Cybersecurity Investigator 2

Recommended Cybersecurity Precautions

Cybersecurity Precaution	Why is this important?
Awareness and Training for city employees	Humans are the biggest cybersecurity risk in any organization. Regular trainings can teach employees how to recognize and respond to social engineering; and how to protect their own accounts and data.
Advanced Awareness and Training for all city administrators and executives	Administrators and executives have more access to sensitive data and may require specialized training to understand their roles and responsibilities
Keep all city software up to date	Most security updates are designed to patch (or fix) existing security vulnerabilities. Hackers can attack through outdated software!
Invest in the most up-to-date antivirus software for the city:	Anti-virus software can prevent, detect, and remove malware
Hire a cybersecurity professional to manage the city network and detect any incidents:	Hiring cybersecurity professionals will increase your overall capacity, allow you to monitor potential incidents, and stay on top of ongoing concerns.
Conduct background checks on all employees	You can find out if any employee has a criminal record for committing a cyber-related crime, like identity theft
Request security documentation from all city vendors	City vendors -- which may include anything from construction to cleaning services to office supply vendors -- might have access to the city network or to sensitive data. Make sure that they take cybersecurity as seriously as you do!
Increase the city's overall bandwidth	Increasing the city's bandwidth will ensure there is enough bandwidth to run the most important applications and keep the website from shutting down in case of a distributed denial of service (DDOS) attack, which attempts to overwhelm a system or network with traffic and shut it down

Invest in firewalls	Firewalls work as a filter, preventing employees from accessing certain websites or transmitting sensitive information.
Run regular cyberattack simulations	Running a simulation allows you to try out and strengthen your response and recovery plan (Note: this is more effective if you have already have a plan in place!)
Encrypt all collected data	Even if there is a data breach, the encrypted data cannot be used
Create incident response and recovery plan for the city	When the next cyberattack occurs, employees will understand their own roles and be able to follow existing procedures
Inventory all of the physical devices, systems, and software in the city	You must know what your assets are before you can protect them
Conduct a security vulnerability assessment	It is important to know where your weak spots are so you can prioritize where to allocate resources
Limit privileges and data access to only the people who need it	The more people who have access to data, the more vulnerable it is.