Industry Brief

mimecast

Industry Brief for Public Sector: State and Local Government

Mimecast is the cloud platform that enables state and local government organizations to secure citizen and other sensitive data as demands for digital public services increase.

The need to enhance and expand digital public services has grown tremendously as technology continues to advance.

Both the public and government employees want to be able to access information, pay bills and update services quickly and seamlessly, using different digital interfaces, including smartphones, tablets and laptops. The public assumes their data is protected, and it is critical for government organizations to safeguard personal data against unprecedented cyber threats. Cyberattacks have the potential to cripple services and affect the day-to-day functioning of state and local government organizations. At the same time, the impact on individuals can be deep and long-lasting.

Public sector organizations play a key role in contributing to the health, stability, and efficiency of the United States' economy. Local and state government organizations hold significant amounts of personal data about their citizens that must be secured.

Why Mimecast:

- More than 750 government organizations trust Mimecast for cyber resilience
- Dramatically reduce the risk of sophisticated attacks including phishing, ransomware weaponized attachments, and malicious URLs
- Reduce the burden on strained IT staff: a single pain of glass for email security, web security, archiving and continuity streamlines configuration, reporting and troubleshooting
- Keep services running and quickly restore data when attacks do get through
- Align budgetary constraints with an affordable, predictable cost of ownership
- Empower employees with security awareness knowledge, making them an asset in protecting against cyber attacks
- Rich APIs to integrate to existing SIEMs, monitoring and reporting systems
- Store data with the assurance and confidence that it is protected at Federal standards – located entirely on U.S. soil and staffed with U.S. Citizens
- On the Texas Department of Information Resources (DIR) approved list for Cybersecurity Awareness Training

With many local governments facing funding challenges, cybersecurity spending is lower than it should be. And, given public entities rely on tax dollars for all operational aspects, a combination of budgetary constraints and limited IT resources prevent many of these organizations from implementing security solutions at a scale and pace required to adequately protect them from today's evolving cyberthreat landscape.

As a result, state and local government organizations are natural targets for ransomware and other cyber-threats, including phishing and malware. Many of these attacks are launched with the intention of crippling the day-to-day operations of public sector institutions and/or stealing valuable PII (personally identifiable information) to sell on the black market for significant monetary gains.

Recent high-profile cybersecurity incidents, such as ransomware attacks against state and local government organizations, highlight the vulnerability of public organizations and the profound impact that successful attacks can have on citizens. Local authorities must inspire public trust by protecting the personal information they hold, and guarding against threats from a variety of sources, including criminal hackers, hacktivists, insiders and foreign nation-states. They must also be prepared to respond and recover quickly when a breach occurs.

A multi-layered security strategy is the most effective way to reduce risk, keep operations running, and safeguard the data that state and local government organizations are entrusted to hold.

Challenges

Moving to the Cloud

HIT Teams are comfortable with their on-premises environments and tend to err on the side of 'if it ain't broke, don't fix it.' However, on-premises hardware can be hard to secure, difficult to scale and cumbersome to update and maintain. Security lapses from unpatched systems and hardware that is not regularly upgraded can pose significant security challenges.

A hacker only needs to find one vulnerability to take down the entire local, and potentially state, network. Transitioning services to the cloud enables government organizations to modernize and streamline services for the public, adopt new technologies and offer newer, better services overtime, improve service efficiencies and reduce operational costs.

Mimecast delivers a 100% cloud-based security solution that enables government organizations to scale (speed or size) as needed. System updates are applied in real time, ensuring organizations always have the latest security protections in place. This all results in reduced IT staff overhead with regards to system patches, updates and hardware upgrades.

Limited Budgets and IT Resources

State and local government organizations have limited budgets for security spending and IT investments. They answer to taxpayers who would much rather see their tax dollars used on something tangible – repaving of roads – than something they can't see (securing data). Government officials are constantly under high scrutiny on how budgets are allocated and as a result, cybersecurity spending is often lower than it should be.

Mimecast provides true cloud architecture, reducing both operating and capital expenses, while dramatically improving performance and preserving the organization's ability to manage and monitor its email and web security posture. A single pane of glass streamlines configuration, reporting and troubleshooting.

A Soft Target for Ransomware

Local governments house a lot of sensitive personally identifiable information (PII) on their citizens. Lean security budgets and limited in-place protections make them soft targets for hackers and nation-state actors who want to steal sensitive data, gain access to state (and national) networks, spy on government activities and cause disruption and/or economic harm to the United States. As a result, the number of ransomware attacks on state and local governments is steadily increasing. There is no guarantee that a hacker will release encrypted/stolen files even if a ransom is paid.

Mimecast provides a cyber resilient solution that protects organizations before, during and after a ransomware attack occurs. Comprehensive email security protects against email-borne threats. Integrated web services boost defenses by preventing infiltration and the spread of attacks. Sync and Recover enables point-in-time archive retrieval of mailboxes, calendars and contacts.

Sophisticated and Customized Phishing Attacks

The digitization of public records has made it easier for hackers to personalize phishing emails and target government employees using more 'realistic' attacks. Many state and local agencies rely on intranet sites to communication with vendors and supplies, introducing another point of vulnerability in which supply chain integrity and security can be compromised. Trusted vendors introduce an additional attack vector as employees are more likely to trust attachments, links and emails that come from these partners.

Mimecast delivers comprehensive protection against email-borne malware including malicious URLs and attachments, spear-phishing and impersonation attacks. Mimecast integrated web security services block access to malicious websites and boost defenses by preventing the infiltration and spread of attacks.

Addressing Security Awareness

Human error is a leading cause of security breaches and can cost government organizations in financial losses (ransoms, business disruption equating to compromised revenue streams) and reputational damage (loss of confidence by the public). One wrong click and the entire local or state network can be compromised. Educating employees enables them to be aware of the evolving threat landscape and make smart decisions that help protect the organization.

Mimecast Security Awareness Training delivers comprehensive cloud-based education modules, risk scoring and phish testing to improve employee security awareness and reduce the organization's cyber risk resulting from 'human error'.

Gold Cybersecurity Excellence Award for Government Industry Solution

The Cybersecurity Excellence Awards is an annual competition honoring individuals and companies that demonstrate excellence, innovation and leadership in information security. Mimecast for State & Local Government was named a gold winner for the 'Government - North America (between 1,000 - 4,999 employees)' category.