Ransomware: Protect and Defend

Post-Incident

Pre-Incident

Lessons Learned
- Evaluate Response
- Create Report
- Implement Recommendations and Improvements

Preventative Measures
- Training & Awareness
- E-mail Filtering
- End Point Controls
- Network Controls
- Robust Patching Program
- Threat Intelligence Analytics

Contain, Eradicate & Recover
- Evaluate Incident
- Isolate Infected Station
- ID Scope of Infection
- What Kind of Ransomware
- Consider Contacting Law Enforcement
- Respond—Restore, Decrypt, Ignore, Pay

Mitigation Measures
- Data Backup
- Quick Restore Capability
- Least Privileged Access
- Incident Response Processes
- Crisis Management Plan
- War Gaming Simulations