OAG-update

October 2019

Office of the Auditor General
State of Rhode Island
(volume 2019-1)

October is national cybersecurity awareness month

Local governments, including two school systems and a fire department in Rhode Island, have been the target of recent ransomware attacks around the country. A ransomware attack can completely "lock" an entity out of access to their computer systems and related data – the interruption of services to citizens can be protracted and the costs to restore systems and functionality can be severe. Typically, a ransom amount (payable in bitcoin) is demanded to restore access to your data. Understanding the risks of ransomware attacks and assessing your readiness to prevent an attack or restore your systems in the event of an attack are critical. With Rhode Island local governments being recently attacked, the risks appear more imminent and the need for awareness and readiness is heightened.

There are things you can and should do to lessen your vulnerability to a ransomware attack:

- ***Implement cybersecurity awareness training for your employees*** **– this is a relatively low-cost but critically important effort. Ransomware attacks are typically accomplished through phishing emails to employees. Cybersecurity training for all employees can help them recognize likely phishing emails and react appropriately.**
- ***Ensure secure, timely and remote backups are performed for all data*** **- as part of an overall disaster recovery plan that will allow you to restore systems and data in the event of a ransomware attack.**
- ***Assess the configuration of your network, firewalls, servers etc.*** **– perform a risk assessment of your policies and procedures and the actual operation of your network and critical systems to determine your readiness to avoid a ransomware attack. Assistance in assessing cybersecurity risks is available through government and law-enforcement agencies as well as consultant/contractors engaged to specifically perform cybersecurity risk assessments.**
- ***Purchase cybersecurity insurance*** **- to minimize the financial impact of an attack.**

There are many resources available to assist local governments in (1) understanding cybersecurity risks and (2) assessing their readiness to minimize vulnerability and interruption of critical operations.

Links for ransomware prevention:

Center for Internet Security - Multi-State Information Sharing and Analysis Center (MS-ISAC)
https://www.cisecurity.org/ms-isac/

US Department of Homeland Security - Cybersecurity and Infrastructure Security Agency (CISA)

https://www.us-cert.gov/ncas/current-activity/2019/07/30/steps-safeguard-against-ransomware-attacks

https://www.us-cert.gov/ncas/tips/ST19-001

Rhode Island Joint Cyber Task Force: http://risp.ri.gov/ccu/cyber.php

OAG-update is intended to provide periodic information of interest to state entities, municipalities, school districts, charter schools and fire districts.

Contact the Office of the Auditor General at 401.222.2435 or dennis.hoyle@rioag.gov

Image by Darwin Laganzon from Pixabay