Many local government officials work closely with vendor or local IT personnel to maintain their computer systems. Here are some questions that officials should ask these providers to ensure that there are safeguards in place to help mitigate the risks associated with attacks.

- How are operating system updates applied to workstations and servers? Are these updates installed automatically or on a set schedule so that all current updates are installed timely?
- Are software and database patches applied timely?
- Do the workstations and servers have antivirus software installed? Is this software configured to receive definition updates automatically? How often does it run a scan to detect malicious software?
- If wireless networks are used, do they use encryption? Has the router password been changed from the default password assigned by the manufacturer? Is the network name hidden?
- Does the backup process capture all data vital to the operation of the office? In addition to the accounting system, are other critical files such as spreadsheets and documents backed up?
- If the office were to fall victim to a ransomware attack, is the backup process configured so that backup data would not be encrypted in the attack?
- Are firewalls properly configured to limit access to your network?