

# How Proofpoint Helps Protect Local Governments

Defend citizen services 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 Service
- 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

Local governments play an important role in modern society. They maintain critical infrastructure and offer a vast range of public services. They are also directly accountable to their citizens. And because they administer elections, they have a duty to preserve core democratic processes in their jurisdictions. Despite their responsibilities, however, local government agencies are often wracked with IT resource constraints. So, it is no wonder criminals and nation-state actors alike find them such inviting targets for cyber attacks.

Proofpoint can help. We take a people-centric approach to cyber defense, focusing on protecting the people who threat actors are most likely to target. Our solutions enable rapid response to threats. They also minimize the risk of financial fraud and they allow local governments to 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

The diversity of services they offer makes local governments an enticing target for cyber criminals. Financially motivated criminals seek the personal data of citizens that local governments hold; they are also interested in accounts payable information for vendors and contractors. Nation-state actors often take a keen interest in election infrastructure; they also target other critical infrastructure, like water systems.

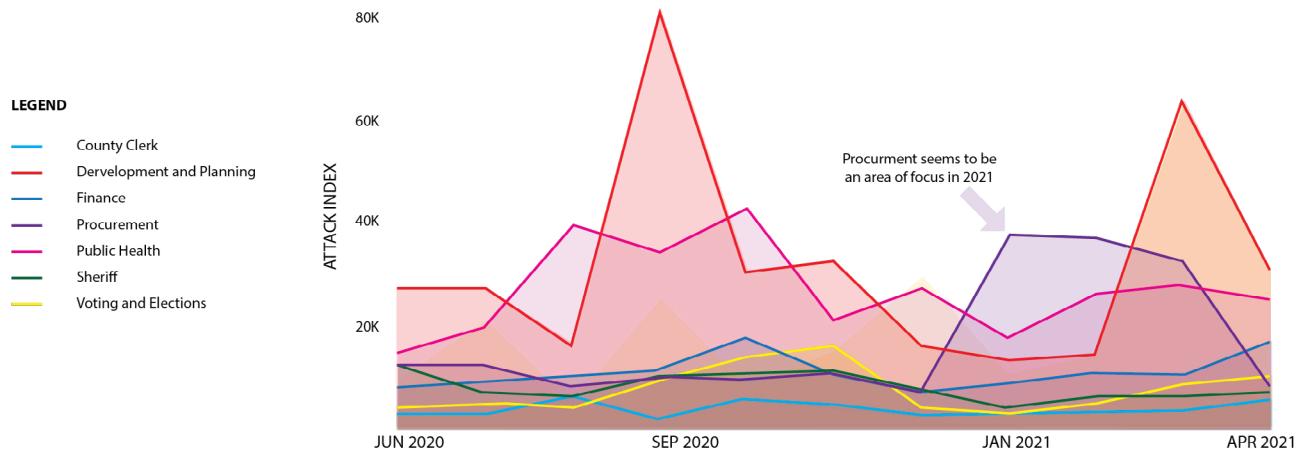


Figure 1: Top seven departments targeted at a county government.

State and federal agencies hold sensitive data in their IT systems as well. But cyber criminals often consider local entities to be easier to infiltrate. This is because local governments do not have the same kind of resources to devote to cybersecurity. And while a lot of attention is 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. This is true in every industry. Attackers use increasingly sophisticated tactics not only to lock systems, but also to exfiltrate data. Since 2020, water departments seem to have been the most common targets for ransomware delivery in local governments. These departments provide a necessary service. So, attackers know they are likely to pay the ransom rather than allow the vital 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 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.

### A People-Centric Approach

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

Figure 1 shows the top seven departments that cyber criminals have targeted at a real county government. Note the cyclical nature of the attacks. One trend headed into 2021 was an increased emphasis on employees in the procurement department. Another trend was a dip in interest in public health agencies. This may have been 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 was the No. 1 way that adversaries got 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 many ways we can help.

### Rapid threat response

Real-time response to attacks is critical in today's fast-moving threat landscape. 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.** Helps your agency understand the historical context of threats to combat 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, they 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

Financially motivated hackers know that a lot of money moves through local governments. Proofpoint solutions to address this concern include the following:

- **Proofpoint Data Loss Prevention.** 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

Local governments work to improve the lives of citizens. Proofpoint can help you protect your most important asset—your people. We help you protect the confidential data that cyber criminals want. Whether they are targeted through email, the web, social media or cloud apps, Proofpoint provides the most effective cybersecurity by protecting interactions between people. We help stop threats before they reach their targets. This helps safeguard valuable data and protects local assets from cyber attacks.

### LEARN MORE

For more information, visit [proofpoint.com](https://www.proofpoint.com).

#### ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 75 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at [www.proofpoint.com](https://www.proofpoint.com).

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners. [Proofpoint.com](https://www.proofpoint.com)