Getting Started: Critical Business Questions for Towns to Assess Cybersecurity

Questions about information security for Town Administrators and business process owners to discuss.

Have we identified our municipality's most critical business functions?

- Have owners of critical business functions met to identify the processes and systems they oversee?
- Have those business processes been documented?
- Who is responsible for each business process and system?
- Have the critical business processes been prioritized for the health and wellbeing of your citizens and protection of financial resources?

More information for identifying critical business processes:

Do we have data backup processes (backups) in place for the most important business systems?

- Does the backup strategy prioritize critical business processes?
- Have we determined the acceptable level of data loss for our critical business processes?
- Are backups frequent enough to restore from data loss?
- Are backups tested regularly to ensure they work?
- Is your backup process documented?
  - Is the backup documentation accessible in the event of an emergency?

More information for understanding data backups, storage, and testing:

- NIST SP 800-34 (Process template): https://csrc.nist.gov/CSRC/media/Publications/sp/800-34/rev-1/final/documents/sp800-34-rev1_bia_template.docx
  - FEMA BIA Worksheet (Quick Reference Template): https://www.fema.gov/media-library-data/1388776348838-b548b013b1cfc61fa92fc4332b615e05/Business_ImpactAnalysis_Worksheet_2014.pdf
  - Oregon Example: https://www.oregon.gov/das/Procurement/Guiddoc/BusImpAnalysQs.doc

Does municipality staff have an understanding of ransomware, how to defend against email fraud, and how to protect themselves online?

- Does staff have access to training for defending against email fraud and how to protect themselves online?
- Is there an internal or external communication process when suspicious activity or emails are identified?

More information for identifying ransomware and email fraud:

Do we know who has access to the data and systems that support critical business functions?

- Is there a list of internal users who have access to critical business systems?
- Is there a list of numbers and contact information for vendors and service providers who have access to critical business systems?
(*business continuity plan*)

More information for user access to critical business systems: