Articles + Publications | March 1, 2024

Unique Aspects of Data Incident Response in Local Government

WRITTEN BY

Stephen C. Piepgrass | Sadia Mirza | Samuel E. "Gene" Fishel | Whitney L. Shephard

This article was originally published in American City & County on March 1, 2024.

For years, private companies have struggled to protect the data of consumers against security incidents and cyber-attacks by malicious threat actors. More recently, there has been a growing surge of data breaches impacting the public sector, and local governments face unique challenges in responding to such incidents.

The triage and analysis required following the discovery of a security incident can be a difficult and costly undertaking for any organization. Even private companies with vast resources and large cybersecurity budgets that seemingly do everything “right” when it comes to protecting themselves against cyberattacks can still find themselves in the unenviable position of responding to a security incident.

The challenges of cybersecurity are particularly intense for state political subdivisions, which often handle a wide variety of personal data because of the number of departments within each locality and the nature of the services those departments provide. These factors can exacerbate the already complex task of determining the scope of a security incident and, subsequently, who an entity is required to notify, and when such notices must be sent.

In addition to facing a major financial loss from both the cost of the initial response and any necessary security hardening measures, for local governments the fallout from the reputational damage caused by consumer data exposure can negatively impact civic engagement and public trust. Security breaches can also interrupt critical services performed by local governments, such as public utilities, law enforcement activities and emergency services.

Local governments face unique risks and challenges when it comes to data security and incident response. Localities house a great deal of personal data and that, combined with a lack of public resources to dedicate to cybersecurity hardening and incident preparedness, makes them an attractive target for threat actors. The frequency at which data breaches are happening at the local government level only seems to be increasing, and localities should anticipate this trend will continue.

In March 2022, the FBI released a special report warning local governments about their increased risk of being victimized by cyber threat actors. According to the report, based on incident reporting to the FBI between January and December 2021, local government entities were one of the most targeted groups by cyber attackers, second only to academia. The methods used by threat actors to gain access to sensitive data have diversified over the years, while also becoming more and more sophisticated. According to the FBI, the most commonly employed techniques against government entities are phishing emails, remote desktop protocol exploitation and software vulnerability exploitation.

For local governments, determining the appropriate next steps can appear nearly impossible, given the number of departments and the diversity of information they often house. While government entities are typically protected from class action lawsuits by sovereign or governmental immunity, they are often still required to provide notice to consumers and/or regulators under state breach notification laws. Who an entity is required to notify and when is dependent upon multiple factors, including the number of consumers impacted, the state of residence of any impacted consumers and the type of information exposed (*e.g.,* personal identifiable information, personal health information, etc.).

There are ways localities can mitigate their risk of suffering a data breach—and restore and maintain trust from the citizens they serve—should they experience an inadvertent exposure of sensitive data or find themselves the victims of a cyber-attack.

When it comes to avoiding common cyberattacks, localities should consider the following steps:

- Implementing user training programs and conducting phishing exercises.
    - Requiring strong passwords and enabling multi-factor authentication for as many accounts as possible.
    - Maintaining offline backup data and ensuring that backup data is encrypted
    - Segmenting networks to mitigate the spread of ransomware.
    - Implementing time-based access for privileged accounts.

Government entities should also be judicious about any private-sector companies they choose to do business with, especially if the services a third party will be providing involve the handling of, or access to, any sensitive personal data belonging to their constituents.

Localities can also take several steps to mitigate harm if a breach occurs. Having an incident response plan in place before falling victim to a breach, as well as proper data management practices that allow for timely identification of the type of information that was accessed, can make responding to an incident a much smoother experience. Proper messaging is another critical aspect of an organization's response. Localities should be prepared to make decisions about the level of information to share, when to share it, and how to respond to any follow-up. In the eyes of regulators, and any impacted consumers, how an entity reacts following a security incident is just as important—if not more so—as any factors that allowed for the occurrence of the incident in the first place.

RELATED INDUSTRIES + PRACTICES

- Incidents + Investigations