Cyber Data Attacks: Are Farmers and Agribusiness Exempt?
AgriGrowth has been an advocate for food systems and agriculture for nearly 50 years.
“If we fail on food, we fail on everything.”

Ecologist Charles Godfray

Expected 9 billion people on earth by 2050
To serve as a **convener, advocate, and thought leader** by creating common ground solutions which move the food and agriculture industry forward.
3 strategic priorities guide our work:

**Advocating** for a positive business climate for Minnesota’s food systems & agriculture

**Building awareness, trust, and support** for our sector with “key influencer” audiences

Serving as a **convener and thought leader** on issues relevant to the future growth and prosperity of our sector.
Over **170** Member organizations

With over **600** professional contacts

AgriGrowth provides a forum for our members to work together to solve challenges related to feeding the world in a safe, sustainable, environmentally responsible and consumer-responsive way.
Who are our members?

- 27.5% Agribusiness
- 21% Associations/Non Profits
- 15% Farmers
- 12% LLCs/Individuals
- 5% Legal/Financial Mgmt
- 5% Academia & Government
- 4.5% Public Affairs/Comm/Marketing
- 3% Transportation
- 3% Ag Lending
- 2% Engineering
- 2% Energy
66% of AgriGrowth members have been committed to our mission for over ten years.

“I had the opportunity to talk directly with Minnesota’s Speaker of the House for 15 minutes at an AgriGrowth event. How else would I get that opportunity?”

Legislative reception member attendee
Reasons members stay engaged

- Having a trusted and credible organization dedicated to advocating for & managing the policy environment, allows members to focus on operating their businesses.
- Cross-sector networking opportunities.
- Stay informed about trends, threats & opportunities within the industry.
- Up-to-date industry news and information.
- Opportunities to collaborate and partner.
AgriGrowth Coalitions and Collaboratives

- Minnesota Business Immigration Coalition
- Real-Time Talent Workforce Initiative, Board seat
- Enterprise Minnesota - State of Manufacturing Report sponsor
- Center For Food Integrity
- WCCO Radio - Business by Carlson: A Quarterly Report
- AGree/AgriGrowth Working Lands Conservation Pilot Project
- A Greater Minnesota Coalition (AGM)
- Ag/Farm Alliance
- MN AgPAC
Member engagement opportunities

Legislative series
  Legislative reception – MEMBERS ONLY
  Legislative Preview Luncheon
  Policy luncheons
  Monthly member policy webinars
  Legislative Recap Luncheon

Workshops and webinars
Speakers and luncheons
Networking opportunities
Member listening sessions
Policy Development Committee
MN AgPAC fundraiser
Industry surveys
Partnerships
Election engagement
Annual Meeting and Conference
<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:30 a.m.</td>
<td>AgriGrowth Business Meeting (AgriGrowth members)</td>
</tr>
<tr>
<td>9:30 a.m.</td>
<td><strong>U.S. Economic Outlook in Agriculture</strong></td>
</tr>
<tr>
<td></td>
<td><em>Dr. Robert Johansson, Chief Economist, USDA</em></td>
</tr>
<tr>
<td>10:30 a.m.</td>
<td><strong>Morning Keynote Address:</strong> <em>Agricultural Sustainability in an Uncertain Season</em></td>
</tr>
<tr>
<td></td>
<td><em>Dr. Margaret M. Zeigler</em></td>
</tr>
<tr>
<td></td>
<td><em>Executive Director, Global Harvest Initiative</em></td>
</tr>
<tr>
<td>11:30 a.m.</td>
<td>Break</td>
</tr>
<tr>
<td>Noon</td>
<td>Luncheon Program</td>
</tr>
<tr>
<td>Noon</td>
<td><strong>2016 Distinguished Service Award Recipient</strong></td>
</tr>
<tr>
<td>1:45 p.m.</td>
<td>Break</td>
</tr>
<tr>
<td>2:00 p.m.</td>
<td><strong>Afternoon Keynote Address</strong></td>
</tr>
<tr>
<td></td>
<td><strong>The Global Economy: An Unconventional Outlook</strong></td>
</tr>
<tr>
<td></td>
<td><em>Dr. Vikram Mansharamani</em></td>
</tr>
<tr>
<td></td>
<td><em>Author, Yale lecturer &amp; Harvard Senior Fellow</em></td>
</tr>
<tr>
<td>3:15 p.m.</td>
<td>Break</td>
</tr>
<tr>
<td>3:35 p.m.</td>
<td><strong>Election Breakdown 2016</strong></td>
</tr>
<tr>
<td></td>
<td><em>Moderator: Mary Lahammer, Program host &amp; political reporter, Twin Cities Public Television (TPT)</em></td>
</tr>
<tr>
<td></td>
<td><em>Panelists: Blois Olson, Fluence Media, Kurt Zellers, MZA+ Co, &amp; Katharine Tinucci, MZA+Co</em></td>
</tr>
<tr>
<td>4:30 p.m.</td>
<td>Conference concludes</td>
</tr>
<tr>
<td></td>
<td>Post-Conference reception begins</td>
</tr>
</tbody>
</table>
Some of the challenges facing the industry

Primary issue of the decade

Workforce shortage

Need for Innovation

Feeding a world population

Bio security & food safety

Transportation

Sustainability

Habitat

Productivity
Robert E. Cattanach
Partner
Dorsey & Whitney
Al Sweeny
Director
Baker Tilly
Madeline Allen
JD, ARM
Lockton Companies
Legal Perspective on Cyber Security

Robert E. Cattanach
Partner, Dorsey & Whitney
October 25, 2016
“[T]here are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.”

- Robert S. Mueller, Director, FBI
New “Vectors” of Threats are Accelerating the Concern

HISTORICALLY...

Bad “Actors”
- Isolated criminals
- Voyeurs

Random Opportunity

Targets
- Credit Cards
- Identity Theft
- Health Insurance

NOW...

Bad “Actors”
- Loosely Organized criminal syndicates
- Foreign States
- Hacktivists for sport/reputation

“Target of Choice”

Targets
- Data bases containing PII / HIPAA – health information
- Intellectual Property
- Advance Access & Market
- Financial Information
- Strategic Objectives
Is this big? How Big

The New Face of Organized Crime

Hackers are no longer lone wolves. They’re now banding together to run fewer—yet much larger—attacks, similar to the organized crime rings of the 20th century Mafia.

80% of cyber-attacks are driven by organized crime rings, in which data, tools, and expertise are widely shared.¹

Source: KPMG
Common Threats

Social Engineering

Request from CFO
Subject: Immediate Wire Transfer

To: Director, Enterprise Financial Services

⚠️ High Importance

Please process a wire transfer payment in the amount of $250,000 and code to “admin expenses” by COB today. Wiring instructions below...

Ransom-ware

Your personal files are encrypted!

Your private key will be destroyed on: 3/10/2015
Time left: 95:30:42

Your files have been safely encrypted on this PC: photos, videos, documents, etc. Click "Show encrypted files" button to view a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.

The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.

Once this has been done, nobody will ever be able to restore files...

In order to decrypt the files press button to open your personal page and follow the instruction.

In case of "file decryption button" malfunction use one of our gates:
http://34r60h6q26q2h+JlcJ24j6u.net
https://34r60h6q26q2h+JlcJ.tar2web.fi

Use your Bitcoin address to enter the site:
15V2TmlH0dgJRFXsNUttwB9aUJD1EvDpWjKm

Click to copy address to clipboard if both button and reserve gate not opening, please follow the steps:
You must install the browser
www.torproject.org/projects/torbrowser.html.en
After installation run the browser and enter address 34r60h6q26q2h+JlcJ.onion
Follow the instruction on the website. We remind you that the sooner you do so, the more chances are left to recover the files.

Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.

Click for Free Decryption on site
Consequences of Data Breach in Any Industry

- $6.5M is the average total cost of data breach
- 11% increase in total cost of data breach
- $217 is the average cost per lost or stolen record
- 8% increase in cost per lost or stolen record

Data Breach – Proactive Steps

1. Know Your Data and where it resides
2. Know (and manage) Your Vendors
3. Have an Incident Response Plan
4. Practice the Plan
5. Evaluate Your Cyberinsurance
Know Your Data: Information Governance

• Know what data is being collected, who has access and how long it will be retained (and why); map the flows

• Institute Information Risk Management Program

• Determine adequate security measures:
  – Cannot protect everything
  – Assume hackers will obtain access
  – Build defenses and monitoring around those critical assets

• Document the process

• Have it tested
Know and Manage Your Vendors

• Review and approve vendors who host sensitive company data
  – IT Vendors
  – Professional service providers
  – Onsite independent contractors and temps
Know and Manage Your Vendors

• Assess vendor security measures before retention
  – Screening of staff, including on-boarding/off-boarding
  – Location and retention of data
    • Will it be stored, or even routed, outside the US?
  – Encryption of data in transit and at rest
  – Intrusion testing
  – Security certifications

• Site visits and audits
Know and Manage Your Vendors

• Contractual requirements and protections
  – Legally binding security obligations
  – The big “I”: Indemnification
  – Ownership of data (including de-identified data)
Incident Response Plan

Identify the Team

a) Team leader (will depend on the nature and severity of the incident)

b) Information Technology

c) Information Security

d) Risk Management

e) Legal – inside and outside counsel

f) Customer Service

g) Public Relations
Practice the Plan

Engage the Team in planning and practice

a) Assign initial responsibilities; articulate escalation criteria
b) Identify and involve backup personnel
c) Primary and backup contact information
d) Practice the plan
   • Start with a table-top exercise
   • Escalate to more life-like scenarios
   • Involve objective third parties
   • Conduct a gap analysis with continuous improvement
Identifying Legal Risks – State Governments

State

• 48 states and the District of Columbia each have their own Breach Notification Laws

• Significant variations (e.g., exceptions for encrypted information; risk assessment threshold)

• Some state’s requirements are incompatible with others (e.g., Massachusetts)

• State Attorneys General – enforcement of state consumer protection laws

• Some states claim to have extraterritorial effect (California)
Cyber Risk Management Framework: Oversight’s Responsibility

I. LEGAL AND COMPLIANCE
- Regulatory requirements (international)
- Certification standards

II. OPERATIONS AND TECHNOLOGY
- Control measures
- Address identified risks
- Compromise
- Mitigate potential

III. HUMAN FACTORS
- Security culture that empowers and helps to ensure
- Proper mix of people, skills, culture, communication

IV. BUSINESS CONTINUITY AND CRISIS MANAGEMENT
- Incident Response Plan
- Contingencies to deal with other crisis and stakeholder management

V. LEADERSHIP AND GOVERNANCE
- Management due diligence,
- Ownership of risk
- Assessing appetite for risk
Evaluating Cyber Insurance

What insurance do you have?

What insurance do you need?

What are the exclusions?
Assessment perspective on cybersecurity risk

Al Sweeny, Director
Agribusiness cyber challenges

Technology
> Drones
> Robots
> RFID tags
> Precision farming

Data
> Seed traits
> Chemical usage
> Soil conditions
Agribusiness cyber risks

Availability attacks
  > Extortion malware
  > Technology breakdown

Data breaches
  > Economic manipulation
  > Intellectual property theft

Activism
  > Anti-GMO
  > Animal rights groups
Available assessment options

Attack surface reduction (indicators of exposure)

> Phishing simulations
> Open Source Intelligence Testing (OSINT)
> Vulnerability scanning
> Third-party risk management (TPRM)

Cybersecurity assessments

> Maturity assessments
> Compliance assessments
Questions?

Al Sweeny
Director, Technology Risk Services
612 876 4924
al.sweeny@bakertilly.com
Insurance & Risk Management Perspective on Cyber
October 25, 2016

Madeline Allen, J D ARM
Network Security and Privacy – Agriculture Risks

- Employee Data
- Farm Data
- “Smart Farming” technology
- Industrial Controls
- Property Damage
- Bodily Injury
Cyber Coverages

- **Network Security Liability**
  - Claim expenses and damages emanating from network and non-network security breaches

- **Privacy Liability**
  - Claim expenses and damages emanating from a violation of a privacy tort, law, or regulation
  - Claim expenses and damages emanating from a violation of a law or regulation arising out of a security breach

- **Privacy Regulatory Proceeding and Fines**
  - Claim expenses in connection with a privacy regulatory inquiry, investigation, or proceeding
  - Damages/fines (varies by market), consumer redress fund
  - Privacy regulations fines
  - PCI fines (varies by market)

- **Privacy Event Expense Reimbursement**
  - Expense reimbursement for third-party forensics costs
  - Public relations costs
  - Legal
  - Mandatory notifications (comply with security breach notification laws)
  - Voluntary notification costs
  - Credit monitoring
  - Call center
First Party Cyber Coverages

- **Data/Electronic Information Loss**
  - Covers the cost of recollecting or retrieving data that was destroyed, damaged or corrupted due to a computer attack.

- **Business Interruption or Network Failure Expenses**
  - Covers cost of lost net revenue and extra expense arising from a computer attack and other human-related perils. Coverage is especially valuable for computer networks with high availability needs.

- **Cyber-extortion**
  - Covers both the cost of investigation and the extortion demand amount related to a threat to commit a computer attack, implant a virus, etc.
What’s Not Covered in a Typical Cyber Policy

- Bodily Injury/Property Damage – Coming Soon!
- Reputational Harm
  - Loss of business income due to loss of client/customer/contracts etc. as the result of a negative publicity event, including data/network security breach or privacy violation.
- Patent Infringement
- Internal/In-house costs
Real-life Examples of Data Security & Privacy Claims

- **Data Center**
  - An HR employee received a request, purportedly from the CFO, to send a list of all employees, including their home address and social security numbers, so the CFO could verify W-2s were issued correctly. The HR employee sent the list of nearly 700 employees’ information...to an imposter.
  - Client purchased cyber insurance and the policy provided coverage for credit/identity monitoring for the employees, and is prepared to handle any law suits that may arise from the disclosure of the employees’ information.

- **German Steel Plant**
  - Hackers accessed the plant’s business network and then gained access to the plant’s industrial control system. The manipulation and disruption in the ICS caused the blast furnace to overheat and disabled the shut-off controls. The result was massive physical damage to the furnace and other parts of the plant, as well as loss of income for the plant that had to spend significant time recovery from the damage.

- **Hospital**
  - Bad guys sent an e-mail containing a malicious link to several hospital staff members. When staffers opened the link, it launched malicious code into the system that encrypted all data and essentially shut down hospital operations.
  - The Hospital paid about 13,000 bit coin to release the encryption key and allow operations to resume.
Data Breach - What are the costs?

- 2015* – Direct costs of a data breach increased due to higher detection, response and lost business numbers.

- Average cost of a data breach: $6.5 million

- Note – Financial services related breach costs are higher than the average ($269 vs. $217 per record)

<table>
<thead>
<tr>
<th>Cost</th>
<th>2013*</th>
<th>2014*</th>
<th>2015*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection &amp; Escalation</td>
<td>$14</td>
<td>$14</td>
<td>$20</td>
</tr>
<tr>
<td>Notification</td>
<td>$20</td>
<td>$18</td>
<td>$19</td>
</tr>
<tr>
<td>Response</td>
<td>$49</td>
<td>$55</td>
<td>$54</td>
</tr>
<tr>
<td>Lost Business</td>
<td>$105</td>
<td>$114</td>
<td>$124</td>
</tr>
<tr>
<td>Total</td>
<td>$188</td>
<td>$201</td>
<td>$217</td>
</tr>
</tbody>
</table>

* Date indicates the release date of the report which uses data gathered from the previous calendar year. Data is based on breaches suffered by 62 companies where no more than 100,000 records were exposed.

Cyber Claims Study – NetDiligence 2014

- Average Claim Payout: $733,109 ($2.9m for large companies and $1.3m for healthcare)
- Average Claim Payout Per Record - $956

Study based on 117 claims reported by carriers and includes only payments made, not total costs of breach. NetDiligence estimates that its study represents only 5-10% of all cyber claims handled by US carriers that year.
Cyber Insurance Marketplace
Two different approaches

**Indemnity**
- Reimbursement policies allow the insured to hire vendors (with consent from the carrier)
- Will vary by carrier and range from recommending vendors who can manage a data breach response to providing a risk transfer solution (reimbursement of privacy event expenses)
- Privacy event expenses are typically subject to a sub-limit and will erode the policy aggregate limit

**Vendor Panels**
- Automatic vendors provided by carriers—established breach panels
- Some carriers offer notification costs outside of the aggregate limit
- Some carriers offer notification costs per affected individual rather than monetary sublimits
We have some NY lawyers participating remotely today. In accordance with NY CLE Rules, the New York Verification Code for this program is _______________. 
Cyber Data Attacks: Are Farmers and Agribusiness Exempt?
Cyber Data Attacks:
Are Farmers and Agribusiness Exempt?
Contact us to learn more!

Perry Aasness
Executive Director
paasness@agrigrowth.org

Mary Kay Delvo
Director of Membership & Development
mkdelvo@agrigrowth.org

www.agrigrowth.org
651-905-8900
Twitter @mn_agrigrowth