The Importance of Data Storage Security in Local Government

You might think that cybercriminals are more likely to attack major cities because they have more data to take. While that's true, hackers are also aware that large cities have larger budgets for IT personnel and security systems than smaller communities. Many hackers are starting to favor the prospect of going after the low-hanging fruit by targeting smaller cities, towns and villages that have scarce budgets for cybersecurity.

Statistics Point to a Lack of Preparedness

The International City/County Management Association (ICMA) conducted a survey of local governments and found that 44% of the respondents admitted to being targets of cybercrime. In polling citizens, ICMA says that over 50% of citizens were not supportive of their local governments. Some of citizens' lack of trust may be due to the fact that ICMA reports 50% of citizens either don't support cybersecurity measures or don't even know that cybersecurity measures are or why they're so important at the local government level.

Unlike larger government systems, local government computer systems tend to be decentralized. The lack of coordinated systems gives cybercriminals the opportunity to create threats at multiple levels.

Why Advocating for Proper Funding is Critical

In addition, local governments historically lack staffing and budgeting for IT programs and specialists that would help them protect the community's sensitive data. States and provinces often have fairly small budgets to tackle cybersecurity concerns and they may need to distribute some portion of those funds to smaller towns and counties, which means that there's not adequate funding for cybersecurity on any level.

Not having the budget for the proper IT measures has a round robin effect on some communities. Lack of attention to cybersecurity may diminish the motivation and enthusiasm for staff and officials to ensure they have the proper cybersecurity measures in place. Lack of enthusiasm may translate into a lack of advocating for the proper funding to protect the community's data.

How Technology Can Bolster Security

The reality is that there's a way for nearly all local governments to protect themselves at a cost they can afford. Digital tools such as board portals have built-in security and stellar customer service, which means that local government staff and officials don't need to spend funds on IT specialists and other programs to ensure they're fulfilling their duty of care.

Tips for Building a Strong Local Government Security Breach Response Plan

The National Institute of Standards and Technology (NIST) developed five functions of the NIST cybersecurity network that serve as the pillars for a comprehensive and successful cybersecurity program. With these components in mind, local governments can follow these tips for building an effective security breach response plan.

1. IDENTIFY

Nail down the varying ways in which your local government could be impacted if a group or individual successfully hacked into your systems. This allows you to prioritize your efforts while developing an identified risk management strategy.

2. PROTECT

Align data security practices to your local government's risk management strategy so that all local government staff are properly educated on their roles in cybersecurity. This ensures that access to information will be protected and kept confidential.

3. DETECT

Implement systems that will identify anomalies and unusual events so that you can best determine the potential impact they could have. These systems will help your local government better identify the occurrence of a security breach at the earliest opportunity.

4. RESPOND

Establish a plan to respond appropriately to a cybersecurity incident quickly and with tact. Preparing a response plan ahead of time minimizes damages and keeps employees and the community informed and up-to-date.

5. RECOVER

Despite efforts to prevent any damages, local governments will inevitably face some negative aftermath following a security breach. Recovery activities should be aimed at the goal of restoring the government's operations to normalcy as soon as possible to reduce the overall impact of the breach.

Learn more about the endless possibilities in governance for government:

www.icompasstech.com

iCompass

A DILIGENT BRAND

Security

icompasstech.com

Overview

As part of the Diligent family of governance solutions, iCompass is the agenda management solution that provides customers with best-in-class security, top-rated customer support and constant innovation designed exclusively for the needs of state and local government. We streamline the governance process to help you better serve your community.

iCompass is the feature-rich, comprehensive platform for government. iCompass provides municipalities with an extensive suite of tools including agenda creation, meeting management, and board management solutions.

Data Hosting

iCompass is housed in world-class hosting data centers that are ISO27001 certified and maintain SOC attestations. The data center provides physical, environmental, and access security with the following controls:

- Intruder and door alarms monitored 24x7
- Mantraps positioned before all restricted areas
- A fully monitored proximity access control system
- HVAC system
- Heat and smoke detectors
- 24x7 on-site security presence
- Dedicated UPS systems and standby emergency power people support (i.e., generators)
- Government issued photo ID required for entry
- External and internal CCTV recording

Anti-Malware

Anti-Malware software is deployed to proactively detect and eradicate any virus or spyware infection from the system.

Data Security

Data is secured using industry standard encryption methods.

- All data in transit is encrypted
- Data center is ISO 27000 certified
- All Passwords and login information is stored and encrypted in a customer unique database

iCompass
A DILIGENT BRAND

Security
icompasstech.com

Data Recovery

iCompass ensures availability of data through varies means of redundancy in the unlikely case of an outage and protects against material loss of data.

Logging & Auditing

Application audits encompassing login history are available to administrators. A centralized monitoring server encompassing system logs are reviewed regularly.

Network vulnerability scans are performed monthly supplying standard classification for the purpose of addressing vulnerabilities via a risk based prioritized approach.

Internal Security Controls

The following internal controls have been implemented:

- Access to the hosted system is restricted to authorized personnel.
- All staff are required to undergo background screening prior to employment.
- Ongoing Security Awareness Training is distributed to all employees.

Application Controls

The iCompass software provides robust access controls for logging onto the system, which includes minimum password length. Customers have the flexibility to manage user permissions, document and meeting access, as required. Customers also have tools to audit public and by staff member document access.