Good Cyber Hygiene Checklist

"[T]he relevant inquiry here is a cost-benefit analysis, that considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity."

– *FTC v. Wyndham,* (3rd Cir. Aug. 24, 2015)

- Start with a risk assessment
- Written policies and procedures focused on cybersecurity and tailored to company
  - Expectations for protection of data
  - Monitoring and expectations of privacy
  - Confidentiality of data
  - Limits of permissible access and use
  - Social engineering
  - Passwords policy & security questions
  - BYOD
- Training of all workforce on your policies and procedures, first, then security training
- Phish all workforce (incl. upper management)
- Multi-factor authentication
- Signature based antivirus and malware detection
- Internal controls / access controls
- No default passwords
- No outdated or unsupported software
- Security patch updates management policy
- Backups: segmented offline, cloud, redundant
- Use reputable cloud services
- Encrypt sensitive data and air-gap hypersensitive data
- Adequate logging and retention
- Incident response plan
- Third-party security risk management program
- Firewall, intrusion detection, and intrusion prevention systems
- Managed services provider (MSP) or managed security services provider (MSSP)
- Cyber risk insurance