# How Consumer and Retail Businesses Can Prepare for the Next Data Breach

*April 17, 2014*

Pillsbury Winthrop Shaw Pittman LLP

# Agenda

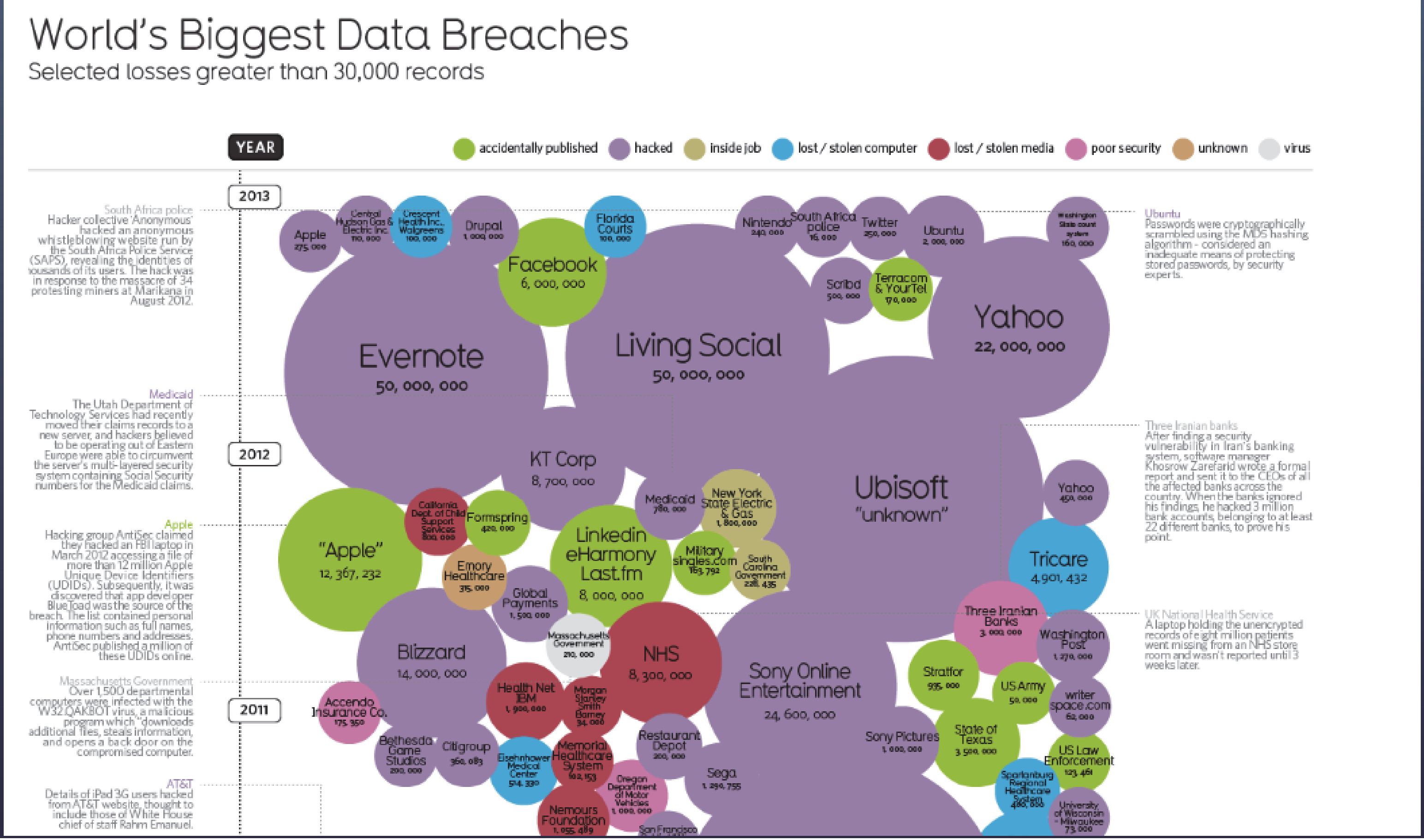
- Introduction and Lessons Learned from Previous Data Breaches
- Risk Management
- Contractual Protections Against Data Breaches
- Cyber Insurance

# The Numbers Are In And It’s Not Pretty…

- *‘Year of the Mega Breach’ for Consumer Data*, Corporate Counsel (Apr. 8, 2014)
- U.S. incurred highest lost business cost, *2013 Cost of Data Breach Study: Global Analysis*, Ponemon Institute (May 2013)
- *Cisco 2014 Annual Security Report*
  - 99% of all mobile malware in 2013 targeted Android devices
  - 91% of web exploits target Java
  - 64% of malware are Trojans, followed by adware at 20%
- *Data Breach Investigations Report, Verizon (2013)*
  - 92% of breaches initiated by external actors, and 52% of breaches result from hacking and 40% from malware
- Reported incidents up 782% from 2006—2012, *National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, U.S. Gov. Accountability Office (Feb. 2013)

# Who Is At Risk? *EVERYONE*

- EVERYONE — www.informationisbeautiful.com



World's Biggest Data Breaches

Selected losses greater than 30,000 records

South Africa police
Hacker collective 'Anonymous' hacked an anonymous whistleblowing website run by the South Africa Police Service (SAPS), revealing the identities of ousands of its users. The hack was in response to the massacre of 34 protesting miners at Marikana in August 2012.

Medicaid
The Utah Department of Technology Services had recently moved their claims records to a new server, and hackers believed to be operating out of Eastern Europe were able to circumvent the server's multi-layered security system containing Social Security numbers for the Medicaid claims.

Apple
Hacking group AntiSec claimed they hacked an FBI laptop in March 2012 accessing a file of more than 12 million Apple Unique Device Identifiers (UDIDs). Subsequently, it was discovered that app developer BlueToad was the source of the breach. The list contained personal information such as full names, phone numbers and addresses. AntiSec published a million of these UDIDs online.

Massachusetts Government
Over 1,500 departmental computers were infected with the W32.QAKBOT virus, a malicious program which "downloads additional files, steals information, and opens a back door on the compromised computer.

AT&T
Details of iPad 3G users hacked from AT&T website, thought to include those of White House chief of staff Rahm Emanuel.

Ubuntu
Passwords were cryptographically scrambled using the MD5 hashing algorithm - considered an inadequate means of protecting stored passwords, by security experts.

Three Iranian banks
After finding a security vulnerability in Iran's banking system, software manager Khosrow Zarefarid wrote a formal report and sent it to the CEOs of all the affected banks across the country. When the banks ignored his findings, he hacked 3 million bank accounts, belonging to at least 22 different banks, to prove his point.

UK National Health Service
A laptop holding the unencrypted records of eight million patients went missing from an NHS store room and wasn't reported until 3 weeks later.

YEAR
● accidentally published
● hacked
● inside job
● lost / stolen computer
● lost / stolen media
● poor security
● unknown
● virus
2013
2012
2011
Apple 275, 000
Central Hudson Gas & Electric Inc. 110, 000
Crescent Health Inc., Walgreens 100, 000
Drupal 1, 000, 000
Facebook 6, 000, 000
Florida Courts 100, 000
Nintendo 240, 000
South Africa police 16, 000
Twitter 250, 000
Ubuntu 2, 000, 000
Washington State court system 160, 000
Scribd 500, 000
Terracom & YourTel 170, 000
Evernote 50, 000, 000
Living Social 50, 000, 000
Yahoo 22, 000, 000
KT Corp 8, 700, 000
Ubisoft "unknown"
Yahoo 450, 000
Medicaid 780, 000
New York State Electric & Gas 1, 800, 000
"Apple" 12, 367, 232
California Dept. of Child Support Services 800, 000
Formspring 420, 000
Linkedin eHarmony Last.fm 8, 000, 000
Military singles.com 163, 792
South Carolina Government 228, 435
Tricare 4,901, 432
Emory Healthcare 315, 000
Global Payments 1, 500, 000
Massachusetts Government 210, 000
NHS 8, 300, 000
Three Iranian Banks 3, 000, 000
Washington Post 1, 270, 000
Blizzard 14, 000, 000
Sony Online Entertainment 24, 600, 000
Stratfor 935, 000
US Army 50, 000
writer space.com 62, 000
Accendo Insurance Co. 175, 350
Health Net IBM 1, 900, 000
Morgan Stanley Smith Barney 34, 000
Bethesda Game Studios 200, 000
Citigroup 360, 083
Eisenhower Medical Center 514, 330
Memorial Healthcare System 102, 153
Restaurant Depot 200, 000
Sony Pictures 1, 000, 000
State of Texas 3, 500, 000
US Law Enforcement 123, 461
Oregon Department of Motor Vehicles 1, 000, 000
Sega 1, 290, 755
Spartanburg Regional Healthcare System 400, 000
University of Wisconsin - Milwaukee 73, 000
Nemours Foundation 1, 055, 489
San Francisco

# *Hot Off the Wire* — “Heartbleed Bug”

- Codenomicon “engineer’s team [] found a potentially serious bug in the world’s biggest open-source encryption service, which is used by pretty much every major site, including places like Google and Facebook, to keep personal information secure.” *Behind the Scenes: The Crazy 72 Hours Leading Up to the Heartbleed Discovery,* Vocativ (Apr. 10, 2014)
  - “[A]llows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.” *Heartbleed Bug, What leaks and how to stop it,* Codenomicon
- “[O]ne of the biggest security threats the Internet has ever seen.” *Widespread Encryption Bug, Heartbleed, Can Capture Your Passwords,* Mashable (Apr. 8, 2014)

# *Hot Off the Wire*— Energy Industry Vulnerable to Cyber Attack?

- Willis Insurance predicts “[a] major cyber-attack on the energy industry ‘is only a matter of time’” *Willis Insurance Predicts Energy Cyber-Attack 'Catastrophe' Ahead*, Forbes (Apr. 8, 2014); *Energy companies need insurance cover for cyber attack 'time bomb‘,* Reuters (Apr. 8, 2014)
  - Willis reported that, in 2012, it received two enquiries about cyber attacks but today “the figure is one a week.”
- “Consensus is growing that the U.S. electricity grid is vulnerable to both hacking and physical attacks, but protecting it remains a work in progress—especially given the spending that would be necessary by financially stretched utilities.” *Double threat: US grid vulnerable on two fronts*, CNBC (Jan. 5, 2014); *Industry sitting on ‘cyber-attack timebomb*’, Petroleum Economist (Apr. 9, 2014)

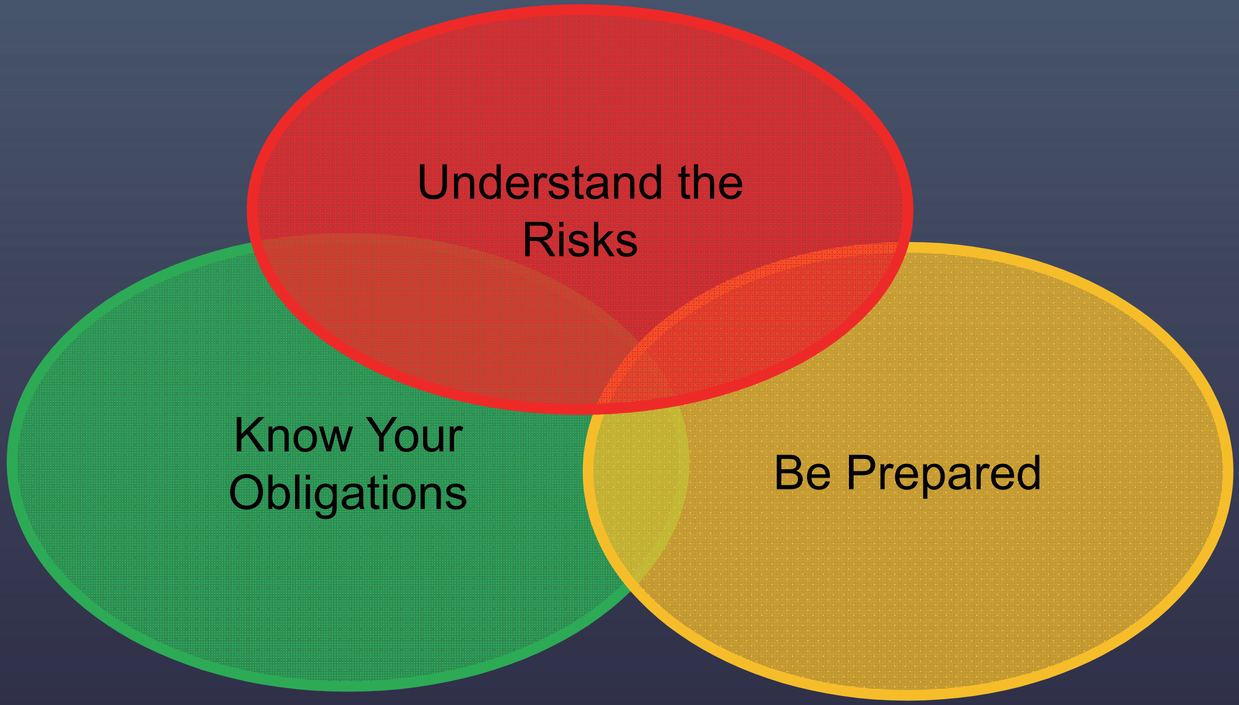
# *Ripped From the Headlines* — Not the First, But Certainly a "Target" for Criticism

- *Target Struck in the Cat-and-Mouse Game of Credit Theft*, The New York Times (Dec. 19, 2013)
  - *Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores, Target.com (Dec. 19, 2013)* — "Approximately 40 million credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013."
- *Target breach worse than thought, states launch joint probe*, Reuters (Jan. 10, 2014)
  - *Target: Data stolen from up to 70 million customers*, USA today (Jan. 10, 2014)
- *Target executive apologizes to Congress for data breach, CBS Money Watch (Feb. 4, 2014); Target, Neiman Marcus Executives Testify on Data Breaches*, CBS New York (Feb. 4, 2014)
- *Heat System Called Door to Target for Hackers*, The New York Times (Feb. 5, 2014)

# Litigation, Investigations, and New Laws Follow

- Consumer Class Actions Filed
  - Within days of an announcement of a data breach, class actions are filed alleging:
    - Negligence/Fraud
    - Breach of Contract
    - State Data Breach Notification Claims/Stored Communication Act
    - Deceptive Business Practice (Deceptive, Unlawful, and Unfair Acts)/Unjust Enrichment
    - Conversion/Bailment
- Public Agency Inquiries/Investigations Initiated and Litigation Ensues
  - State Attorney Generals
  - Federal Trade Commission
  - Department of Health & Human Services
- Target and Others Testify Before Congress About Data Breaches
- New Legislation Introduced — California Assembly Bill 1710

# Managing and Mitigating Legal Risk



# Know Your Obligations

- Hundreds of laws and regulations in the US alone
    - State laws and Massachusetts regulations
    - GLBA
    - HIPAA
    - FCRA and FTC
    - Deceptive practices
- Presidential Cybersecurity Directive and NIST Framework
- Payment Card Industry Data Security Standards
- International Obligations

# Know Your Obligations

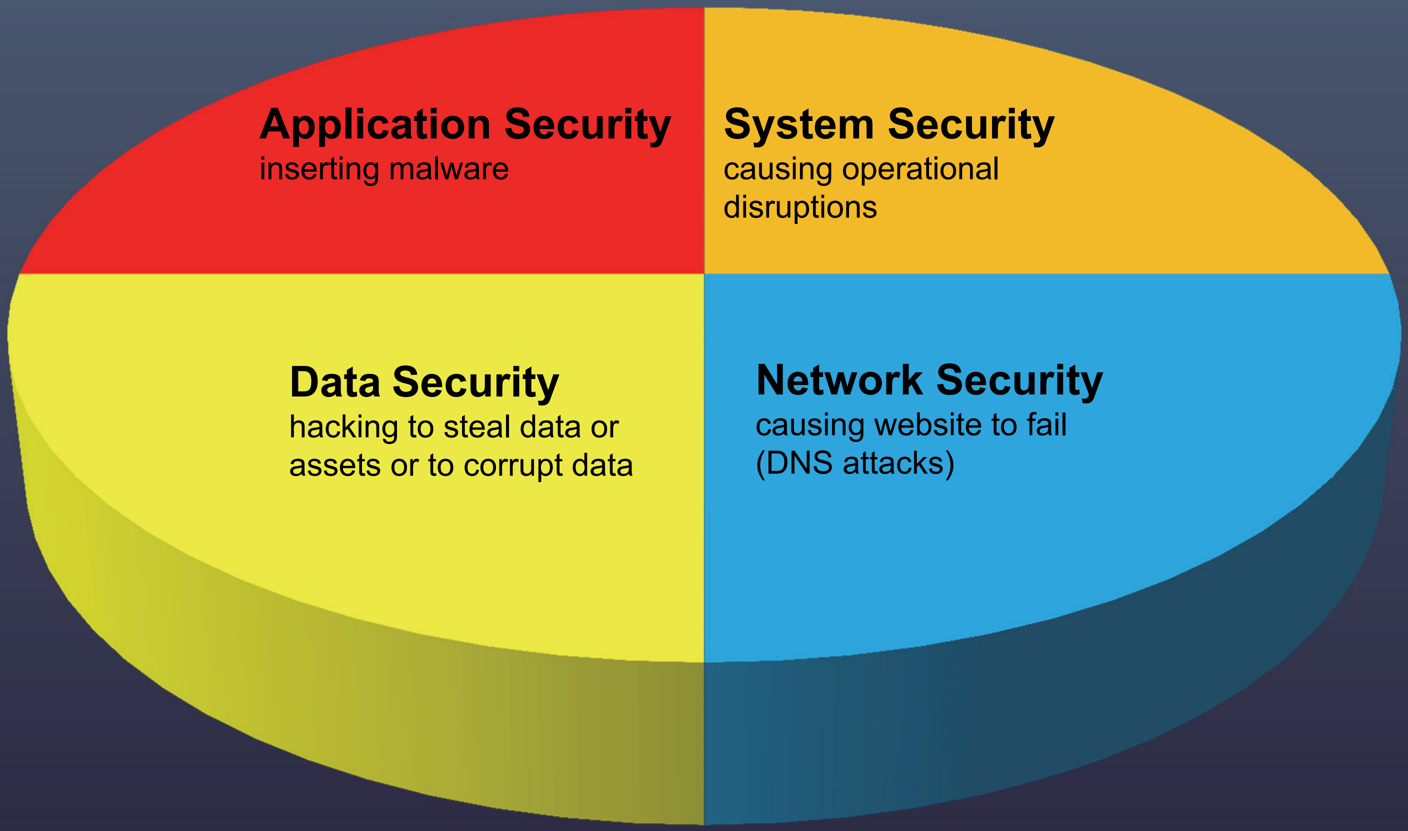
## Legal/Regulatory

- Risk Assessment
- Access Restrictions
  - Authentication/ Applications
- Security Management
  - Data storage, transmission, destruction
  - Physical, technical, systems
  - Employee monitoring
- Training
- Vendor Oversight
- Information/System Security
- Intrusion Detection
- Testing
- Annual Review
- Incident Response Plan
- Contingency Planning
- Device/Media Controls
- Data Identification and Mapping
- Designated Responsible Employee

## Cybersecurity Framework

- Identify
  - Asset management
  - Business environment
  - Policies and Procedures
  - Risk Assessment/Management
- Protect
  - Access control
  - Training
  - Data Security/Management
  - Incident Response Plan
  - Protective Technology
- Detect
  - Anomalies
  - Security Monitoring
  - Processes
- Respond
  - Response Planning
  - Communications
  - Analysis
  - Mitigation
  - Improvements
- Recover
  - Recovery Planning
  - Improvements
  - Communications

# Understand the Risks



**Application Security**
inserting malware

**System Security**
causing operational disruptions

**Data Security**
hacking to steal data or assets or to corrupt data

**Network Security**
causing website to fail (DNS attacks)

# Understand the Risks

Employees

- Paste confidential acquisition information into a webmail message sent to your competitor
- Download hacker tools to their work computer accidentally or with the intention of stealing your customer's private data
- Post your confidential executive communications or financial data on www.internalmemos.com or some other internet posting site like Yahoo Finance
- Use a P2P client and inadvertently expose your proprietary information to millions of other P2P users

Vendors

- Use your customer information to market their own products…or your competitors'
- Lack proper security for protecting your customers' credit card numbers
- Provide a route for hackers to access your website, your customer data, your financial data, your trade secrets, your employee information
- Fail to use or follow through with security measures

Hackers/Thieves

- Steal equipment (laptops, servers) or media (backup tapes, portable devices)
- Exploit web-based insecurities to gain access to your data and systems
- Exploit employee insecurities and obtain user login information to your systems
- Use "Trojan Horses" and other malicious attacks to overtake your system

# Understand the Risks

- Customer Information- arguably the company's most important asset
  - Security breaches
  - Oversight of how third parties handle your data and abide by contractual commitments
- Employee Information- especially where used to discipline or terminate
- Intellectual Property
- Privacy Promises
  - What is the company committing to do in terms of sharing, etc.?
  - Collection of information or monitoring/recording information in an illegal manner (albeit unintentionally)
  - Data sharing and mining, especially for marketing purposes
- Identity theft- causes business as well as consumer fraud or loss

# Understand the Risks

## Ponemon Institute LLC 2013 Cost of Data Breach Study

- The study found the average cost per data breach was **$5.4 million** in 2012. The cost per compromised record was **$188 per record**.

## Ponemon Institute LLC 2013 Cost of Cyber Crime Study

- Average annualized cost of cybercrime incurred by a benchmark sample of U.S. organizations was **$11.6 million**.
- Organizations experienced an average of **122 successful attacks per week**.

## Net Diligence Cyber Liability and Data Breach Insurance Claims

- The average number of records exposed per incident was **1.4 million**.
- The average cost per incident was **$3.7 million**

# Understand the Risks

The risks are more than just immediate monetary impact:

- □ Financial Loss
- □ Regulatory Fines
- □ Reputation Loss
- □ Loss of System Availability
- □ Lost Productivity
- □ Loss of Intellectual Property
- □ Civil Litigation
- □ Government Enforcement

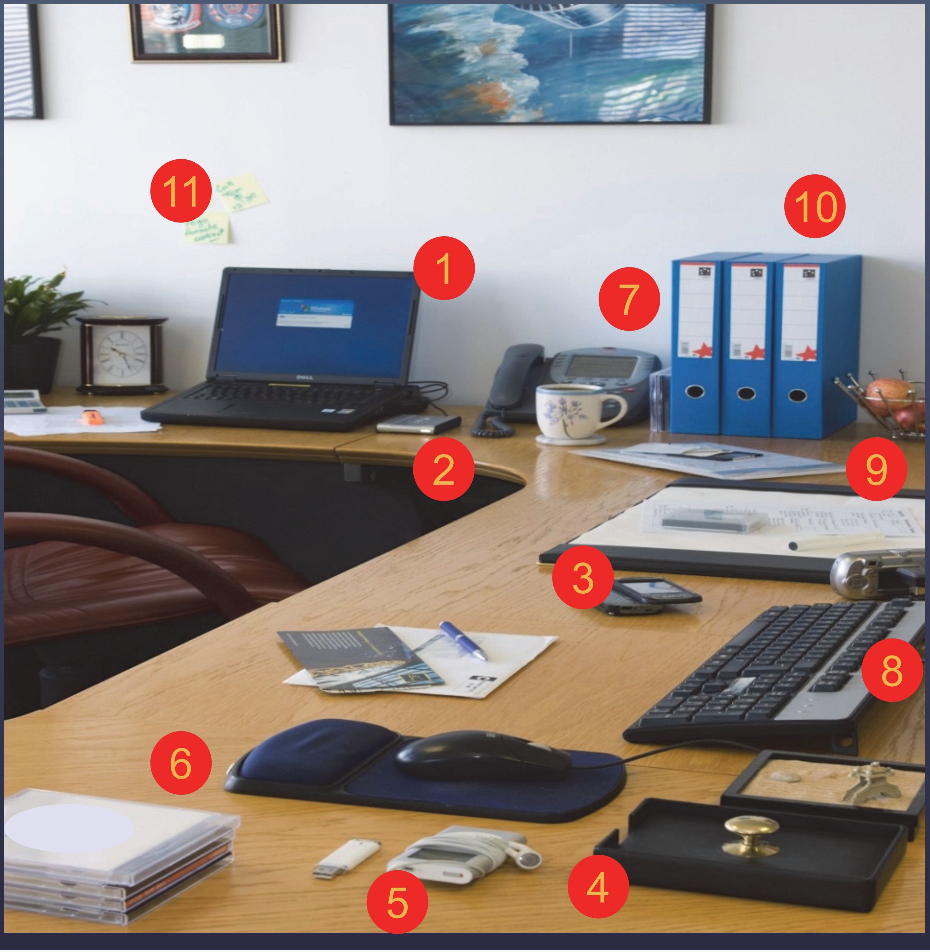
# Be Prepared

## NIST Cybersecurity Plan Framework

Available at http://www.nist.gov/cyberframework/index.cfm

- Identify
  - Asset management
  - Business environment
  - Policies and Procedures
  - Risk Assessment/Management
- Protect
  - Access control
  - Training
  - Data Security/Management
  - Incident Response Plan
  - Protective Technology
- Detect
  - Anomalies
  - Security Monitoring
  - Processes
- Respond
  - Response Planning
  - Communications
  - Analysis
  - Mitigation
  - Improvements
- Recover
  - Recovery Planning
  - Improvements
  - Communications

# Be Prepared



1. Laptop computer
2. External HD
3. Smartphone
4. iPod/Tablet
5. USB memory stick
6. DVDs/CDs
7. Telephone/Voicemail
8. Desktop computer
9. Backup tape
10. Paper records
11. Sticky notes

# Be Prepared

## Administrative Security Controls

- Policies and Procedures
  - Collect only what you need
  - Destroy unnecessary data
- Organizational Structure / Reporting
- Consistency and Proportionality
- Accountability Metrics and Review
- Enforcement and Monitoring

# Be Prepared

## Physical Security Controls

- Access Controls and Permissions
- Personnel and System Surveillance
- Segregation of Systems
- Redundancy and Location
- Separation of Duties

# Be Prepared

"The Hard Drive"

**Data lives in:**

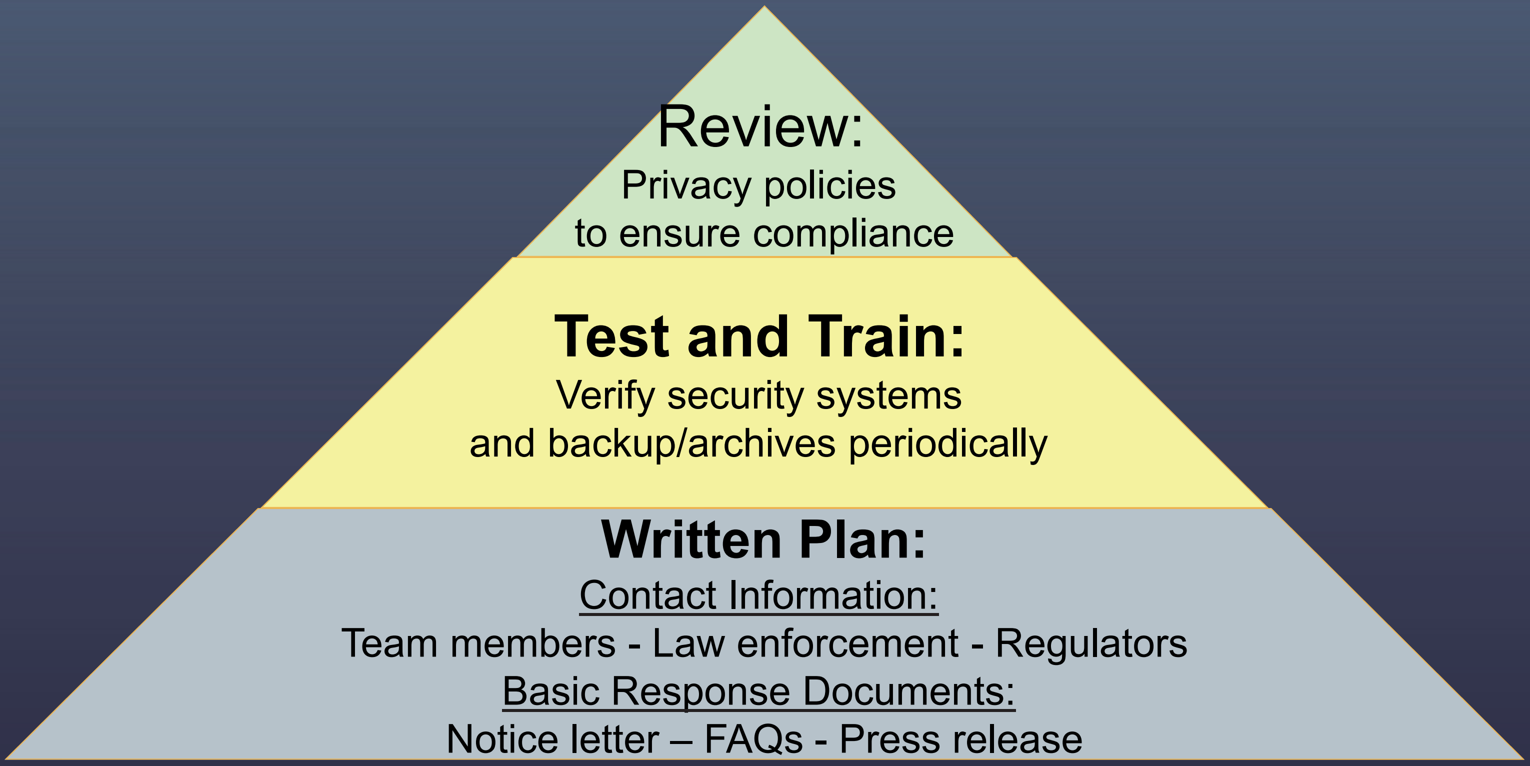
- PCs
- Smart Phones
- External Devices
- Servers
- iPods/iPads
- Copy Machines
- Printers
- Cloud Storage

# Be Prepared

## Logical Security Controls

- Tokens
- Passwords
- Two-way authentication
- Biometrics
- Access rights/restrictions
- I/O Monitoring
- Intrusion detection
- “Principle of Least Privilege”

# Be Prepared



**Review:**

Privacy policies
to ensure compliance

**Test and Train:**

Verify security systems
and backup/archives periodically

**Written Plan:**

Contact Information:

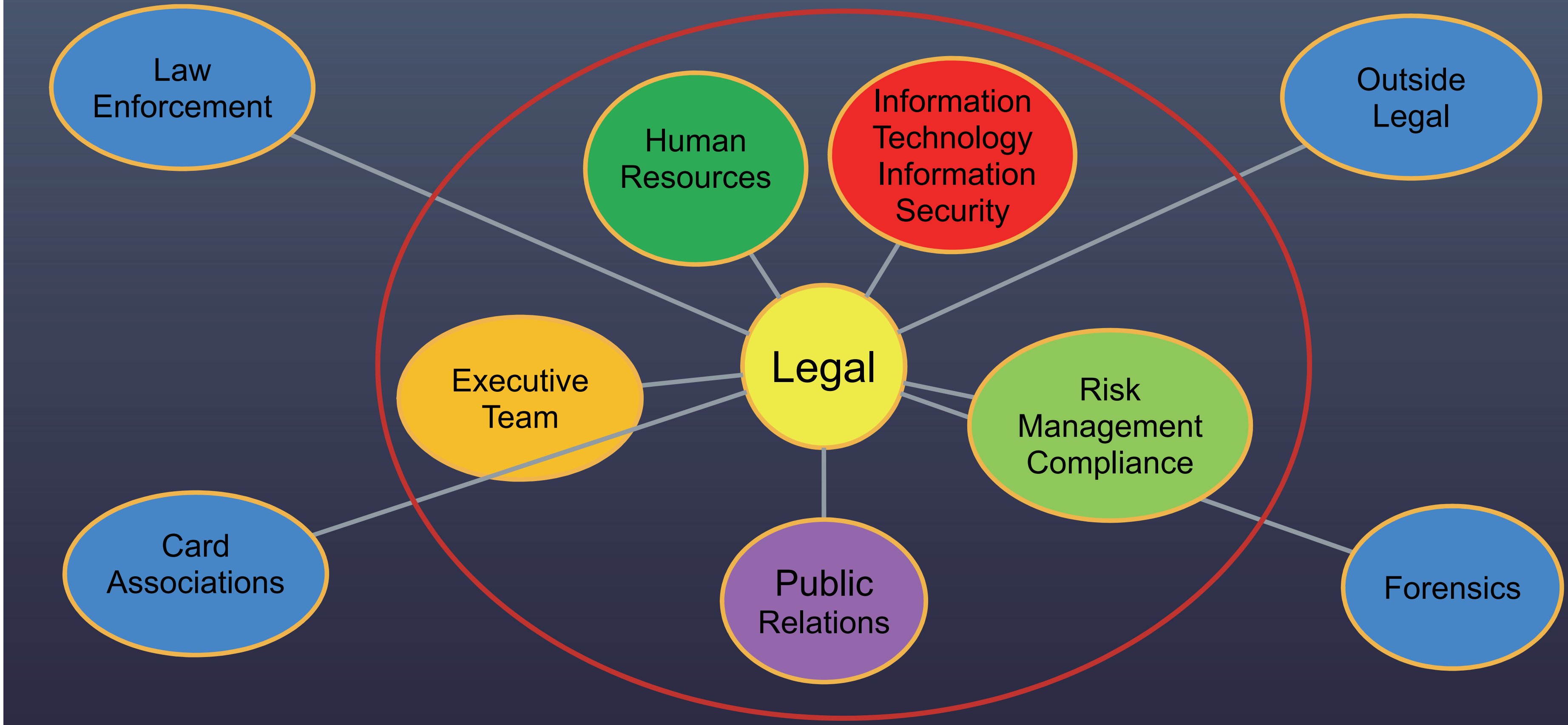
Team members - Law enforcement - Regulators

Basic Response Documents:

Notice letter – FAQs - Press release

# Be Prepared

The Risk Management Team



pillsbury

# Be Prepared

## Incident Response Planning

- Identify Team Members
  - Contact information
  - Identify, vet and get approvals for outside experts and vendors
- Incident Action plan
  - Alarms
  - Reporting up
  - Centralized mechanism for reports
- Incident Response Stages
  - Preparation
  - Early Team Meeting
  - Training
  - Investigation
  - Containment Assessment
  - Notification
  - Ownership and Management Oversight

# Be Prepared

- Basic Response Documentation
  - Notice Letter
  - Card Association Notice
  - Regulator Notice
  - FAQs
  - Agency Notifications
  - Press release templates
- Credit Monitoring Contacts
- Call Center Contacts
- Legal and Forensic Expert Contracts
- Annual drills

# Be Prepared

## Ongoing Review

- Be able and willing to adjust practices and policies
- Watch for trends in regulatory actions and litigation
- Ensure legal is involved in material changes and contracts
  - New products or services
  - Expansion or contraction of company, products, services
  - Sales or purchases of assets, companies
  - Offshore operation
  - Special marketing arrangements

# Be Prepared

## Training – Training - Training

- Employees need to be trained and re-trained on the importance of maintaining security.
- Training needs to address social engineering techniques that are typically very effective at convincing employees to provide sensitive data.
  - Calls from help-desk
  - Calls to help-desk
  - Phishing attacks
  - Physical compromise
  - USB devices

Sample Security Awareness materials are available at:

- http://cyberexchange.isc2.org
- http://technet.microsoft.com/en-us/security/cc165442.aspx

# Be Prepared

## Vendor Oversight

- Transmission security
- Access security
  - Authentication protocols
- Storage security
  - Vendor choice
  - Contract provisions
  - Audit rights and representations

# Contractual Protections Against Data Breach

## Step 1 – Due Diligence – Understand your transaction

- What data is implicated in the transaction?
  - PII or PHI?
  - Credit card information?
  - Less sensitive data?
- What access will the Supplier have with respect to the data?
  - Are they making changes to software with no access to live data?
  - Will they have access to test data only?
  - Will they have access to production data?
- Other Data Attributes
  - Is the data encrypted? In flight? At rest?
  - Where will it reside? Customer data center? Dedicated Infrastructure at Supplier data center? In shared infrastructure?
- These factors determine the risk profile of the transaction and impact what contract protections are needed

# Contractual Protections Against Data Breach

## Step 2 - Include Security Obligations

- Supplier shall maintain an information security program that -
  - ensures security of Customer Data and
  - protects against unauthorized use or access of Customer Data
- Supplier shall comply with Customer's Policies & Procedures
  - Specific IT requirements. Supplier shall -
    - encrypt all data
    - maintain firewalls and security gateways
    - monitor usage of User IDs / Passwords to access System
  - Customer has right to modify Customer policies – only question is cost
- Cloud Contracts
  - Cloud Providers will not sign up for Customer's Policies and Procedures
    - Business model depends on standardized service offering
  - Cloud Providers require the right to change their security policies

# Contractual Protections Against Data Breach

## Step 3 – Audit and Compliance Provisions

- Customer should have robust rights to audit Supplier
- Supplier should provide Customer with audits performed for Supplier by third parties
  - SAS 70 Type 2 – previously used to evaluate Supplier's security, but was not designed to be a security audit
  - AICPA established SSAE 16 and Service Organization Controls ("SOC") reporting Framework in June 2011
    - **SOC 1** – tests controls at a Supplier relevant to internal controls over **financial reporting**
    - **SOC 2** – tests controls at a service organization relevant to **security, availability, processing integrity, confidentiality and privacy**
    - **Type I versus Type II** – Type I verifies the existence of the controls, and Type II audits whether the controls are being observed
- ISO 27001 Certification
  - Add rep and warranty that Supplier will provide this Certification annually

# Contractual Protections Against Data Breach

## Step 4 - Subcontracting and other Protections

- Subcontracting
  - Approval Right or Notice at a minimum
  - Key is understand who may access data
  - Subs obligated to comply with same security obligations as Supplier
  - Supplier responsible for actions of subcontractors
- Restrictions on Supplier’s Delivery Location
  - Supplier will not change location from which it provides Services without Customer’s consent
- Obligations to Destroy/Clean Media
  - Supplier shall remove all Customer Data from any media which is retired and destroy or securely erase such media as Customer directs
  - Instructions on wiping, shredding, destroying can be very specific

# Contractual Protections Against Data Breach

## Step 5 - What if there is a Cybersecurity Incident?

**Supplier shall -**

- notify Customer within X Hours
- investigate the Incident and provide a report
- remediate the Incident in accordance with plan approved by Customer
- conduct forensic investigation to determine cause and what data / systems are implicated
- provide daily updates of its investigation to Customer and permit Customer reasonable access to the investigation
- cooperate with Customer's investigation
- Customer (and not Supplier) makes final decision on whether notices will be sent to affected individuals

# Contractual Protections Against Data Breach

## Step 6 – Liability Provisions for Supplier Accountability

- Liability Provisions are evolving
- Traditionally Supplier's liability for data breach was unlimited
- Today, due to increasing number of cybersecurity incidents, Suppliers seek to limit liability as much as possible by:
  - inserting liability cap
  - limit liability to their breach of data security obligations
  - preserve defense that damages are consequential (not recoverable)

# Contractual Protections Against Data Breach

## Step 6 – Liability Provisions for Supplier Accountability

- Supplier should be liable for any issues caused by Supplier's "fault or negligence" (includes an omission as well as not performing an obligation)
- Separate liability pool for these damages
  - Separate from General Liability Cap
  - Reserved for data breaches (Not reduced by other damage types)
- Stipulate types of costs that are recoverable to avoid claim that the damages are "consequential" and therefore not recoverable. Costs include:
  - Preparation / sending of Notices
  - Call Center
  - Credit monitoring services,  identity restoration services
  - Identity theft insurance
  - Fees Paid to consultants and lawyers to investigate

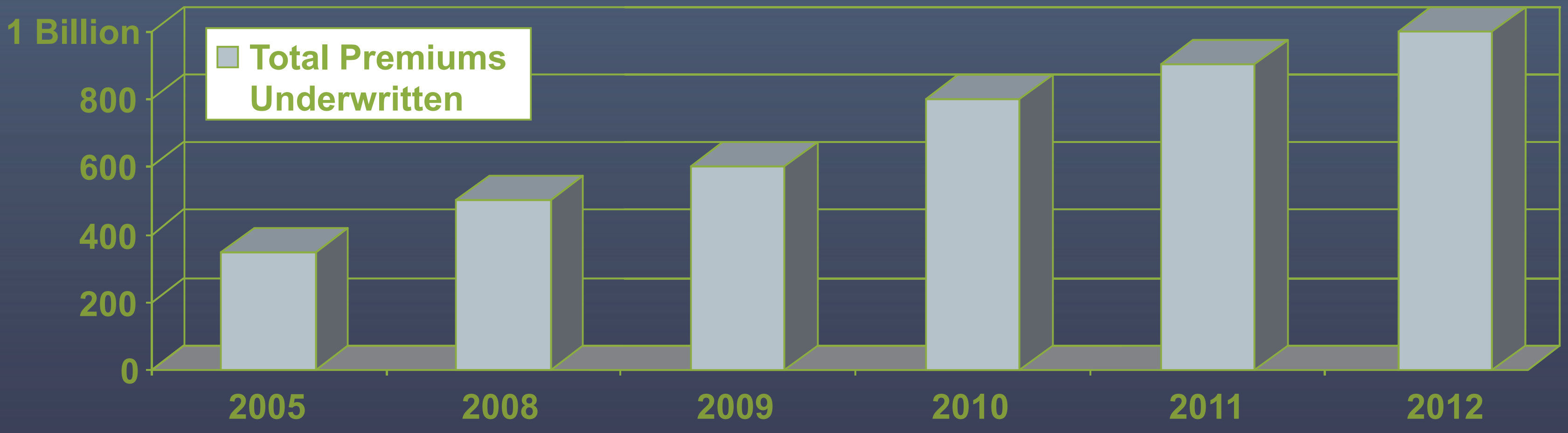
# Contractual Protections Against Data Breach

## Step 7 – Indemnities

“Supplier agrees to indemnify, defend and hold harmless Customer against claims and losses arising out of its acts or omissions that result in data breach”

- Trigger – does not rely on breach of contract
- Indemnity obligations frequently are not subject to a liability cap
- But indemnities require giving control of defending the claims to the Supplier, which has downsides -
  - Potential Liability is extremely high
  - Company’s reputation and future business can be at stake
  - Regulated entities cannot cede control of the claim, as regulators will not permit it
- So Indemnities should not be your only avenue of recourse
  - Contract should stipulate that data breaches losses caused by the acts or omissions of the supplier are recoverable.

# Cyber Insurance Market Trends



- Premiums ≈ $15,000 to $35,000 per $1,000,000 of limits, for low retentions
- Soft market:  Premiums steadily declining
- Large corporations were early adopters
- Most growth is among middle market companies

# Where are the Gaps with Traditional Insurance?

| | General Liability | Property | E&O/D&O | Crime | Cyber |
|---|---|---|---|---|---|
| Network security | POSSIBLE | POSSIBLE | POSSIBLE | POSSIBLE | COVERAGE |
| Privacy breach | POSSIBLE | POSSIBLE | POSSIBLE | POSSIBLE | COVERAGE |
| Media liability | POSSIBLE | NONE | POSSIBLE | NONE | COVERAGE |
| Professional services | POSSIBLE | NONE | POSSIBLE | POSSIBLE | COVERAGE |
| Virus Transmission | POSSIBLE | POSSIBLE | POSSIBLE | POSSIBLE | COVERAGE |
| Damage to data | POSSIBLE | POSSIBLE | POSSIBLE | POSSIBLE | COVERAGE |
| Breach notification | POSSIBLE | NONE | POSSIBLE | POSSIBLE | COVERAGE |
| Regulatory investigation | POSSIBLE | NONE | POSSIBLE | POSSIBLE | COVERAGE |
| Extortion | POSSIBLE | NONE | POSSIBLE | POSSIBLE | COVERAGE |
| Virus/hacker attack | POSSIBLE | POSSIBLE | POSSIBLE | POSSIBLE | COVERAGE |
| Denial of service attack | POSSIBLE | POSSIBLE | POSSIBLE | POSSIBLE | COVERAGE |
| Business interruption loss | NONE | POSSIBLE | POSSIBLE | NONE | COVERAGE |

# What Does Cyber Insurance Cover?

- Third-Party Claims:
  - Data security breaches
  - Privacy breaches
  - Content liability (libel, infringement, etc.)
- First-Party Losses:
  - Loss of data
  - Revenue loss due to interruption of data systems
  - “E-vandalism,” “e-extortion”

# 3rd Party Cyber Coverage: What's Included?

- Claim Expenses
  - Costs of defending against lawsuits
  - Judgments and settlements
- Regulatory Response Costs
  - Costs of responding to regulatory investigations
  - Settlement costs

# 1$^{st}$ Party Cyber Coverage: What's Included?

- Some Or All Of The Following:
- Crisis Management Expenses
  - Notification costs
  - Credit monitoring services
  - Public relations consultants
  - Forensic investigation
  - Pursuit of indemnity rights
  - Regulatory compliance costs

# 1st Party Cyber Coverage: What's Included?

- Some Or All Of The Following:
- Costs of restoring, recreating or re-collecting:
  - Lost data
  - Stolen data
  - Damaged data
- Revenue loss and extra expense due to interruption of your operations due to, e.g.,
  - Hacking
  - Virus transmission
  - Other security failures
- Cyber extortion

# Top Ten Tips For Buying Cyber Insurance

1: Make sure your limits and sub-limits are adequate

2: Ask for retroactive coverage

3: Watch out for “panel” and “consent” provisions

4: Make sure you are covered for your vendors’ errors and omissions

5: Make sure you are covered for loss of data, not just theft or unauthorized access

6: Avoid “one size fits all” crisis management coverage

7: Ask for a partial subrogation waiver

8: Harmonize cyber insurance with your indemnity agreements

9: Harmonize cyber insurance with your other insurance & vendors’ insurance

10: Negotiate favorable defense provisions

# What If You Don’t Have Cyber Insurance?

- Insurance industry often asserts that there is no coverage under most conventional insurance for privacy and network security breaches, but many courts disagree.
  - The most recent example: DSW, Inc. v. National Union (6th Cir. July 17, 2012) holds that costs of customer communications, public relations, lawsuits, attorneys’ fees, and fines  imposed by Visa and Mastercard resulting from a hacking incident in which 1.4M customers’ information was stolen were covered losses under a crime policy
- Therefore, even if you have cyber insurance policy, tender to your other insurers!  You have little to lose and much to gain.

# Thank You for Participating!

**Joseph E. Kendall**
**Partner**
**Pillsbury Winthrop Shaw Pittman LLP**
Phone: 202.663.8350
joseph.kendall@pillsburylaw.com

**Catherine D. Meyer**
**Senior Counsel**
**Pillsbury Winthrop Shaw Pittman LLP**
Phone: 213.488.7362
catherine.meyer@pillsburylaw.com

**Amy L Pierce**
**Counsel**
**Pillsbury Winthrop Shaw Pittman LLP**
Phone: 916.329.4765
amy.pierce@pillsburylaw.com

**Rene L. Siemens**
**Partner**
**Pillsbury Winthrop Shaw Pittman LLP**
Phone: 213.488.7277
reynold.siemens@pillsburylaw.com