Risk Management: Data Protection, Privacy and Breach Response

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

InfoAg
August 3, 2016

© 2016 Husch Blackwell LLP
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).
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**
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
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
World's Biggest Data Breaches

Selected losses greater than 30,000 records

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
World's Biggest Data Breaches

Selected losses greater than 30,000 records
(updated 24th Mar 2015)

- Anthem 80,000,000
- Home Depot 55,000,000
- JP Morgan Chase 76,000,000
- Ebay 145,000,000
- Target 70,000,000
- AOL 2,400,000

Ponemon 2015 Cost of Data Breach Study

Breach Cost Components

- Detection & Escalation costs: 9%
- Notification Costs: 9%
- Post-breach Costs: 25%
- Lost Business: 57%
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
10 Activity Channels for Breach Response

- Security
- Legal
- Forensic
- Law Enforcement
- Regulators
- Insurance Coverage
- Public Relations
- Stakeholders
- Notifications
- Personnel Management
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
Breach Readiness Coordination

- Information Gathering
- Incident Response Governance Team
- Service Provider Relationships
- Breach Response Readiness Plan
- Training

Coordinate through Legal Counsel
“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.
## Why Cyber Insurance?

<table>
<thead>
<tr>
<th>Event</th>
<th>CGL or PL</th>
<th>Property</th>
<th>D&amp;O</th>
<th>Crime</th>
<th>Cyber Liability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Security Breach</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>COVERED</td>
</tr>
<tr>
<td>Privacy Breach</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>COVERED</td>
</tr>
<tr>
<td>Media Liability</td>
<td>POSSIBLE</td>
<td>NONE</td>
<td>POSSIBLE</td>
<td>NONE</td>
<td>COVERED</td>
</tr>
<tr>
<td>Virus Transmission</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>COVERED</td>
</tr>
<tr>
<td>Damage to Data</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>COVERED</td>
</tr>
<tr>
<td>Breach Notification</td>
<td>NONE</td>
<td>NONE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>COVERED</td>
</tr>
<tr>
<td>Regulatory Investigation</td>
<td>POSSIBLE</td>
<td>NONE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>COVERED</td>
</tr>
<tr>
<td>Extortion</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>COVERED</td>
</tr>
<tr>
<td>Virus/Hacker Attack</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>COVERED</td>
</tr>
<tr>
<td>Denial of Service Attack</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>COVERED</td>
</tr>
<tr>
<td>Network Business Interruption</td>
<td>NONE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>NONE</td>
<td>COVERED</td>
</tr>
</tbody>
</table>
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
Questions?