proofpoint.

SOLUTION BRIEF

How Proofpoint Helps Protect Local Governments

Defend City Hall from cyber threats with our people-centric solutions

Products

- Proofpoint Email Encryption
- Proofpoint Email Protection
- Proofpoint Email Fraud Defense
- Proofpoint Threat Response Auto-Pull (TRAP)
- Proofpoint Threat Intelligence Services (PTIS)
- Proofpoint Content Capture

Key Benefits

- Protect critical infrastructure such as roads, bridges, water systems and elections
- Prevent financial and real estate fraud
- Enable rapid response to incoming threats
- Manage legal and compliance risk

Media coverage of government in the United States typically focuses on what happens at the national and state levels. But local governments are just as important, if not even more so. Local governments are more directly accountable to their citizens than their federal or state counterparts. They are more in tune with the needs of their people. And they provide myriad services that define their quality of life.

The diverse services that local governments offer, however, make them attractive targets for cyber criminals. These local entities are vulnerable to many kinds of financial fraud, among them the growing threat of ransomware. Local governments also have the important duty to preserve core democratic processes in their jurisdictions. They administer elections, which also makes them of interest to nation-state actors.

Proofpoint can help protect local governments from these threats. Our people-centric approach to cyber defense focuses on protecting the individuals most likely to be targeted. Our solutions enable rapid response to threats. They minimize the risk of financial fraud. And they let local governments manage legal and compliance risk by preserving all communications.

Local Government Cybersecurity Challenges

Local entities are usually responsible for the following:

- Local streets
- Fire, police and other emergency responders
- Water and sewer infrastructure
- Planning and zoning
- Public transportation
- Parks and recreation
- Election administration

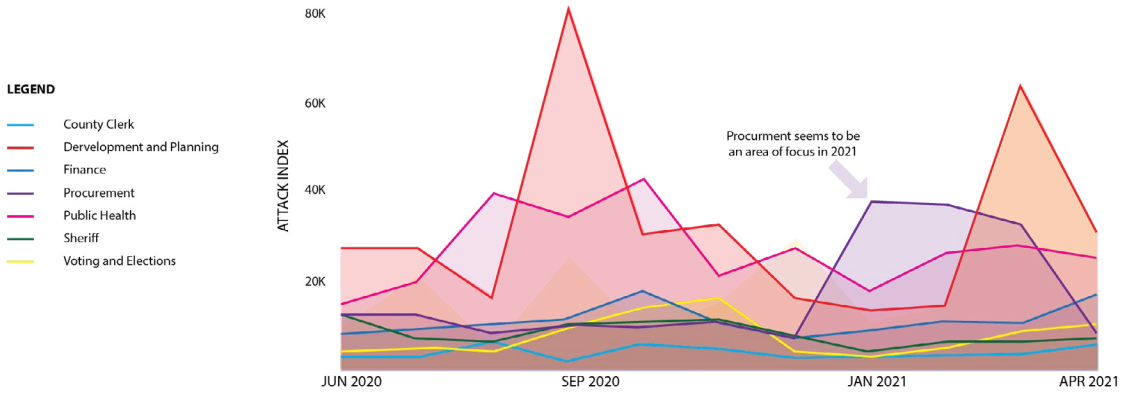

Figure 1: Top seven departments targeted at a county government.

This diversity of services makes local governments an enticing target for cyber criminals. Financially motivated criminals covet the personal data of citizens that local governments hold; they are also interested in accounts payable information about vendors and contractors. Nation-state actors are interested in election infrastructure; they are also sometimes interested in other critical infrastructure, like water systems.

State and federal agencies may have a lot of the same sensitive data in their IT systems. But cyber criminals often consider local entities to be easier to infiltrate because they have fewer resources to devote to cybersecurity. And while much attention has been given to the vulnerability of national critical infrastructure like the electric grid, the shutdown of a local water or sewer system could be disastrous for hundreds of thousands of people.

A spike in ransomware at water and sewer utilities

Ransomware is a growing threat in every industry. And attackers use increasingly sophisticated tactics not only to lock up systems, but also to exfiltrate data. Since 2020, water departments seem to have been the most common targets for ransomware delivery within local governments. Water departments provide a necessary service. So attackers know that water agencies are likely to pay the ransom rather than allow the service to stop, even for just a short time.

Attacks on planning and zoning during real estate booms

Real estate fraud is cyclical, but it causes true damage. When prices appreciate rapidly, cyber criminals increase their attacks on planning and zoning departments. They hope to profit from fraudulent transactions or gain insider knowledge of development plans.

Nation-state interest in election infrastructure

Election interference by nation-states is already a well-known problem. And local governments often take the brunt of these attacks. The entities that administer the elections face cyclical threats that increase in the weeks leading up to election day. Hackers can gain valuable personal identifiable information (PII) on citizens. They can potentially even alter vote tallies.

Financial fraud with emergency responders

While fire, police and ambulance services do not hold PII on every citizen like other local departments might, these entities spend a lot of money. Financially motivated attackers tend to target people who manage supply-chain and logistics aspects of these departments. Through these employees, the criminals can launch business email compromise (BEC) attacks that send fraudulent invoices.

Taking a People-Centric Approach

These days, cyber attacks target people, not technology. This means that your local government district must respond with a people-centric approach to securing sensitive data.

Figure 1 illustrates the top seven departments that cyber criminals have targeted at an actual county government. Note the cyclical nature of the attacks on each department. One interesting trend headed into 2021 is an increased emphasis on employees in the procurement department. Another trend is a dip in interest in public health agencies. This may be in anticipation of the economy stabilizing after the COVID-19 pandemic. Note also that the development and planning department had two major spikes in attacks over a 12-month period.

Phishing emails remain the No. 1 way that adversaries get into networks. According to our Proofpoint 2021 State of the Phish report, 57% of respondents said that their organization experienced a successful phishing attack in 2020. The percentage of organizations for which this attack resulted in data loss ballooned to 60%. This represents a 40% increase over 2019.

How Proofpoint Can Help

Proofpoint gives you the tools you need to protect your people across multiple departments. This section describes the many ways we can help.

Rapid threat response

Real-time response to attacks is critical in today's fast-moving threat landscape. And cyber criminals use email more than any other vector to attack local government employees. When governments can't respond in a timely manner, adversaries have more time to move laterally in the network and cause damage.

Proofpoint solutions to address these concerns include the following:

- **Proofpoint Email Protection.** As the industry-leading email gateway, this helps you identify and block malicious email using machine learning and multilayered detection techniques.
- **Proofpoint Email Fraud Defense.** Augments defense with comprehensive brand protection and visibility on attacks in the supply chain.
- **Proofpoint Threat Response Auto-Pull (TRAP).** Brings automation to the manual processes that your messaging and security administrators go through to analyze suspicious email that has made it through filters.
- **Proofpoint Threat Intelligence Services (PTIS).** Helps your agency understand the historical context of threats to fight them better in the future.

Mitigation of legal and compliance risk

Local governments must defend against lawsuits. They must also use the legal system for public safety. What's more, governments face requirements and regulations that many other industries do not. Entities must retain all content from all tools that employees use to communicate. They must also make it easily accessible by topic and user.

Proofpoint solutions to address these concerns include the following:

- **Proofpoint Content Capture.** Archives required content to your data store or downstream services while maintaining a clear and compliant chain of custody.
- **Proofpoint Email Encryption.** Keeps the content of emails from being intercepted by triggered encryption. For example, users can trigger encrypted messages automatically by adding a keyword of choice to the subject line.

Financial fraud defense

A lot of money moves through local governments. This fact does not escape the notice of financially motivated hackers.

Proofpoint solutions to address this concern include the following:

- **Proofpoint Data Loss Prevention (DLP).** Mitigates the risk of email data loss and protects against email fraud.
- **Proofpoint Email Encryption.** Keeps the content of emails from being intercepted by triggered encryption. For example, users can trigger encrypted messages automatically by adding a keyword of choice to the subject line.

Conclusion

An increasingly centralized news media focuses on the politics of Washington. But local governments do some of the most consequential work to improve the lives of citizens. To keep this work going, Proofpoint can help your agency protect its most important asset—its people. By doing that, you protect the confidential data that cyber criminals want. Whether they are targeted through email, the web, social media or cloud apps, we provide the most effective cybersecurity by protecting interactions between people. We help stop threats before they reach their targets. This helps safeguard your valuable data and protects local assets from cyber attacks.

LEARN MORE

For more information, visit **proofpoint.com**.