Cybersecurity Checklist for Cities

T=Time | $=Money

Policies, Planning and Training

$$TT	Create a cybersecurity strategic plan.
TT	Create a security policy signed by all employees and review with new employees during their orientation.
T	Create mobile device and “bring your own device” policies with clear security protocols.
T	Create email distribution lists to share and coordinate threat and vulnerability information with interested parties within your organization.
T	Conduct regular internal security meetings.
TT	Create a cybersecurity awareness training program, tied closely to an established security policy.
TT	Create an incident response plan specifying, in advance, what IT staff would do if x, y or z category of attack occurs.
T	Perform routine login account audits ensuring all accounts are active that should be. Disable accounts not used in a certain number of days.
T	Create a solid policy for in-out employee processing to ensure that all account access is shut down when employees separate from your organization.
T	Standardize on active-directory (AD) or Lightweight Directory Access Protocol (LDAP) compatible applications so passwords can quickly be deactivated across multiple systems.
T	Be cautious of “cloud” applications, as passwords may not be recoverable and often data access cannot be disabled by the agency.
T	Enforce strict password requirements meeting industry standards for complexity, length, and reset time limits.
$	Procure multi-factor authentication tools requiring a use to provide “something you have and something you know” for remote access to the network.
T	Implement a patch management program to keep servers and desktops up to date with the latest security patches that prevent known vulnerabilities.
$$$	Seek funding for a hardware replacement program so aging hardware doesn’t become unsupportable and vulnerable.
$$TT	Create a Continuity of Operations Plan (COOP) to document manual procedures during outages and prioritize recovery of systems.
$$TT	Create a disaster recovery plan to back up and recover data, equipment and infrastructure in the event of a disaster.
$T	Create a Continuity of Government (COG) plan in case of a major natural disaster, whereby certain governmental decision-making authority may be temporarily assigned to alternates.

Staffing

$$$	Create a full-time information security position.
$$	Fund staff training and certifications. You are competing with hackers who receive upwards of $100,000 per person in training to learn how to breach your network.

Services

$$T	Procure routine outside security audits, including penetration testing and Payment Card Industry (PCI) scanning for credit card systems.
$$	Procure additional security services through your Internet service provider (ISP) such as Distributed Denial of Service (DDoS) monitoring and mitigation.
$$$	Procure 24/7 managed security services through Security Operations Centers to identify real-time security threats and develop preventive counter measures.

Physical Security, Software and Hardware

TT	Maintain and routinely test backups keeping in mind public records and/or information access laws, records retention schedules and policies.
$$	Maintain redundant, off-site data storage in a hardened environment. (In computing, hardening is usually the process of securing a system by reducing its surface of vulnerability.)
$$$TT	Harden data centers.
T	Permit limited physical access to data centers, and perform regular security audits of those entering data-center facilities.
$$$TT	Consider moving to cloud services in a Tier 4 data center. A Tier 4 center guarantees 99.995 percent "up time," allowing less than an hour of interrupted service during a one-year period.
$T	Automate and maintain up-to-date virus protection for servers and desktops.
$$T	Procure next generation firewalls and tools including features such as intrusion prevention/detection, data loss prevention, anti-spam filters, anti-bot filters, content filtering and reporting, and threat emulation.
$$TT	Procure Security Information and Event Management (SIEM) event correlation and reporting tools.

Source: Deesing, Lea. *What City Officials Need to Know About Cybersecurity*. Government Technology, 23 June 2015. Web. 2 March 2017 Accessed.