COMPASS
CYBER SECURITY

CYBER SECURITY ASSESSMENT CHECKLIST

WHAT TO CONSIDER WHEN PERFORMING A CYBER SECURITY ASSESSMENT

A Cyber Security Assessment is the first step in securing your organization's sensitive data. 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. Below are some of the most valuable things for your organization to consider.

PEOPLE (EMPLOYEE TRAINING AND AWARENESS)

☐ **1. Are you asking 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. Are you simulating "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. Are you allocating the 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. Are you looking at all of your 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. Are you tailoring 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. Are your policies comprehensive?**
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. Are you addressing all network devices?**
Many "IT Audits" don't assess every device in an organization, which could cause a major vulnerability to go undetected. Make sure your audit evaluates every technological component specific to your organization, including mobile devices.

☐ **2. Are the findings reports concise and actionable?**
The results of an IT security audit/assessment can be daunting so make sure the results of your assessment will be presented in an understandable and actionable format. COMPASS will assist you in interpreting the findings and give recommendations how to remediate the vulnerabilities within your network.

☐ **3. Are you planning for the future?**
Assessments will only show you a picture of your vulnerabilities at one point in time. Since new vulnerabilities are being discovered each day, it is important to plan for continued scans throughout the year to be proactive against a data breach.

For more information, please contact info@compasscyber.com or 667-401-5108.