Cyberliability

Questions for your IT Department

- Do you have up to date Anti-Virus monitoring and removal software? Is it updated frequently via a subscription service?
- Do you have an Acceptable Use Policy for equipment? (Workstations and mobile devices) What policies are in place for those who break the policy?
- Do you implement multi-factor authentication? Password, Stored credentials, passcodes, certificates?
- Do your users practice safe data practices in accordance with your company Safety Policy? ie. Do your users have strong, frequently changed passwords that they do not give out?, Are mobile devices not only passcode protected but also encrypted and not left at risk of theft?
- Should you get Cyber Liability Insurance in case of a breach?
- Have you had a PEN (Penetration) Test performed on your network?
- Do you utilize Data Breach Detection Software?
- How are you keeping track of your devices? MDM, lo-jack, Undercover
- Are your users who deal with protected information trained on the laws and rules?

References

NIST Computer Security Incident Handling Guide

http://www.nist.gov/manuscript-publication-search.cfm?pub_id=911736

PONEMON Cost of Data Breech

http://www.ponemon.org/library/2013-cost-of-data-breach-global-analysis

Oregon Senate Bill – 583 (2007) Identity Theft

http://www.oregon.gov/DAS/CIO/ESO/pages/idtheft.aspx

Federal Trade Commission Bureau of Consumer Protection – Data Security

www.ftc.gov/infosecurity

US Dept. of Health and Human Services - HIPAA

http://www.hhs.gov/ocr/privacy/

Cyber Program offered by CIS

http://www.cisoregon.com

Cyber Program (either Primary or Excess) with AIG

http://www.aig.com/_3171_417963.html

Contact

Alycia M. Johnson
Director of Executive Risk
WSC Insurance
alyciaj@wscinsurance.com

Bates Russell
IS Project Coordinator
Clackamas County Technology Services
brussell@clackamas.us