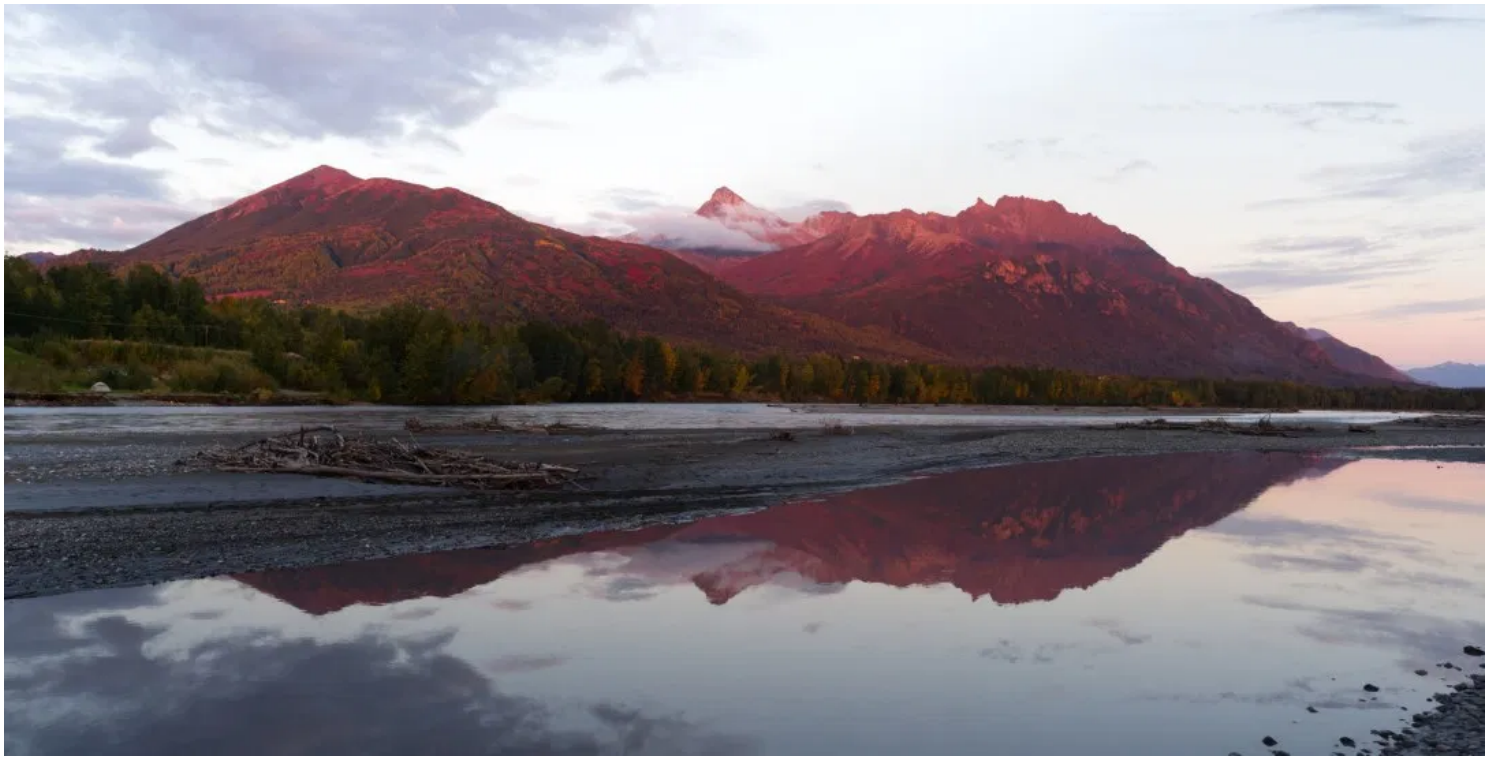

How One Alaskan Borough Survived A Cyber Attack

By **NLC Staff** on **October 1, 2019**

In today's cyber landscape, every city, town and village in America is vulnerable to hackers. And while some local governments are taking steps to prevent and mitigate harm, many more municipalities remain completely unprepared, leaving their communities in danger of losing millions of dollars and priceless data.

This is an urgent issue for cities of all sizes. To help local leaders address it, the National League of Cities will release the *first-ever* cybersecurity guide for local leaders later this month. But in honor of National Cyber Security Month, we're bringing you a sneak peak of our report.

Case Study: Matanuska-Susitna Borough, Alaska

In Matanuska-Susitna (also called Mat-Su), a borough of about 103,000 people in southern Alaska, local officials felt secure. Before the attack, the borough monitored web, email, and network traffic; they'd already weathered DDOS attacks, viruses, malware, and ransomware; and they had a good backup/disaster recovery system designed to withstand the next big Alaskan earthquake.

But in mid-2018, several Alaskan local and state government organizations were hit by cyberattacks. Matanuska-Susitna was hit with an advanced malware suite on July 23, 2018, which took down 150 servers and nearly 600 desktop computers. Mat-Su and the nearby city of Valdez were completely incapacitated. The two governments were both infected with ransomware, but responded differently: Valdez decided to pay the ransom, whereas Mat-Su did not.

Upon investigation, Mat-Su found that the attack had infected and encrypted their backups. Primary cleanup and mitigation took three months and cost $2.5 million. To reduce the risk of a new infection, both cities completely rebuilt their networks and scrubbed all data imported to the new networks.

There are many models for cybersecurity, the most common of which, *prevention*, is no longer enough. After the attack, Mat-Su augmented its security protocols: today, its multi-level email filters capture more than 650,000 bad emails an hour. But despite the robust prevention processes, there are still dozens of targeted email attacks that get through daily. Alone, the prevention method has to be correct 99 percent of the time. For that reason, Mat-Su now uses the *detect and contain* approach as well.

Recommendations from the National Symposium for Cybersecurity in Government

Last week, government leaders, researchers and advocates gathered to discuss cybersecurity best practices at the Symposium for Cybersecurity in Government. The event was a collaboration

between CompTIA/Public Technology Institute (PTI) and other state and local organizations to identify best practices and pitfalls for leaders.

There were five clear takeaways from the event. In order to detect and contain cyberattacks, Local governments, like Mat-Su, should:

- Get creative with budgeting
- Use trusted third-party security services,
- Routinely check the workforce for information gaps,
- Craft a culture of good practices, and
- Have a response plan ready to go should an attack occur

Any city could be attacked, so training staff to identify and curtail risks, as well as implementing measures to respond when attacks occur, is critical.

About the author: *Kyle Funk is the research assistant, urban innovation, at the National League of Cities.*

Cybersecurity Webinar: Is Your City Vulnerable to a Cyber Attack? Chances are the answer to the question above is yes, and chances are there is more you can do to reduce the risk to your city's infrastructure and its citizens. To help raise awareness

Get Your City Cyber Ready with CISA's Cyber Essentials

Malicious Russian Cyber Activity is Targeting Government Networks