Focus on Cyber Security.

Sherri Ramsay
Senior Advisor to the CEO,
CyberPoint International, LLC

11.8.13
robustness
(noun) the ability to absorb shocks and keep operating
The Cyber Threat is real...and growing!
The evolving cyber threat.

1990s: Exploitation

Early 2000s: Disruption

2012: Destruction

2013 & Beyond: Subjugation
The evolving **target set** in the US.

1990s: Military

Early 2000s: Government

2012: Industry

2013 & Beyond: Critical Infrastructure
The **Stakes.**

A power grid interruption caused by a cyber attack has the potential to cost utilities and other infrastructure facilities millions of dollars in lost revenue, regulatory fines and costs to restore operations.
So...
Think **cyber security** across the entire **operations cycle**.
Before...

• Make the networks defensible
  – Secure enterprise design and implementation
  – Open standards
  – Defense in depth
## Twenty Critical Security Controls

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Device Inventory</td>
<td>2</td>
<td>Software Inventory</td>
<td>3</td>
<td>Secure Configurations for Hardware &amp; Software</td>
</tr>
<tr>
<td>4</td>
<td>Vulnerability Assessment and Remediation</td>
<td>5</td>
<td>Malware Defenses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Application Security Software Control</td>
<td>7</td>
<td>Wireless Device Control</td>
<td>8</td>
<td>Data Recovery</td>
</tr>
<tr>
<td>9</td>
<td>Security Skills Assessment &amp; Training</td>
<td>10</td>
<td>Configurations for Network Devices</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Ports, Protocols, and Services</td>
<td>13</td>
<td>Administrative Privileges</td>
<td>14</td>
<td>Log Maintenance, Monitoring, &amp; Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Need to Know</td>
<td>16</td>
<td>Account Control</td>
<td>17</td>
<td>Data Loss Prevention</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Incident Response</td>
<td>19</td>
<td>Secure Network Engineering</td>
<td>20</td>
<td>Pen Tests and Red Teams</td>
</tr>
</tbody>
</table>
During...

• Provide operations-based defense
  – Active management of cyber assets
  – Automated continuous monitoring
  – Training – both individual and team
After...

- Rapid response
- Remediation
Key: Situational Awareness
Cyber is a team sport!
Thank you, have a great day!

Sherri Ramsay
Senior Advisor to the CEO,
CyberPoint International, LLC
sramsay@cyberpointllc.com