Ransomware Resources 2.1

Checklist and Resources 2.1

Adding Lasting Value ▸ An Urgent Need to Understand the Threat

Preparation is the key to success; **Awareness** is crucial

Incident Response Plan; build it, test it, revise it

Inventory of Valuable Information; detect anomalies

Valuation of Information, Risk, Recovery Costs, Remedies

Gap Analysis between capabilities and vulnerabilities

Preselect external partners for rapid response

Evaluate cyber-insurance options

Ask insurance broker for guidance and resources

Budget for Recovery; Build a Plan “B”

Backup, Backup, Backup

Network with peers, providers and Government partners

Ransomware Resources 2.1

Checklist and Resources 2.1

Center for Internet Security:
https://www.cisecurity.org/
National Council of ISACs:
http://www.nationalisacs.org/
ISSA:
http://portland.issa.org/
ISACA:
http://www.isaca-oregon.org/
OWASP:
https://www.owasp.org/
InfraGard:
https://www.infragard.org/
Microsoft:
http://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx
SANS (OUCH!).com:
-- August 2016: Ransomware
https://securingthehuman.sans.org/resources/newsletters/ouch/2016
NIST Computer Incident Response Guide
http://dx.doi.org/10.6028/NIST.SP.800-61r2 (Complete & complex outline)
MalwareBytes.com:
https://forums.malwarebytes.org/index.php?/forum/39-malware-removal-guides-and-self-help-guides/
https://blog.malwarebytes.com/
MalwareTips.com:
http://malwaretips.com/blogs/category/ransomware/
Many Ransomware Blogs:
(sample)
http://avien.net/blog/ransomware-resources/
Software Patching automation:
http://www.flexerasoftware.com/enterprise/products/software-vulnerability-management/personal-software-inspector/tab/faq
Cloud Backup Services: (samples)
Idrive:
https://www.idrive.com/
Crashplan:
https://www.crashplan.com/en-us/
Backblaze:
https://www.backblaze.com/