
  - 2012 – 17%
  - 2013 – 17%
- Hacking and Rogue Employee
  - 2008 – 31%
  - 2012 – 44%
  - 2013 – 44%

ACE insured.™

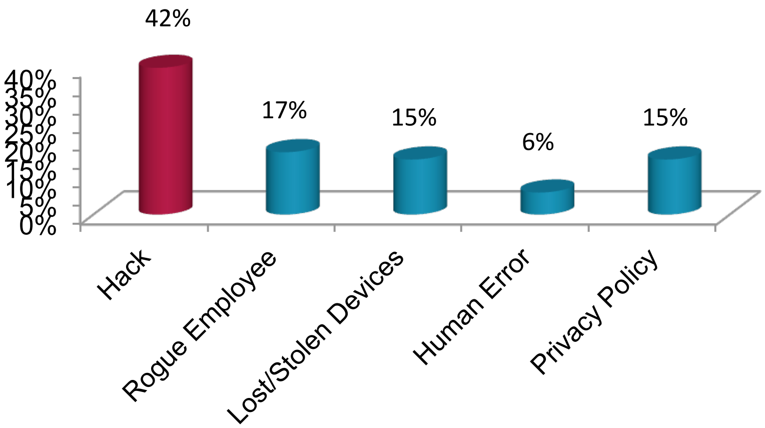
This presentation is solely for informational purposes. It is not intended as legal advice. It may not be copied or disseminated in any way without the written permission of a member of the ACE Group. ©Copyright 2014

Triggers by Industry Segment (ACE Data)

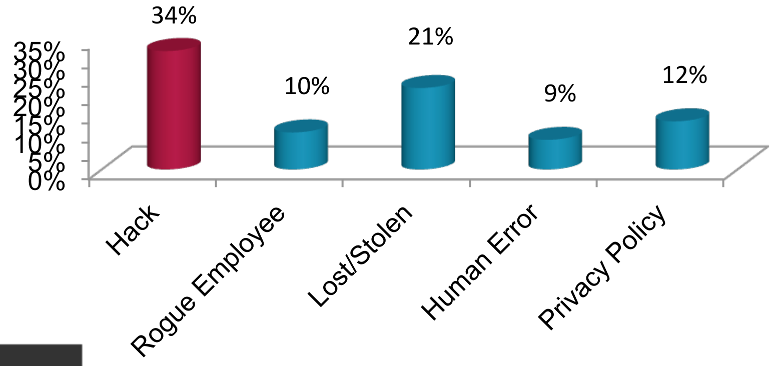
Healthcare



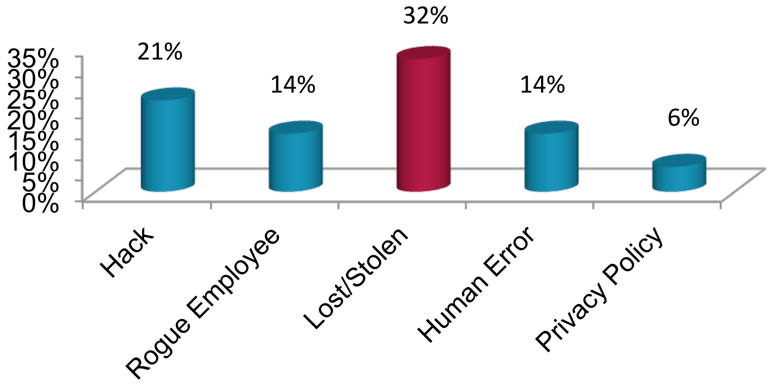
Retail



Technology



Professional Services

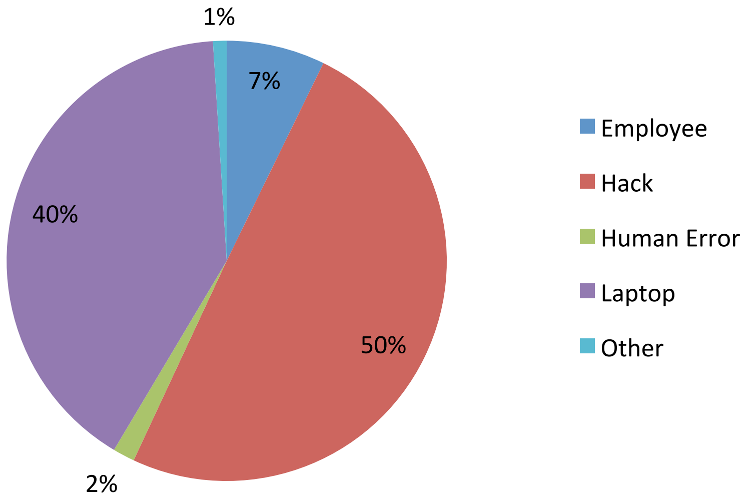


This presentation is solely for informational purposes. It is not intended as legal advice. It may not be copied or disseminated in any way without the written permission of a member of the ACE Group. ©Copyright 2014

How Much Does It Cost?

- Ponemon Institute Study
  - 2014 - $201 per record; Average total cost - $3.5M
  - 2013 - $188 per record
  - Both direct and indirect expenses

Cost by Trigger (ACE DATA)



Every Breach Response is Unique

Cost Range of Each Service

- Legal Fees:
  Under $5,000 up to about $350,000
- Forensics:
  About $10,000 to Seven Figures
- Notification & Call Center - three ways to notify, but approximately $3 per record
- Credit Monitoring:
  Payment per Enrollee or Restoration Service
- Crisis Management Costs

Objectives: Protect your Brand and Limit Third Party Exposure

ACE insured.™

This presentation is solely for informational purposes. It is not intended as legal advice. It may not be copied or disseminated in any way without the written permission of a member of the ACE Group. ©Copyright 2014

Loss Example 1 – Spear Phishing

Situation

- Employee receives email link from a vendor regarding a procedural update
- Employee complies, downloads spyware/malware onto computer network
- Malware manipulates employee's email and sends additional phishing emails to external contacts
  - Phishing emails are opened and placed on 3rd party networks

Covered Costs

- Network Security Liability — $1,500,000 for legal fees and 3rd party suits stemming from the cost to repair their damaged networks

Lessons Learned

- ✓ Coverage for customer/employee information
- ✓ Regulatory proceeding coverage extends to Privacy and Network Liability
- ✓ Network Liability arises out of the failure of network security, including unauthorized access and use of corporate systems

This presentation is solely for informational purposes. It is not intended as legal advice. It may not be copied or disseminated in any way without the written permission of a member of the ACE Group. ©Copyright 2014

Loss Example 2 – Skimming Devices

Situation

- Large retailer discovers compromised pin pads in multiple stores
- Based on investigation, someone tampered with pin pads to capture CC information
- Addresses of impacted customers not available, retailer conducts substitute notice/notifies applicable regulators
- Incident results in four separate class action lawsuits
- Court grants insured's motion to dismiss for plaintiffs' lack of standing based on Clapper

Covered Costs

- $350,000 for legal, forensics and crisis management costs
- $700,000 for defense costs

Lessons Learned

- ✓ Most breach notification statutes provide three ways to notify individuals
- ✓ Most lawsuits result in filing of multiple pleadings
- ✓ Use of crisis management services can be critical if there is media attention on the breach

ACE insured.™

This presentation is solely for informational purposes. It is not intended as legal advice. It may not be copied or disseminated in any way without the written permission of a member of the ACE Group.

Loss Example 3 – PCI Fines

Situation

- Users of $250 million online retailer’s website began experiencing fraudulent credit card charges
- Retailer’s web hosting company conducts a review of data stored on the servers
  - Virus found and removed
- Breach results in compromise of ~1 million records and fraudulent use of 50 credit cards
- Retailer incurs fines/penalties for not being Payment Card Industry (PCI) compliant

Covered Costs

- $750,000 for notification, call center services and legal fees to determine the insured’s regulatory obligations
- $500,000 in assessments for lack of PCI compliance

Lessons Learned

✓ Important to research breach response vendors prior to a breach

✓ Understand PCI compliance and engage proper QSA

✓ Assessments for PCI DSS non-compliance can be significant

insured.™

This presentation is solely for informational purposes. It is not intended as legal advice. It may not be copied or disseminated in any way without the written permission of a member of the ACE Group. ©Copyright 2014

The last word

“We’ve spent over 12 years building our reputation, brand, and trust with our customers. It’ s painful to see us take so many steps back due to a single incident.”

-Zappos CEO Tony Hsieh

“Everyone has a plan… until they get punched in the face”

- Mike Tyson

The future

- $5Bn market before 2020*
- Continued expansion of buyers
- Market consolidation:
  - Specialists
  - Everyone else offering add-on
- IT risk integrated as part of enterprise risk management
- Network risk only increasing

*Advisen Research