CYBERSECURITY HYGIENE: A CRUCIAL IMPERATIVE FOR GOVERNMENT

September 2024

By Randy Hargus, Consultant

The reliance on digital infrastructure has brought about significant benefits for government, including enhanced efficiency and improved service delivery. However, it has also introduced new risks, particularly in the form of cyber threats. The importance of maintaining robust cybersecurity hygiene cannot be overstated. As custodians of vast amounts of sensitive information and operators of critical infrastructure, government must prioritize cybersecurity to safeguard their systems and the public they serve.

This article explores cybersecurity hygiene and the steps local governments can take to enhance their cybersecurity posture.

With vast amounts of sensitive information at stake, including citizens' personal data, financial records, and control systems for critical infrastructure, the consequences of a successful cyberattack can be devastating. These include service disruptions, financial losses, and erosion of public trust.

Several high-profile incidents have highlighted the vulnerabilities of municipal systems. For instance:

- **2019**: A ransomware attack on the City of Baltimore caused widespread disruption, affecting everything from property transactions to email communications. The city faced over $18 million in costs, including the ransom demand and the subsequent recovery efforts, a significant financial blow that could have been allocated to other critical municipal needs.

- **2018**: A ransomware attack on the City of Atlanta disrupted online billing and court services. The attack's aftermath was costly, with estimates suggesting recovery efforts exceeded $17 million.

- **2019**: A ransomware attack on Riviera Beach, FL, paralyzed municipal operations by encrypting their data. The city paid the $600,000.00 ransom but still faced significant costs for the full recovery of its data.

- **2020**: A ransomware attack on the City of Durham, NC, disrupted its systems, including its dispatch services. The city did not pay the ransom but incurred significant recovery costs.

- **2024**: The Bucks County, Pennsylvania emergency communications dispatching system was hijacked with ransomware.

Understanding Cybersecurity Hygiene

Cybersecurity hygiene refers to the regular practices and routines that individuals and organizations follow to maintain the health and protection of their digital systems. For municipalities, cybersecurity hygiene involves a comprehensive approach to securing their digital assets, from software and hardware to networks and data.

Key components of cybersecurity hygiene include:

- **Regular Software Updates and Patch Management:** Cybercriminals often exploit vulnerabilities in outdated software. Regularly updating and patching software closes these gaps, reducing the risk of a successful attack.

- **Strong Authentication Protocols:** Implementing strong password policies and multi-factor authentication (MFA) can significantly reduce the risk of unauthorized access. MFA, in particular, adds an additional layer of security by requiring users to provide two or more verification factors to gain access.

- **Data Backup and Recovery Plans:** Regularly backing up critical data ensures that it can be restored in the event of a cyberattack, natural disaster, or other emergencies. These backups should be stored in secure, offsite locations to prevent them from being compromised alongside primary systems.

- **Employee Training and Awareness:** Human error is one of the most common entry points for cyberattacks. Regular training and awareness programs help employees recognize phishing attempts, social engineering tactics, and other common cyber threats.

- **Access Control and Least Privilege Principle:** Access to sensitive information should be restricted based on individual roles and responsibilities. The principle of least privilege ensures that employees have only the access necessary to perform their jobs, minimizing the potential for insider threats or accidental data breaches.

- **Network Monitoring and Incident Response:** Continuous monitoring of networks for suspicious activity allows for early detection of potential threats. A robust incident response plan ensures municipalities can quickly and effectively respond to and recover from cyber incidents.

Why Cybersecurity Hygiene is Essential for Cities and Counties

1. **Protecting Sensitive Data:** Local agencies handle a wide array of sensitive data, including residents' personal information, financial records, and public safety communications. Ensuring the confidentiality, integrity, and availability of this data is paramount. A breach could lead to identity theft, financial fraud, or even compromise public safety.

2. **Ensuring Continuity of Services:** Municipal services are often critical to the daily functioning of communities. Cyberattacks that disrupt these services can have widespread and potentially severe consequences. For example, a ransomware attack that prevents accessto systems could prevent residents from accessing essential services such as water, electricity, or emergency response.

3. **Maintaining Public Trust:** Public trust is the cornerstone of effective governance. Citizens expect their local governments to protect their personal information and ensure the continuity of services. A significant cyber breach can erode this trust, leading to long-term reputational damage.

4. **Cost Savings:** While investing in cybersecurity measures may seem costly upfront, the long-term savings are substantial. The financial impact of a cyberattack—including recovery costs, legal fees, and potential ransom payments—can far exceed the cost of preventive measures. Moreover, strong cybersecurity hygiene can reduce insurance premiums, as insurers often offer lower rates to organizations with proven security practices.

5. **Enhancing Cyber Resilience:** Agencies with strong cybersecurity hygiene practices are better equipped to respond to and recover quickly from a cyberattack or other disaster. This resilience is crucial in minimizing the impact of an attack and restoring normal operations.

Practical Steps to Enhance Cybersecurity Hygiene

Municipalities can take several practical steps to improve their cybersecurity hygiene and protect against the growing threat landscape:

- **Conduct Regular Security Audits:** Regular audits of systems and networks can identify vulnerabilities and areas for improvement. To ensure a comprehensive assessment, these audits should be conducted by both internal teams and external experts.

- **Implement and Enforce Strong Policies:** Cybersecurity policies should be clearly defined, communicated, and enforced across the organization. This includes policies on password management, data handling, and incident reporting.

- **Invest in Cybersecurity Training:** Regular training for all employees—from IT staff to frontline workers —ensures everyone understands their role in maintaining cybersecurity hygiene. Training should be updated regularly to reflect new threats and evolving best practices.

- **Develop a Comprehensive Incident Response Plan:** An effective incident response plan outlines the steps to take in the event of a cyberattack, including communication protocols, recovery procedures, and roles and responsibilities. Regularly testing and updating the plan ensures that it remains adequate and relevant.

- **Engage with Cybersecurity Experts:** Partnering with cybersecurity experts, such as managed security service providers (MSSPs), can provide agencies with specialized knowledge and resources. These experts can assist with everything from threat detection and response to compliance management.

- **Leverage Technology Solutions:** Advanced technologies such as artificial intelligence (AI) and machine learning (ML) can enhance cybersecurity efforts by identifying and responding to threats in real-time. Agencies should explore using these technologies to bolster their defenses.

The Cybersecurity and Infrastructure Security Agency (CISA) is a government agency that provides expansive resources and services to both prevent, and respond to, cybersecurity events. See https://www.cisa.gov/.

Conclusion

As government continues to embrace digital transformation, the importance of cybersecurity hygiene cannot be overstated. The growing threat landscape demands a proactive and comprehensive approach to protecting digital assets, ensuring the continuity of services, and maintaining public trust. By adopting strong cybersecurity hygiene practices, municipalities can safeguard their systems, comply with regulations, and build a resilient digital infrastructure that serves the needs of their communities.

In the face of increasingly sophisticated cyber threats, cybersecurity hygiene is not just a best practice but a critical responsibility for municipalities. By prioritizing these efforts, local governments can secure their operations, protect their citizens, and ensure the continued delivery of vital public services.