HUSCH BLACKWELL

Risk Management: Data Protection, Privacy and Breach Response

Presented by Joan K. Archer, Ph.D., J.D.
Husch Blackwell, LLP

InfoAg

August 3, 2016

Points of Risk Related to Farm Data Protection

"Cyber criminals and hactivists will Increasingly target farm data."

FBI/USDA Cyber Division Private Industry Notification, "*Smart Farming May Increase Cyber Targeting Against US Food and Agriculture Sector,"* (March 31, 2016).

HUSCH BLACKWELL

Protection of Farm Data

What is Farm Data:

- **Personal information**
- **Financial Information**
- **Operational Information**

Privacy

Overarching Rules for Privacy Protection

- Collect, use and retain data in a manner consistent with privacy laws
- Implement systems and audit them to ensure actual privacy protection practices are consistent with the law and customer-facing statements

Privacy

Privacy Protection Components:

- Conduct security risk assessments
- Remediate vulnerabilities
- Provide security training for employees
- Create and implement policies, including access and use policies
- Enforce policies
- Conduct security audits
- Implement best practices for archiving system logs for purposes of investigation and internal policy compliance

Privacy

Five Specific Points of Risk

1) Geography (a country's governing laws)
2) Physical Infrastructure (the vast network of public cables and private hardware)
3) Logic layer (the protocols that automatically transmit and route data packets to the addressed location)
4) Cyber personas (identifiers such as IP addresses and usernames)
5) People (individuals, not always easily linked to cyber personas)

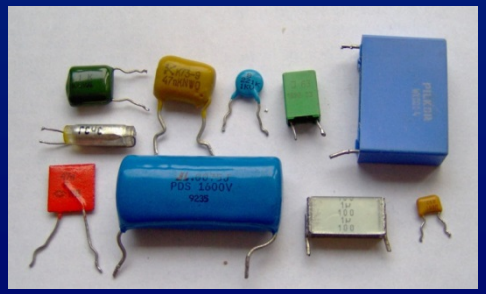
Address Parts of This Risk Through Good Contract Drafting

Focus on:

- Limitations of Liability
- Indemnification
- Process

Contract Components to Consider

- **Definitions** – data, sensitive data, “anonymized” information according to what standard?
- **Standard of care** – what level of precautions must be taken, by whom and when, and are you liable for actions of independent contractors?



Contract Components to Consider

- **Breach procedures** – identify the contact persons, notice timelines and procedures, expenses, investigation coordination obligations, which party covers expense of different tasks?
- **Oversight** – audit rights, assessments, monitoring, training?
- **Return, delete, destroy** – when and how must data be retained or relinquished?
- **Representations and warranties—**cold
- **Indemnification rights and Limitation of liability**

Contract Components to Consider

- **Administrative controls** – internal policies, restricted access, encryption, and logging?
- **Employee devices** – internal policies banning, allowing, or limiting use to minimize risk?
- **Business Continuity/Disaster Recovery Plans**
- **Penetration testing** (internal and external)
- **Cyber Insurance** – is it required, how much, what is excluded?
- **Business continuity / disaster recovery plans**

HUSCH BLACKWELL

Data Breach Response

HUSCH BLACKWELL

Data Breach Response

"There are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be again."

- FBI Director Robert Mueller, 2012

HUSCH BLACKWELL

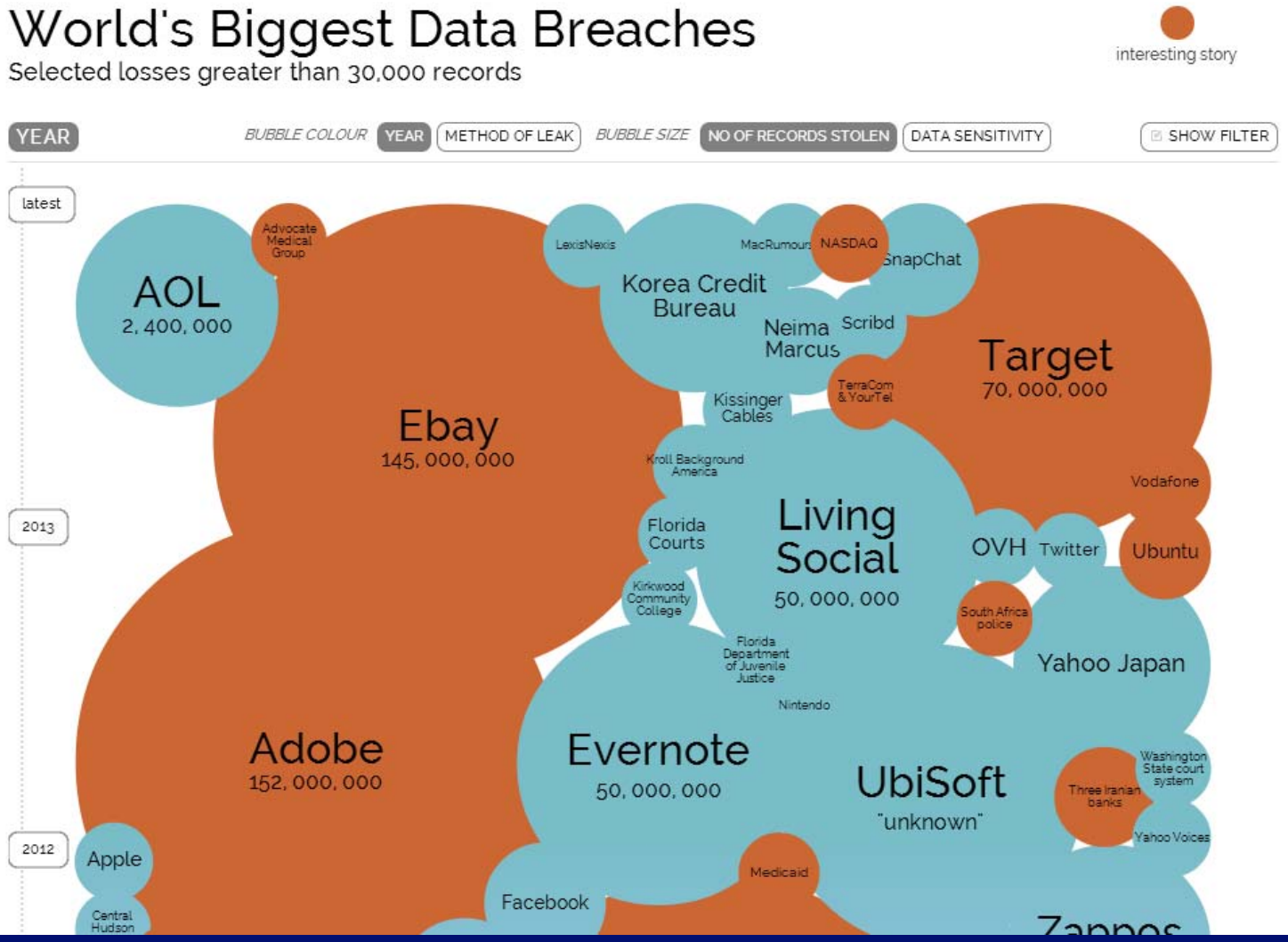
Data Breach Response

"You're going to be hacked. Have a plan."

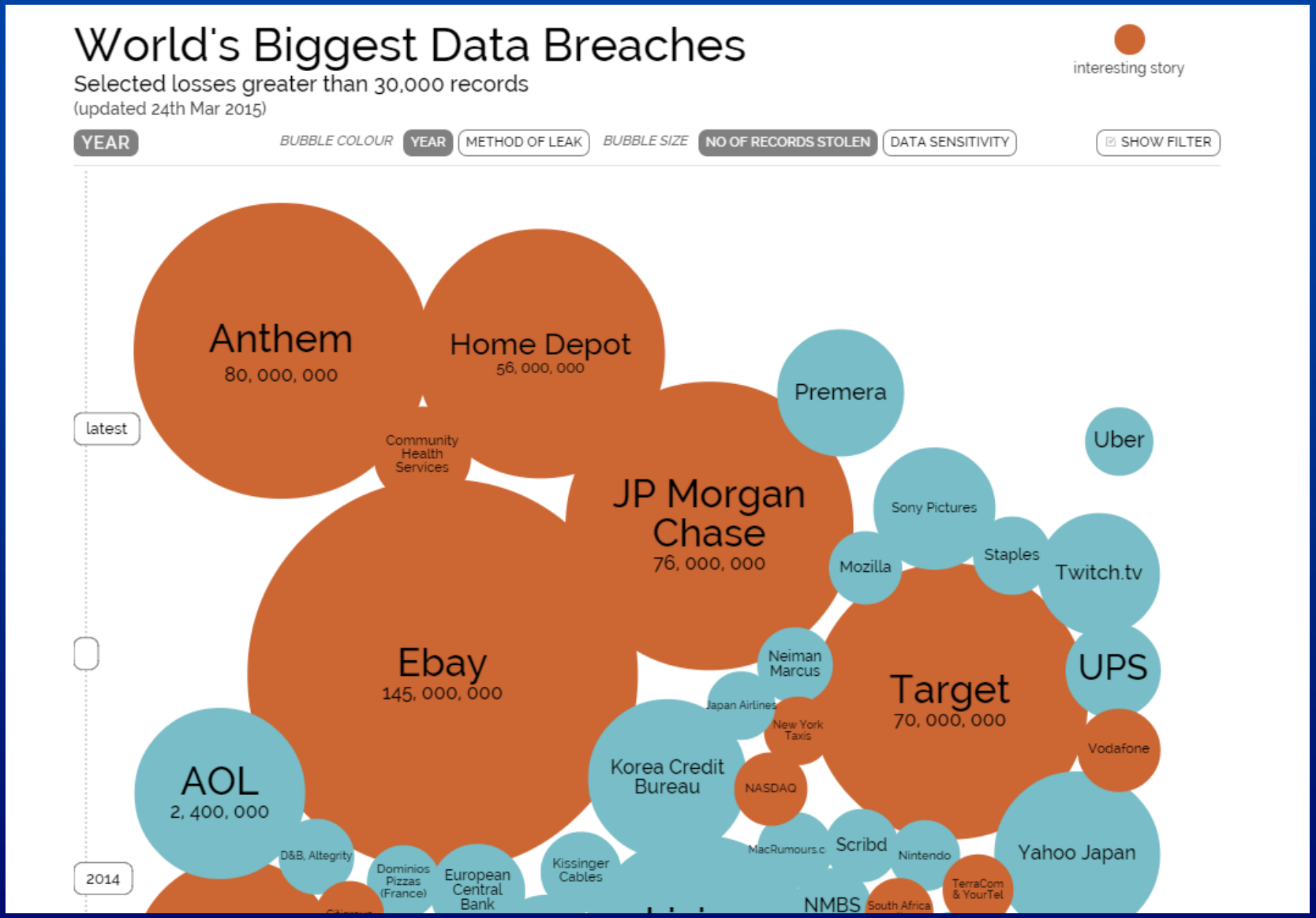
- FBI Cyber Division Assistant Director Joseph Demarest, 2014

Recent Security Breach Examples

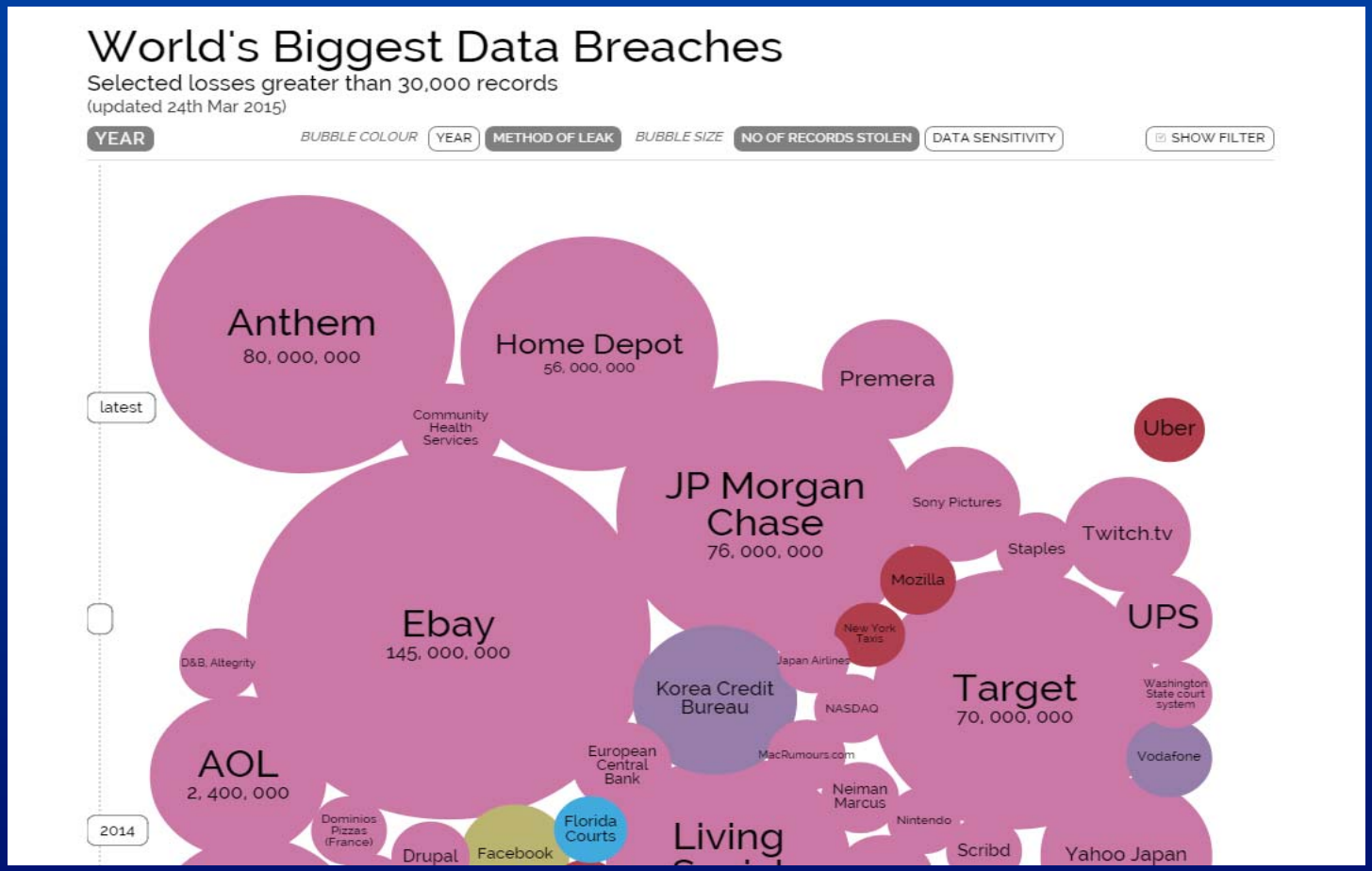
- Target
- PF Chang's
- Ransomware
- Hard Rock Casino
- Milwaukee Bucks
- Houston Astros
- IRS Fraud
- Business Espionage
- Law Firm Breaches



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



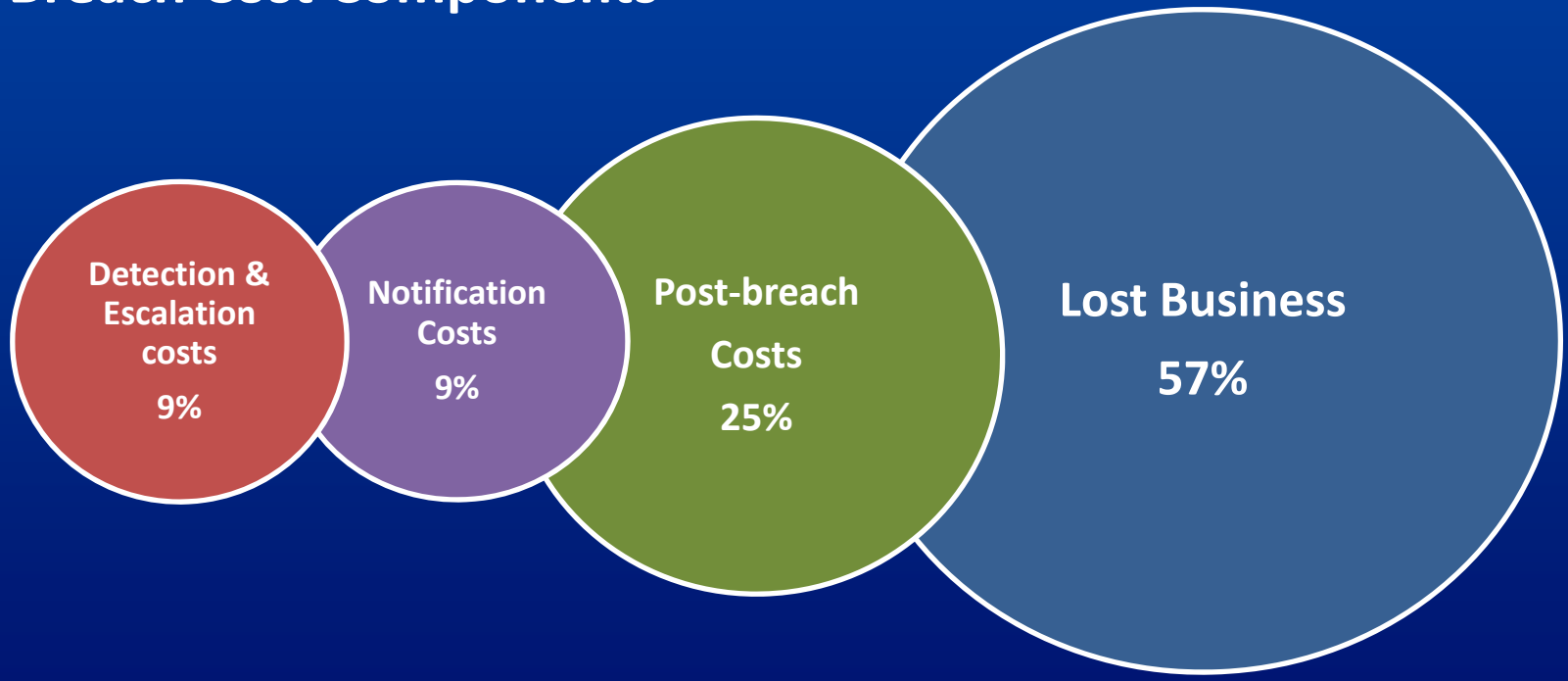
Leak Method:

- Accidentally Published
- Hacked
- Inside Job
- Lost/Stolen Computer
- Lost/Stolen Media
- Poor Security
- All

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Ponemon 2015 Cost of Data Breach Study

Breach Cost Components



Factors that Reduce Breach Response Costs

- Incident Response Team
- Extensive Use of Encryption
- Business Continuity Management (BCM) Involvement
- Chief Information Security Officer (CISO)
- Employee Training (Annually)
- Board-level and Attorney Involvement
- Insurance Protection
- Third-Party Audits/Internal Audits

HUSCH BLACKWELL

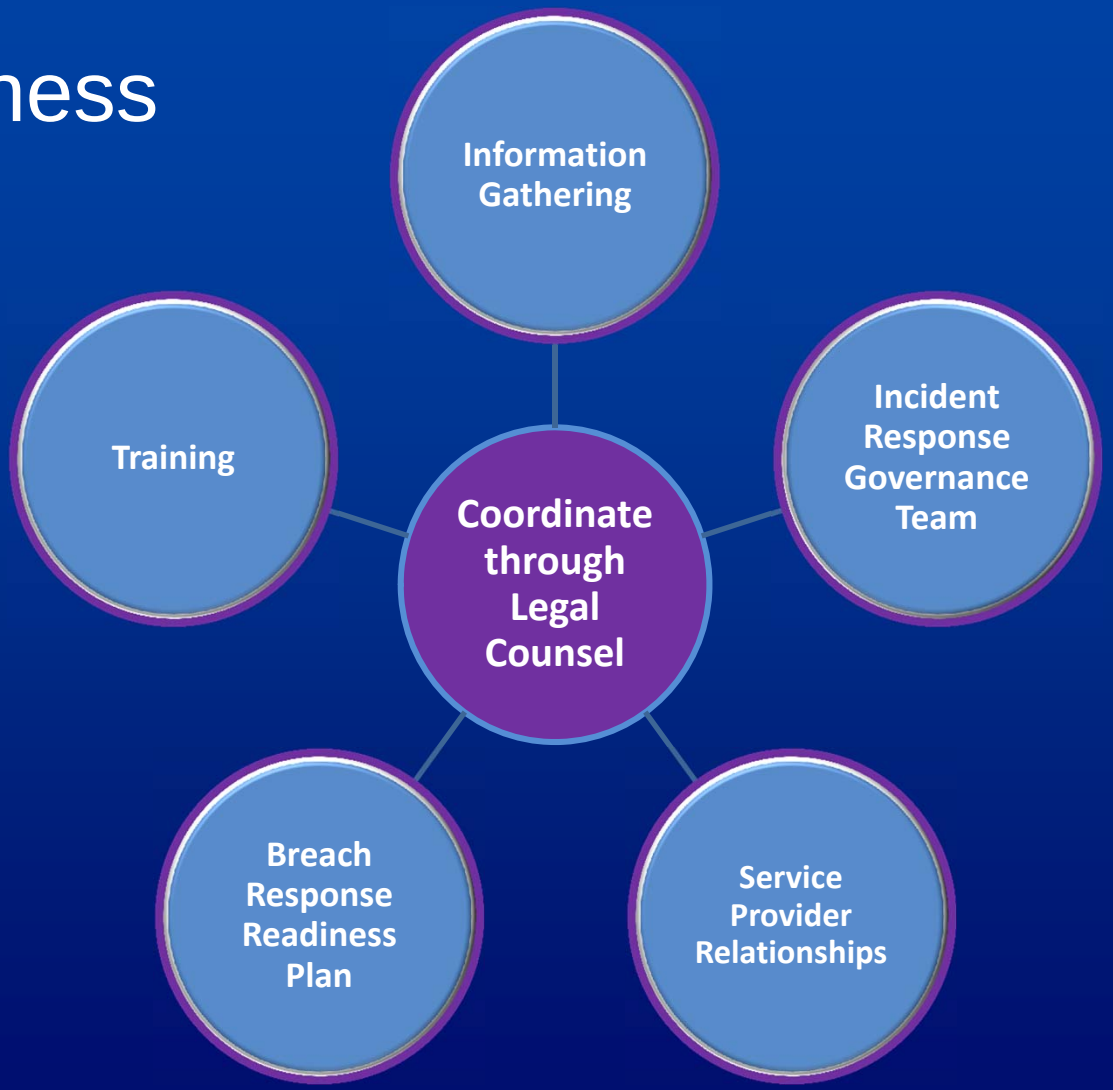
10 Activity Channels for Breach Response

Breach Readiness

- Coordinate Readiness Planning through Legal Counsel
- Gather Information for Readiness Planning
- Identify and Involve Incident Response Members
- Establish Service Provider Relationships
- Prepare Breach Response Readiness Plan
- Train the Team

HUSCH BLACKWELL

Breach Readiness Coordination



DOJ Best Practices for Victim Response and Reporting of Cyber Incidents (April 2015)

"Any Internet-connected organization can fall prey to a disruptive network intrusion or costly cyber attack. A quick, effective response to cyber incidents can prove critical to minimizing the resulting harm and expediting recovery. The best time to plan such a response is now, before an incident occurs."

DOJ Best Practices for Victim Response and Reporting of Cyber Incidents (April 2015)

- Identify your “crown jewels.”
- Have an actionable plan in place before an intrusion occurs.
- Have appropriate technology and services in place before an intrusion occurs.
- Have appropriate authorization in place to permit network monitoring.
- Ensure your legal counsel is familiar with technology and cyber incident management to reduce response time during an incident.
- Ensure organization policies align with your cyber incident response plan.
- Engage with law enforcement before an incident.
- Establish relationships with cyber information sharing organizations.

HUSCH BLACKWELL

Why Cyber Insurance?

	CGL or PL	Property	D&O	Crime	Cyber Liability
Data Security Breach	POSSIBLE	POSSIBLE	POSSIBLE	POSSIBLE	COVERED
Privacy Breach	POSSIBLE	POSSIBLE	POSSIBLE	POSSIBLE	COVERED
Media Liability	POSSIBLE	NONE	POSSIBLE	NONE	COVERED
Virus Transmission	POSSIBLE	POSSIBLE	POSSIBLE	POSSIBLE	COVERED
Damage to Data	POSSIBLE	POSSIBLE	POSSIBLE	POSSIBLE	COVERED
Breach Notification	NONE	NONE	POSSIBLE	POSSIBLE	COVERED
Regulatory Investigation	POSSIBLE	NONE	POSSIBLE	POSSIBLE	COVERED
Extortion	NONE	NONE	NONE	NONE	COVERED
Virus/Hacker Attack	POSSIBLE	POSSIBLE	POSSIBLE	POSSIBLE	COVERED
Denial of Service Attack	POSSIBLE	POSSIBLE	POSSIBLE	POSSIBLE	COVERED
Network Business Interruption	NONE	POSSIBLE	POSSIBLE	NONE	COVERED

Cyber Coverage-After a Break In

- Review All Policies
- Assess Notice Requirements
- Contact Broker As Soon As Practical
- Be Aware of Policy Restrictions on Covered Losses

HUSCH BLACKWELL

Questions?

HUSCH BLACKWELL

Joan K. Archer, Ph.D., J.D.
Partner

HUSCH BLACKWELL LLP
4801 Main Street, Suite 1000
Kansas City, MO 64112-2551
Direct: 816.983.8191
Mobile: 913.707.5869
Joan.Archer@huschblackwell.com