CYBERSECURITY CHECKLIST

- [ ] **1. Cybersecurity Education:** Good security starts with a great security training program.
  - **a.** Educate employees on cybersecurity risks
  - **b.** Use phishing tests to determine the effectiveness of your training and show employees what malicious emails look like.
  - **c.** Track employee progress and focus on those who don't perform well during phishing tests.

- [ ] **2. Patch Management:** A key component of your defense program should include an automatic patching solution. Make sure you are running the most secure version of software.
  - **a.** Create a patch management update policy and stick to it.

- [ ] **3. Passphrases:** Previously termed "passwords," passphrases indicate a longer and more secure method of login protection and often use a sentence or phrase rather than a word as their base. Network passphrase policy should require strong passphrases (a combination of upper & lower-case letters, numbers and special characters) with periodic changes and no repeats.
  - **a.** Educate employees on the difference between passwords and passphrases and why secure credentials are crucial.
  - **b.** Create a passphrase policy and enforce it.

- [ ] **4. Event logging:** Logging is an important tool in discovering potential attacks and/or dishonest employees.

- [ ] **5. Risk Analysis:** Understanding the weaknesses in your network is half the battle.
  - **a.** Utilize a third party to assess the risk in your environment. If you're outsourcing your cybersecurity tasks, use a different company for your analysis.
  - **b.** Identify your vulnerabilities and create a plan to address them.

- [ ] **6. Segment, Segment, and Segment:** Not everyone on your network needs access to everything on the network. VLAN's are part of any secure network plan. Segment your network based on needs and risk as well as quality of service.
  - **a.** Review the current permissions in your organization.
  - **b.** Assess the validity of existing permissions and adjust as necessary.
  - **c.** Create a policy for network permissions and enforce it.

- [ ] **7. Backup and Backup the Backup:** If your network is compromised and/or fails, you'll need to restore as soon as possible. Backups that are backed up and secured off-site can be the game changer.
  - **a.** Perform routine Disaster Recovery (DR) Tests to ensure your backups and DR plan functions as intended.

- [ ] **8. Encryption:** Encrypting your data will store it in an unreadable format, especially mobile devices.

- [ ] **9. Limit Remote Access:** Not everyone on your network needs remote access to the network. Limit access to only secure means such as VPN.
  - **a.** Review the current permissions for remote access within your organization.
  - **b.** Assess the validity of existing permissions and adjust as necessary.
  - **c.** Create a policy for remote access and enforce it.

- [ ] **10. WI-FI:** One of the great weaknesses to any network is WI-FI.
  - **a.** Segment and turn on WPA2 encryption.

IT'S OK TO BE PARANOID. *Stay informed about risk on your network, It may seem fanatical, but it could prevent a major breach in your network.*

Call 1 (855) SAFE.NAV or email us at:
contact@acsltd.com to get started. **acsltd.com**

acs
Your Technology Compass