Attachment 2

.fro
#gbz
2d;b
:filte
ay:non
1px 5px
}.gbxms{back
osoft.Blur(p
'pixelradius=
#c0c0c0;d
>om:1}.gbtc,.gb
z-inline-box;disp
px #ccc}.gbzt,.gbgt{cursor:po
;padding:0 5px;position:relati
f;font-weight:bold}.gbtsa{pac
{border-top-width:0}.gbtb
b_8d5afc09.png);_background:u
ts,.gbgt-hvr,.gbgt:focus{back
!important}.gbpdjs
backgro

IDAHO CYBERSECURITY
Workshop Recommendations

Drawing on the contemt of workshop presentations, scenario driven discussion, participant feedback, and interviews with stakeholders, the following recommendations were developed from the 2014 and 2015 Idaho Cybersecurity Interdependencies Workshops. These recommendations act as a guide for activities and content for the 2016 event.

- Educate employees at all levels of an organization to understand the role cyber systems play in their business--how much and what kind of data is stored there, what they impact, and how they help them to complete mission critical tasks--as well as their role in keeping those systems secure and functioning.

- Integrate cyber security with physical security as part of a company-wide security integration.

- Utilize resources to check your policies and train your staff. The FBI is willing to provide briefings, and ICS-CERT has self-assessment tools

- Develop a cyber policy, train your employees in it, and develop performance measures around it.

- Identify your mission critical systems and simulate system outages and how to respond. Identify ways you could segment these systems from the remainder of your network.

- Use the same tools as hackers to test your system. This might mean incentivizing employees to find security gaps, or performing cursory research and hacks on your own systems.

- Develop training materials and regular webinars and other training opportunities to help organizations grow cyber security plans and facilitate information sharing.

- Provide training for executive leadership, legal departments, human resources, and other key departments to encourage organization-wide cyber security.

- Grow state-wide knowledge of the Idaho cyber security annex through training and outreach.

- Provide resources specific to small businesses and sectors where cyber security may not be prioritized (example: agriculture).

- Develop a single repository for cyber security preparedness information

- Develop formal partnership for information sharing around cyber security and other critical infrastructure concerns