NORTH STAR GROUP

COMPASS CYBER SECURITY

WHAT TO CONSIDER WHEN PERFORMING A CYBER SECURITY ASSESSMENT

A Cyber Security Assessment is much more than a review of your technology. It's vital to analyze both technical and non-technical components of your organization on each of the three pillars of cyber security: people, policies and technology. **Here are some things to consider.**

PEOPLE
EMPLOYEE TRAINING AND AWARENESS

- [ ] **1. Ask scenario-based questions.** Applying a policy to a real-world situation will help better assess your employee's understanding of your organization's policies and procedures.

- [ ] **2. Simulate "social engineering" attacks (ex. phishing emails).** This will prepare employees for the type of attacks they are likely to face, and will make your entire organization more aware of cyber threats and more vigilant when encountering a real attack.

- [ ] **3. Allocate proper time and resources.** Training is often given low priority, but is one of the most essential parts of a cyber security infrastructure. It's important to spend just as much time assessing employee's knowledge of policies and best practices as you would assessing your technical vulnerabilities.

POLICIES AND PROCEDURES

- [ ] **1. Look at all policies documented across all departments.** Policies are often scattered across different departments. When assessing your policies, make sure to collect all security related policies.

- [ ] **2. Tailor your policies to your organization.** Not all organizations are the same, so your policies should be customized to fit your environment. It is important to balance security with usability so that your employees can function productively without compromising data.

- [ ] **3. Be Extensive.** Each policy needs to answer every question imaginable to be effective. Even a simple Password Management Policy should have more than 30 elements that outline how employees should create, update, share, and store their passwords.

TECHNOLOGY

- [ ] **1. Address Network, Server, and Web Application Vulnerabilities.** Many "IT Audits" don't assess every node in an organization, which could cause a major vulnerability to go undetected.

- [ ] **2. Perform Penetration Tests.** While obtaining a list of vulnerabilities within a network is helpful, it doesn't show which are exploitable if a bad actor were to target your organization. Penetration tests will show which of your vulnerabilities can allow a data breach to occur.

- [ ] **3. Do periodic engineering assessments of your network.** Networks tend to grow on an "as needed" basis, which causes a "spaghetti effect." Since the new functionality wasn't designed at the outset, it typically ends up as an appendage to the main network. This commonly creates security holes and unnoticed vulnerabilities. Keeping your network diagrams up to date allows you to see a more complete picture and will help you spot points of weakness you would otherwise miss.

Checklist derived from the original North Star Group blog post, **"Protect Your Data: Focus on Cyber Security's 3 Pillars."**