SECURITY UNDER ATTACK

ORLEANS PARISH COMMUNICATION DISTRICT FENDS OFF CITYWIDE CYBERATTACK

ORLEANS PARISH COMMUNICATION DISTRICT

- Established: 1982
- Area Served: Orleans Parish, New Orleans, LA
- Total Number of Employees: 180

THE EMERGING THREAT: CYBERATTACKS ON PUBLIC SAFETY AGENCIES

With the rise of the digital age, many law enforcement processes have become quicker and more efficient. Records and other files are increasingly being digitized, eliminating literal piles of paperwork and streamlining the overall reporting process to help keep law enforcement officers on the streets instead of behind a desk. Many agencies rely on the internet and interconnected systems for emergency calls as well as other daily tasks that help agencies respond to their citizens' needs.

But with the increased dependence on digital technology comes its own risks, such as potential attacks on those computer networking systems as agencies fall victim to cybercrime. Hackers use cyberattacks such as ransomware on law enforcement agencies and local governments as an attempt to exploit sensitive information and disrupt essential government services. These attacks, which encrypt files so agencies can no longer access the information until a ransom is paid, are part of a national trend of cyberattacks by hackers savvy enough to exploit system vulnerabilities. Recovery can be a long and difficult process that may require the services of a data recovery specialist, and some agencies pay to recover their files. However, there is no guarantee that all files will be recovered even if the ransom is paid.

FEELING SECURE EVEN WHEN DISASTER STRIKES

The last thing an agency wants to hear on any given day is a call for emergency shutdown because they have been targeted by a sophisticated cyberattack. Unfortunately, it has become increasingly common, and in December 2019, the city of New Orleans became the latest victim of a ransomware attack.

Tyrell Morris, Executive Director for Orleans Parish Communication District (OPCD), received the message from New Orleans Homeland Security the morning of the attack. His team immediately sprung into action, unplugging and shutting down all of the department's computer systems as part of their planned process in response to such a situation.

OPCD is an independent agency of the state government, however they still use individual consoles for everyday work that are connected to the city's network and needed to be unplugged. There was also a switch in the server room that brought the city internet into the department, Morris said, which he and his team quickly turned off.

In the hours and days following the attack, OPCD became increasingly aware that many of its systems were unaffected by the attack on the rest of the city.

> **"[As] we begin to look at what happened, the same ransomware that attacked the city at 5:00 a.m. that morning made an attempt to attack our CAD firewall at the same time. It was successful on the city's side; it was unsuccessful on ours."**
>
> – Executive Director Tyrell Morris

Although Morris first learned of the attack through the established New Orleans' system-wide process, he was appreciative of the calls and texts he received from Motorola Solutions representatives regarding the breach.

"They offered their support in any way," he said. "I think the biggest support was helping us to rapidly deploy PremierOne Mobile."

The Monday following the Friday attack, New Orleans Police Department (NOPD) detectives were working on personal computers from home, shut out of access to some essential law enforcement networks. After the cyberattack led officials to flip the killswitch on the city's computer systems, officers were unable to retrieve information about license plates, access police reports or enter arrest warrants into a national database, law enforcement sources said. None of these usually routine tasks could be completed through the standard electronic channels.

"We knew that the faster we could deploy [PremierOne Mobile], the faster they could resume doing electronic police reports because they were doing everything by hand and by paper and that was a nightmare," Morris said.

"We also did NCIC integration through CAD so they didn't have to run on a secondary system to run names and things like that," he said. "We took over all of the warrant confirmation process for the police department because they had to use computers they didn't have. So, Motorola [Solutions] was here on the ground with us, getting that back up and running," said Morris.

MOVING FORWARD

Cyberattacks have proven so disruptive that in some cases public agencies and private businesses have either paid the ransom, taken out costly insurance policies or rebuilt entire networks in order to better ward off future attacks.

After hackers breached the city's defenses in December, New Orleans Mayor LaToya Cantrell's administration budgeted to raise the city's $3 million insurance policy to $10 million. The city also moved to replace outdated or compromised computers and paid workers to wipe computer drives and upgrade software.

Before OPCD brought any system back up, Morris and his team made sure all the data and systems were cleaned.

"We had to get these sophisticated ransomware finders and cleaners and every system had to be done," he said. Because the agency's Integrated Call Control and CAD systems run on separate networks, OPCD did not believe the phones had been compromised. However, Motorola Solutions performed a system check to ensure both systems were performing at optimal levels and functioning properly, according to Morris.

As a result of the attack, Director Morris said a decision had been made by city and agency administrators to transition all available critical public safety systems to the cloud, in hopes of being better prepared to combat future cyberattacks.

A TRUSTED CLOUD AND SERVICE PARTNER

According to Morris, directly after the attack on City of New Orleans systems, Motorola Solutions was on the ground to help OPCD get systems back up and running, assisting the agency as it became the beacon of hope to surrounding agencies and departments during this crisis.

After he and other agency administrators made the decision to move critical systems to the cloud, Morris quickly realized that information security management is getting increasingly complex and best left to partners who know how to handle what's needed.

Having a partner in preparing for and preventing cybersecurity threats could make all the difference for your agency. However, the potential benefits of pairing your mission-critical technology ecosystem with end-to-end services can only be achieved by selecting the right provider—one that can successfully deliver seamless orchestration of people, processes and tools. While it's possible to institute the right processes, hire the right people and secure the right tools in-house at your agency, such efforts can be highly challenging and costly.

Protecting your agency's technology investment is essential, because it's no longer a question of if you'll be hacked, but when.

To learn more about how Motorola Solutions safeguards operations and protects critical network infrastructure from cyber threats, visit www.motorolasolutions.com/cybersecurity

KNOW WHAT MATTERS, WHEN IT MATTERS

We build software for mission-critical environments where every second matters. PremierOne and other applications in our CommandCentral software suite unify data and streamline workflows from call to case closure in order to put your information to better use, improve safety for critical personnel and restore your focus on the communities you serve. Backed by a trusted, 90-year expert with proven public safety leadership, our suite is transforming the public safety experience with a focus on evolution, not revolution, in order to help you digitally transform your operation.

For more information about PremierOne CAD, please visit motorolasolutions.com/p1-cad

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, Il 60661 U.S.A. **motorolasolutions.com**