TENNESSEE COMPTROLLER OF THE TREASURY

Suggestions for Developing a Cybersecurity Response Plan

Being prepared to respond to a cyber attack will reduce the impact that it has on office operations. It is important to have a written plan that can be referenced in the event the office experiences an incident. The following are some suggestions for developing a plan. This plan should be developed in cooperation with the office's IT personnel or vendor.

- The plan should note what to do immediately after realizing you have fallen victim. This may require speaking with the office's IT personnel or vendor to know the best course of action. (For example, what should you do if you receive a ransom request or if you click on an email attachment that you think may be malicious? Should you turn off the machine, disconnect from the internet, change passwords, etc.?) Having talked with your IT personnel/vendor before this happens and documenting what do will save time in a critical situation.
- After the immediate response to the event, you should notify your IT personnel/vendor. Their contact information should be documented in the plan.
- Along with help from your IT personnel/vendor, assess the situation to see what data has been affected. Do you have an inventory of the data stored on each machine so that you will know what information may have been compromised? Are there any Word, Excel, text, or other files on desktops or in other folders that may contain sensitive information? Examples would be direct deposit payroll files or other files that are uploaded to your bank or investment files that contain Social Security numbers.
- Given the nature of the breach, determine if law enforcement should be contacted. You may also need to contact your bank.
- Based on the information compromised, you should determine the need to contact affected individuals. You will want to be familiar with Section 47-18-2107, *Tennessee Code Annotated* that addresses the breach of certain information.
- Do you have cyber insurance? If so, document the contact information for the insurance provider.
- If it is determined that the system will not be operational and will need to be restored, reference your disaster recovery plan for instructions on restoring the system.