Guide to Building Your Cybersecurity Roadmap

1. Conduct a threat and risk assessment. (Hint - You may wish to engage professional services to conduct this, but ensure that you are engaged in the business risk discussions).
    a. Identify critical business information systems, devices and data.
    b. Define the predominant cyber threats and potential vulnerabilities to your information systems, devices, and data.
    c. Identify the major business risks associated to those cyber threats.
2. Define the "current state."
    a. What security controls do you have in place?
    b. What people, processes and technology do you have invested in cybersecurity?
    c. What measures do you have that provide an indication of how secure you are?
3. Define the "desired state" which is feasible and achievable within organizational constraints. (Hint - it would be beneficial to leverage available IT and cybersecurity expertise to help you define this to ensure that you capture technical aspects of the desired state)
4. Identify the key gaps in your program that you need to fill.
5. Create a phased plan that addresses those gaps. Identify goals that can address cybersecurity program requirements and the 'people, processes, and technology' needed for the:
    - Short term (within the next 6 months)
    - Medium term (within the next year)
    - Longer term (within 2-3 years)
6. Follow the plan and identify what you need to monitor and measure to ensure program sustainment and improvements. This should include:
    a. Monitoring risk levels and maintaining risks at an acceptable level (your organizational risk tolerance)
    b. Monitoring compliance
    c. Regularly reviewing policies and procedures
    d. Regularly testing your:
        i. Cybersecurity incident response plan
        ii. Back ups
    e. Conducting annual cybersecurity audits.