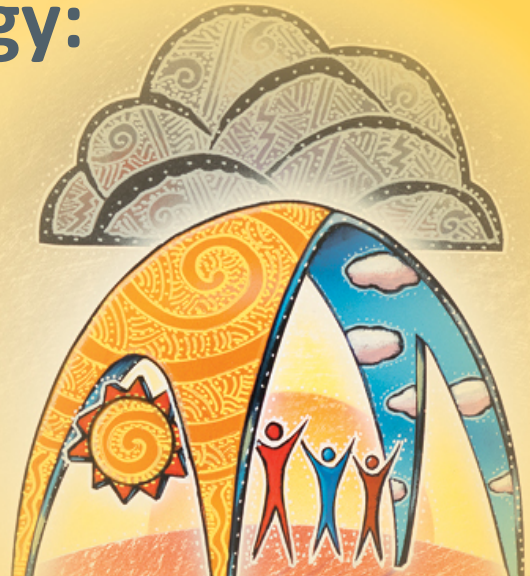
RLI
DIFFERENT WORKS

RLI PROFESSIONAL SERVICES GROUP
PROFESSIONAL LEARNING EVENT
PSGLE 108

Cyber, Privacy and Technology: Data Privacy 101



Copyright Materials

This presentation is protected by US and International Copyright laws. Reproduction, distribution, display and use of the presentation without written permission of the speaker is prohibited.

© RLI Professional Services Group

RLI®
DIFFERENT WORKS

COURSE DESCRIPTION

No one is immune from data breaches. There are more than a handful of types of data security breaches, and data security is threatened in a number of different ways. Professionals often have access to their clients' personal and financial details. Laws protect "personal information," and professional service firms are obligated to abide by those laws. How can professional service firms protect themselves against—or at least prepare themselves for—what could be an inevitable breach?

LEARNING OBJECTIVES

Participants in this course will learn about:

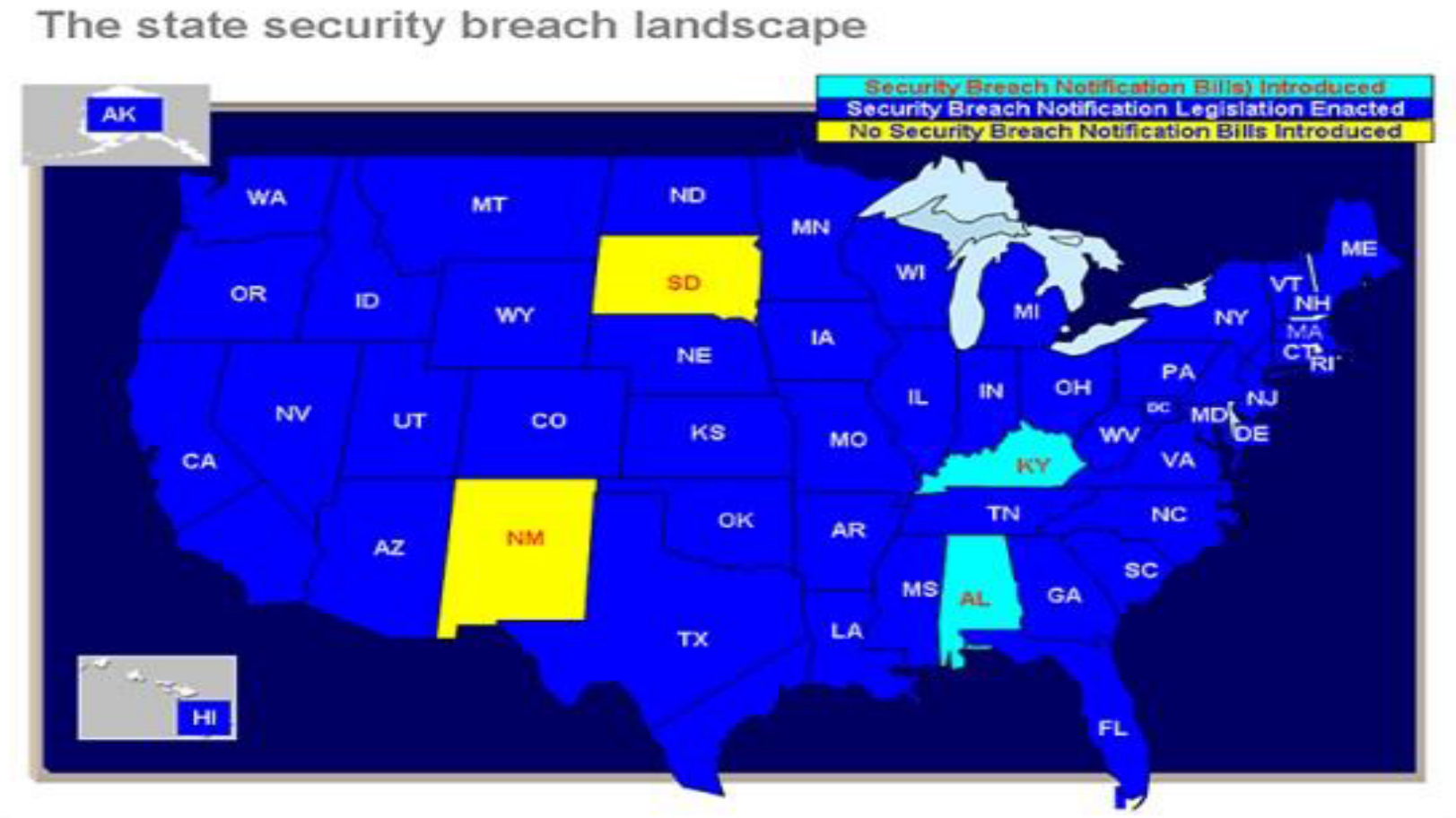
- The evolution of data breach laws
- Data breach at a glance
- Security best practices
- Key protections under cyber, privacy and technology insurance coverage
- Incident response best practices
- How to minimize the impact of suits if they occur

Laws protect “personal information”

Individual first name or initial + last name plus the following:

- ✓ User IDs, passwords, mother’s maiden name, answers to other security questions
- ✓ Government identification number (driver’s license, SSN)
- ✓ Financial account numbers and security codes
- ✓ Employee identification number
- ✓ Biometric data: fingerprints
- ✓ Medical Information/ Personal Health Information(PHI)
- ✓ Personally Identifiable Information(PII)

DATA BREACH LAWS VARY BY STATE



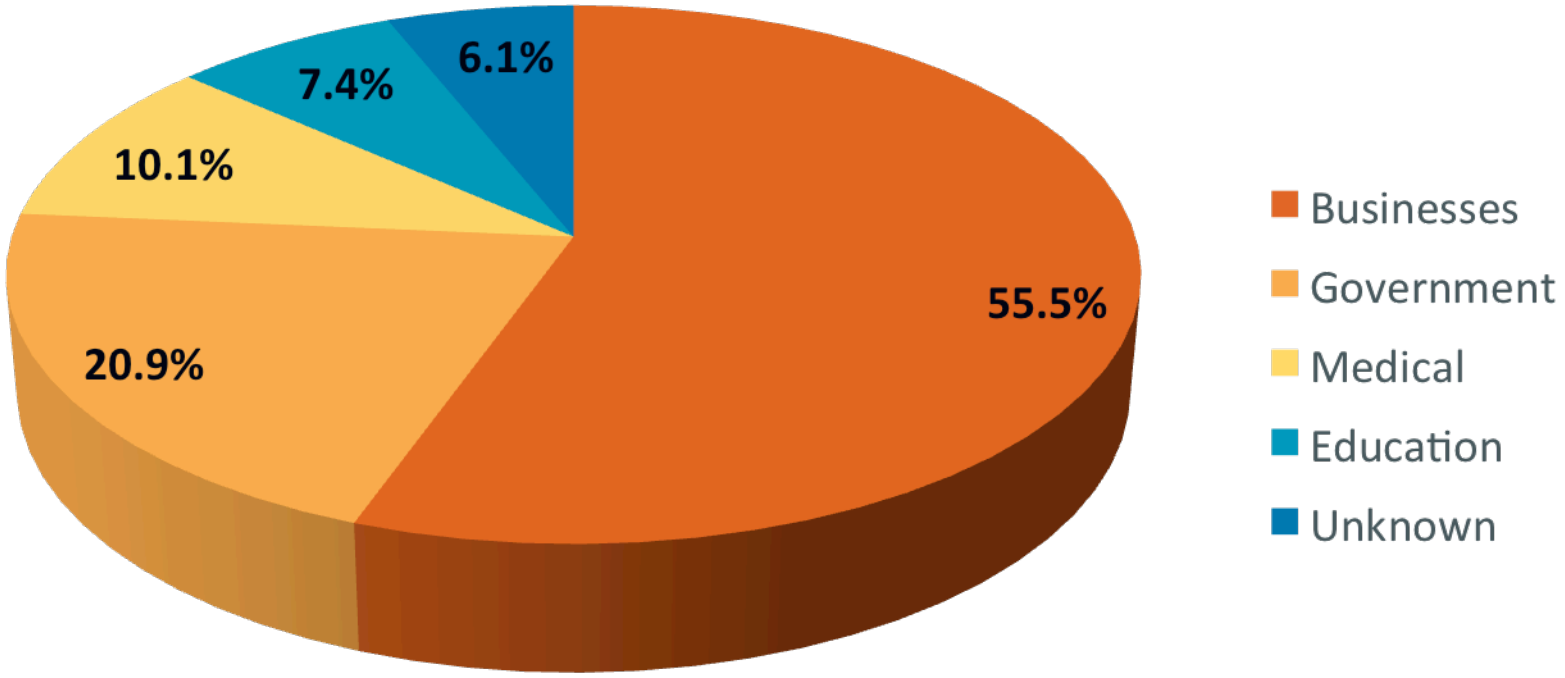
Source: NetDiligence

To notify or not to notify…

Varies by state, but may not be required when:

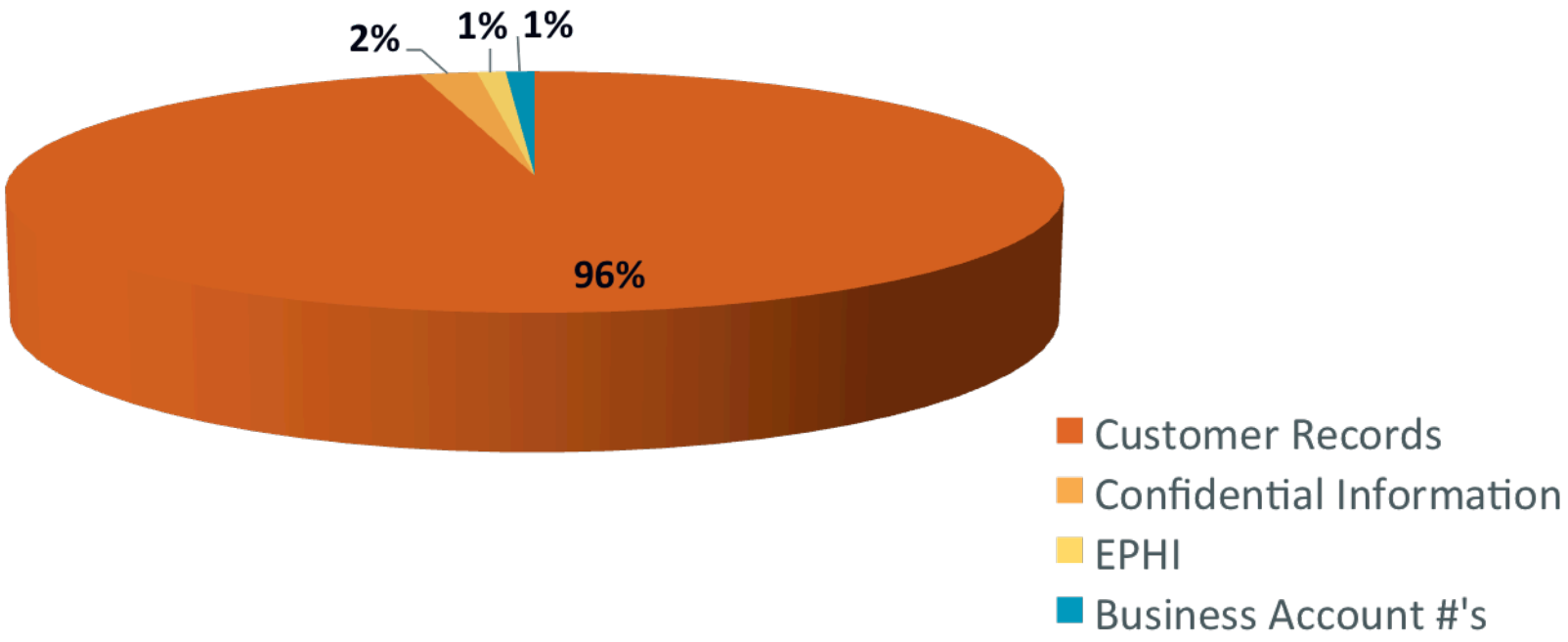
- Breached data is protected by at least 128-bit encryption
- Breached data elements are not considered "protected"
- Breach was stopped before information was wrongfully acquired
- Data was accessed by an unauthorized employee but the data was not used or further disclosed

Percentage of Reported Incidents



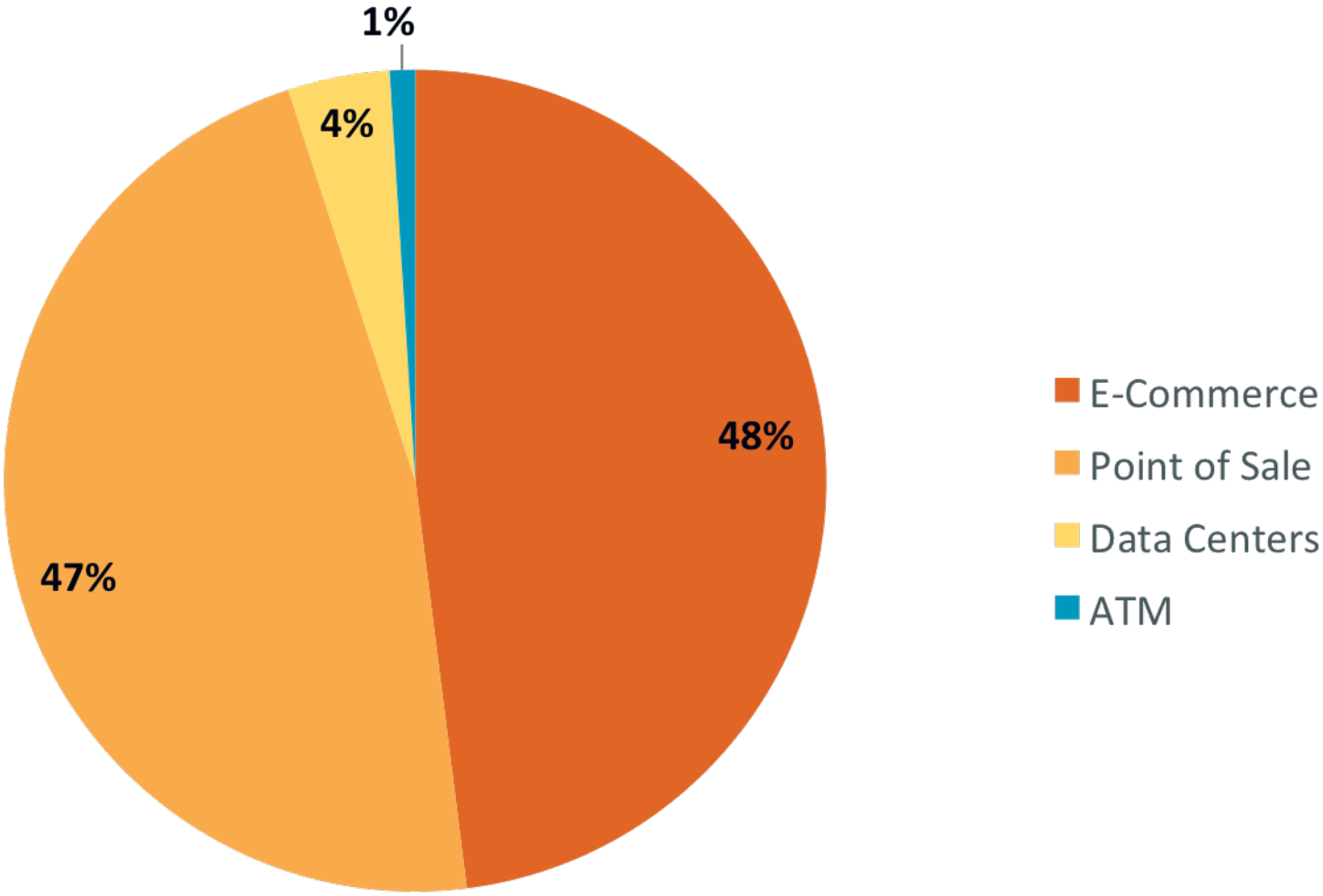
Source: Risk Based Security

Types of Data Targeted



Trustwave 2013 Global Security Report

Top Target Assets



Trustwave 2013 Global Security Report

HOW DOES A SECURITY BREACH HAPPEN?

Inside Threats

- Employee negligence
  - ➢Security failures
  - ➢Lost mobile devices
- Employee ignorance
  - ➢Improper disposal of personal information (dumpsters)
  - ➢Lack of education and awareness
- Malicious employees

Outside Threats

- Hackers
- Malware
- Phishing
- Thieves (including Social Engineering Tools)
- Vendors

…and the statistics show

Hacking remained the leading cause—**72.5%** of cyber incidents

Hacking accounted for **21.9%** of exposed records

Insiders accounted for:

- 17.1% of reported incidents
- 67.6% of exposed records

Insider wrong-doing accounted for:

- 6.2% of reported incidents
- 57.5% of exposed records

Insider errors accounted for:

- 7.8% of reported incidents
- 5.2% of exposed records

Source: Risk Based Security

MOBILE TECHNOLOGIES: A CLOSER LOOK

What are they?

- ✓ Laptops and tablets
- ✓ Smart phones
- ✓ USB thumb (Flash) drives
- ✓ Cloud technologies (storage)

Their Importance in risk and liability

- ✓ Consumer demand and preferences
- ✓ Increased mobility = increased exposure
- ✓ More ways to spread, share, and lose information
- ✓ Struggle for businesses (especially small) to protect these emerging technologies and tools
- ✓ Whether lost or stolen, laptops and any mobile devices that hold data are a consistent and expensive threat
- ✓ 35% of breaches involved lost devices

KEY RISK CONTROLS

- Employee Training/ Awareness
- Policies
  - Privacy policies
  - Information security policies
  - Computer usage policies
- Personal Information Inventory
- Anti-virus programs
- Access controls (firewalls, passwords)
- Contractual and (Reasonable) Risk-Based Oversight Controls for Third-Party Handling of Personal Information
- Know applicable laws

KEY RISK CONTROLS

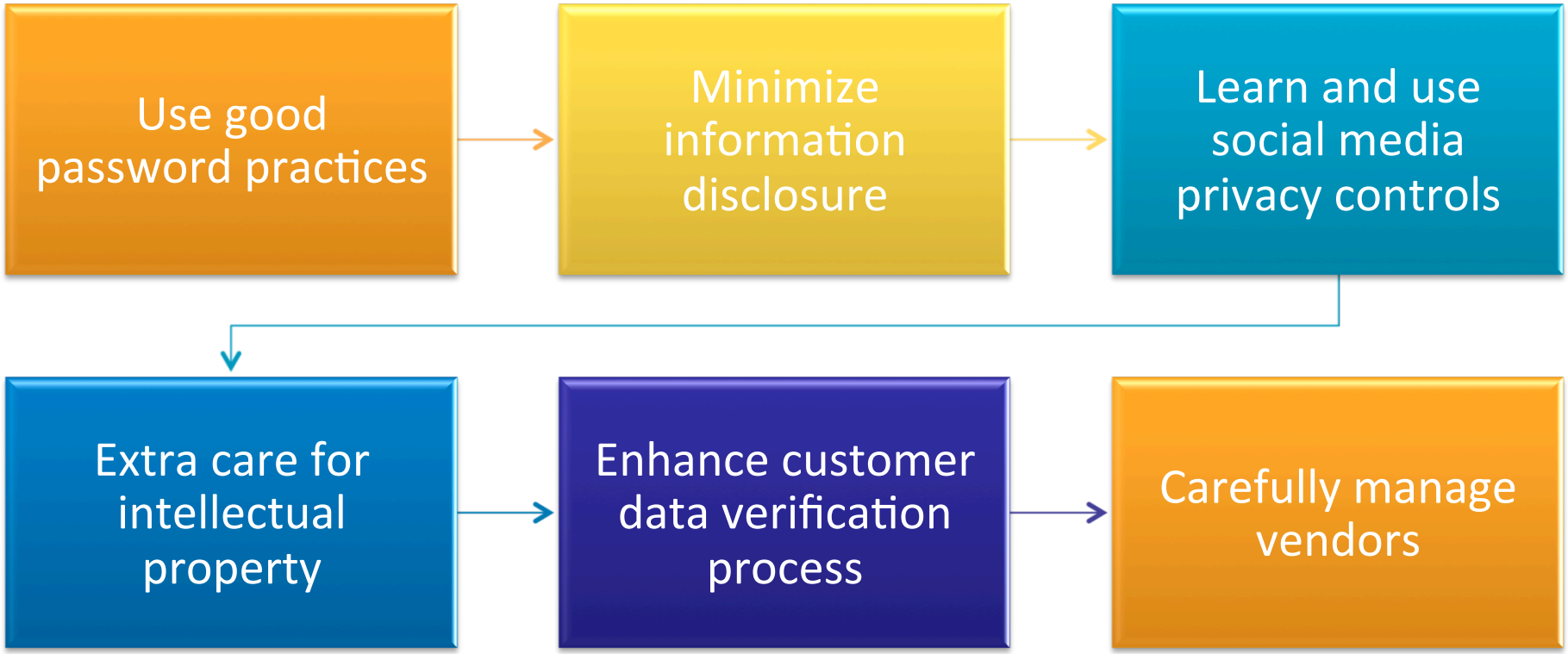
Employee awareness and training

- ✓ Educate all employees on the importance of data and information security
- ✓ Conduct security awareness training
- ✓ Create a culture of proactively managing cybersecurity risk
- ✓ Implement policies for system access
- ✓ Help employees understand what to look for in identifying a potential security breach

KEY RISK CONTROLS

- Use a dedicated computer for online banking
- Do not collect what you do not need
- Do not keep data unnecessarily
- Do not forget physical security
- Run current version of anti-virus program
- Install and maintain firewalls
- Manage your wireless network
- Keep applications patched

KEY RISK CONTROLS



VENDOR MANAGEMENT

In 63% of incident response investigations, a major component of IT support was outsourced to a third party responsible for system support. (2013 Trustwave Global Security Report)

Key principles of vendor risk management:

- Research and due diligence
- Contractual risk transfer
- Continuous monitoring and auditing

BUILD YOUR TEAM

Be ready with name, mobile phone, email

- ✓ Leadership
- ✓ IT
- ✓ Communications / PR
- ✓ Customer Relations
- ✓ Privacy Experts
- ✓ Outside legal counsel
- ✓ Insurance company

COLLABORATE

Identify and coordinate your plans with:

- Computer forensic consultants
- Other risk avoidance/ crisis management consultants

RETAIN EXPERIENCED LEGAL COUNSEL

- cyber incident avoidance
- loss mitigation and breach response plans
- updates on legal developments
- monitoring competitors' and others' security practices

AUDIT

Periodically audit:

- ❑ Administrative
- ❑ Technical
- ❑ Physical infrastructure

Reaffirm that they are **properly protected**.

P4–privacy protection package for designated professionals

What do the seven insuring clauses cover?

1. **Enterprise Privacy Liability** –Liability as a result of a privacy breach (lost/ stolen laptop, dumpster diving, paper theft)

2. **Network Security Liability** –Liability as a result of a network security breach (virus, denial of service attack, etc.)

3. **Electronic Media Liability** – Liability as a result of information posted on the Insured's website

4. **Crisis Management** – Costs associated with responding to a network security or privacy breach – Public relations, Legal, Notification, Credit monitoring, Forensics

P4–privacy protection package for designated professionals

What else do the seven insuring clauses cover?

5. **Network Interruption Business Income & Extra Expense (BIEE)** – Business income and extra expense as a result of a network security breach

6. **Data Loss** – costs to replace, restore, or recollect corrupted data

7. **Cyber Extortion** – costs and expenses associated with an extortion attempt

   - ✓ Denial of service attack
   - ✓ Release or destroy private information
   - ✓ Corrupt, alter, steal, destroy, delete, or damage data asset or the computer system
   - ✓ Interrupt or suspend computer system

we already have coverage, don't we?

General Liability - Significant coverage issues

Likely no coverage for:

- Bodily Injury
- Property Damage
- Personal/advertising injury

Exclusions may apply:

- Electronic data
- Professional Services
- Contractual Liability
- Care, custody & control

Are you sure we don't have this coverage?

Property- Potentially Some Coverage

Limited Coverage:

- Business Income/Extra Expense due to electronic vandalism
- Data Loss due to electronic vandalism

No Coverage:

- Crisis Management Expenses (notification, credit monitoring, forensic)
- Cyber Extortion (ransom)

CLAIMS STATISTICS

Average cost per breach: **$1 million**

11% of the claims involved companies in the **professional services sector**

Cost of a cyber incident ranged from **$13,000 to $10.5 million**

A **typical claim** costs **$25,000 to $400,000**

Mean for **crisis management services** was $346,000 per incident, including:

- Forensics
- Notification
- Call center services
- Credit monitoring
- Legal guidance– averaging $258,000

June 2013 Report from NetDiligence

FREQUENT ALLEGATIONS OF A PRIVACY BREACH

- Failure to protect customer information/privacy
- Reduction in value of claimants' PII
- Failure to notify/timely notify
- Cost to reissue cards/open new accounts
- Cost of fraudulent purchases
- Cost to inspect and repair computing devices
- Redress—
  - credit monitoring
  - identity theft insurance
- Regulatory Actions—fines and penalties

Claim Examples

Example of Enterprise Privacy Liability

- An employee loses his company laptop. The laptop contains copies of patient medical records. A class action lawsuit was filed against the company for damages resulting from their failure to protect personal and confidential information.

Example of Network Security Breach

- An employee's company laptop was stolen from a bar during Happy Hour. The laptop contains private financial information of its customers. The employee did not have proper network security protection in place for the laptop and the information was leaked to the public. The customers sue the Company for damages resulting from the employee's failure to protect their private financial information.

CLAIM EXAMPLES

Examples of Electronic Media Liability:

- While preparing a product brochure posted on a the Company's website, an employee includes pictures and diagrams taken from a competitor's marketing material. The company is subsequently sued for copyright infringement.

- The Company's website contains ads and links to their key business partners. The Company is sued by one of their business partner's competitors, who claims the ad displayed on the Company's website infringes on the competitor's slogan.

BREACH RESPONSE

BREACH RESPONSE

Credit monitoring?

Media response?

Who will answer the phone?

Insurance coverage?

Breach response Do's

- Respond quickly (but not too quickly!)
- Bring in the right team
- Preserve evidence
- Contain & remediate
- Let the forensics drive the decision-making
- Document analysis
- Engage outside legal counsel
- Be guarded, consistent, and honest in communications
- Plan for likely reaction of customers, employees, & key stakeholders
- Mitigate harm
- Conduct a data inventory
- Insurance coverage

Breach response Dont's

- Rely on IT for forensics
- Respond slowly
- Hire the wrong forensic team
- Overburden a few
- Or include too many
- Let too many edit documents
- Make notification decision too early
- Make inaccurate or misleading disclosures

- Send notification letter without legal advice
- Forget to preserve data
- Treat notification like a PR campaign
- Forget to notify your insurer

SMALL BUSINESS CYBER SECURITY

Disconnect between concern and action:

- 83% of small businesses allow employee personal devices for work
- 37% of small businesses have suffered a cyber attack
  - 82% of those attacks involved a virus
  - 32% have experienced phishing
- 82% of small businesses have secured laptops but only 32% protect smartphones and only 39% protect tablets

Source: October 2012 AT&T and the Polytechnic Institute of NYU Small Business Cyber Security Key Findings

WHAT DOES IT COST?

Notification Cost Calculator

How many notices do you need to send?	60
How many different versions of the notification letter will you need?	2

Notices

Setup	$1,000
Address List Management	$550
Notice Printing	$170
Postage	$26
Total Cost for Notices	$1,747

Call Center

Setup	$2,800
Fielding In-bound Calls	$8
Total Cost for Call Center	$2,808
Total Notification Cost	$4,555

Reset

NetDiligence in partnership with Immersion

But What if…

Data Breach Cost Calculator

Total Number of Affected Records?	60
Type of Data Breached?	Credit Card
Number of Years for Credit Monitoring?	1
Data is in a centralized system/location?	Yes / No
Actual Fraud is expected already?	Yes / No
Is PCI compliance an issue?	Yes / No
Federal Class Action Lawsuit filed?	Yes / No

INCIDENT INVESTIGATION

Forensics Investigation	$14,008
Security Remediation	$70,008
Data Breach Law Legal Guidance	$10,000
eDiscovery Litigation	$70,042
Subtotal	$164,058

CUSTOMER NOTIFICATION / CRISIS MANAGEMENT

Customer Notification	$60
Call Center	$5
Credit Monitoring	$945
ID Fraud Remediation	$42
Public Relations Service	$14,000
Subtotal	$15,052

REGULATORY AND INDUSTRY SANCTIONS

FTC Fines	$525,000
State AG Fines	$4,200
HHS Fines	$0
PCI Fines	$0
Subtotal	$529,200

CLASS ACTION LAWSUIT

Legal Defense & Damages	$53
Bank Card Reissuance Liability	$360
Subtotal	$413

Total Cost	$708,723
Per Record Cost	$11,812

Reset

Important Information: The numbers presented in the NetDiligence® Data Breach Cost Calculator are estimates and provided for education and illustration purposes only. Actual expenses and liability exposures due to identity theft or data breach incident may vary based on variables not considered in this calculator. Numerical results presented in the Data Breach Cost Calculator are based on a proprietary formula developed by NetDiligence and its insurance industry partners. This formula takes into account information available in the public domain and information obtained through various websites that track breach statistics. Please note: This calculator is not intended to predict insurable perils or related costs and has no bearing on any insurance policy.

RESOURCES

- *www.fcc.gov/cyberplanner*
- *www.dhs.gov/stopthinkconnect*
- *Legal Counsel*
- *Your broker*
- *Your insurance company*

Thank you for your time!

QUESTIONS??

This concludes the Professional Services Group Learning Event

RLI DIFFERENT WORKS

Laurel Tenuto, Client Risk Management Coordinator

Laurel.Tenuto@lrlicorp.com

Marie Bernier, Senior Risk Management Consultant, Professional Enterprise Risk Solutions

Marie.Bernier@rlicorp.com

THANK YOU!