What is Cyber really?
NJ Public Entity Cyber Claims
## MEL JIF Cyber Risk Management Program

<table>
<thead>
<tr>
<th>Tier</th>
<th>Technical Competency</th>
<th>Cyber Hygiene</th>
<th>Tech Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Minimum back-up practices</td>
<td>Training</td>
<td>Incident response plan</td>
</tr>
<tr>
<td></td>
<td>Patch</td>
<td>Tech practices policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Defensive software</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Controlled server access</td>
<td>Policies</td>
<td>Leadership has expertise</td>
</tr>
<tr>
<td></td>
<td>Access privilege controls</td>
<td>Protect information</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Technology support</td>
<td>Password strength</td>
<td></td>
</tr>
</tbody>
</table>
## MEL JIF Cyber Risk Management Program

### Tier 1
- **Minimum Backup Practices**
  - Weekly Backups Off-Network, Check Backups
- **Patching**
  - Be Aware, Patch ASAP
- **Defensive Software**
  - Antivirus, Firewall, Anti-SPAM, Close Unused Ports, Microsoft “Protected Mode”
- **Cyber Hygiene Training**
  - Malware Identification, Passwords, Security Incidents, Social Engineering
- **Policy & Procedures**
  - Incident Response Plan, Technology Practices Policy
- **Password Strength**
  - Strong, Unique, Mix Cases and Characters, Annually Changed

### Tier 2
- **Physical Network Protection**
  - Restricted Access, Safe from Hazards
- **Access Privilege Controls**
  - Only Access What is Needed, Review
- **Technology Support**
  - Staff or Contractors
- **Protect Information**
  - Encrypt Files with PII/PHI
- **Multi-Factor Authentication**
  - Remote Login
MEL JIF Cyber Risk Management Program

Additional Practices

- Security Review of Vendors
- Inventory Devices and All Digital Assets
- Inventory Authorized & Unauthorized Software, and Whitelist Approved Software
- Internet Content Filtering
- Additional Cyber Hygiene Training
- CIS Critical Security Controls and NIST Cybersecurity Framework
THANK YOU

Questions? Comments?

Edward Cooney
VP, Account Executive
Underwriting Manager
P: 973-659-6424
ecooney@connerstrong.com

Joseph Hrubash
SVP, Account Executive
Executive Director
P: 973-659-6577
jhrubash@permainc.com
# Losses

<table>
<thead>
<tr>
<th>Year</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
<th>2017</th>
<th>2018</th>
<th>2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss</td>
<td>4</td>
<td>2</td>
<td>3</td>
<td>11</td>
<td>18</td>
<td>15</td>
</tr>
<tr>
<td>Amount</td>
<td>$9,000</td>
<td>$1,500</td>
<td>$28,000</td>
<td>$119,000</td>
<td>$617,000</td>
<td>$663,000</td>
</tr>
</tbody>
</table>

- Increase from 2014 to 2019: 7,367%
- Increase from 2014 to 2019: 1,867%
- Increase from 2014 to 2019: 425%
- Increase from 2014 to 2019: 518%
Appealed to elected official ego

Scared them with national claims

Brethren shared stories

Networked with IT Directors group

Pool pays costs
- **Baseline Phishing Test**  
  - How vulnerable are you?

- **Cyber 101 Training**  
  - 30 minute “EVERYTHING”

- **Monthly Phishing Test**  
  - Varies

- **Monthly Online Refresher**  
  - Videos, Games, Interactive
CHALLENGES

- **Member IT Staff**
  - Suspicious
  - Fiefdoms
  - External Vendors
  - Too Busy

- **ICRMP**
  - Unknown
  - Staff Time
  - Member Follow Up

- **Elected Officials**
  - Bureaucracy
  - Another Vendor
  - Disengaged
  - Blind to Risk

- **KnowBe4**
  - Build Platform
  - Pricing
  - Miscommunication
59 Members Enrolled
8,500 Employees

100 Members In Process
11,500 Employees

$95,000 - KnowBe4
25% Staff Time
PARTNER WITH TECHNOLOGY

- Treat as emergency
- Include cyber security response in disaster plan
- Conduct regular reviews of plan
- Add IT to emergency management team
- Conduct simulations & drills
OTHER TOOLS

- Breach Notification Guides
- Acceptable Use Policy
- Information Security Policy
- BYOD Policy
- Physical Security Policy
- Social Networking Policy