pluck

Case Study

Overseeing recovery from a citywide Ransomware attack

In May 2019, former Baltimore Mayor Pugh stepped down due to a growing criminal probe that ultimately resulted in her indictment and conviction. Bernard C. “Jack” Young, the sitting City Council President, was sworn in to serve the remainder of her term. Young asked Sheryl to return to the Baltimore City government as Deputy Chief of Staff for Operations during this period; she’d served in City government from 2007 to 2012. In this role, Sheryl was responsible for overseeing Baltimore City’s core operating agencies.

Prioritizing service restoration

On the day Mayor Young was sworn in, Baltimore was hit by a crippling Ransomware attack. Like many cities, Baltimore had an aging IT infrastructure and many outdated computer applications. City officials estimated the cost of the “file-locking” attack at $18 million, including system restoration and lost revenue.

Sheryl directed the City’s recovery efforts, bringing together the right resources, overseeing the development of a recovery plan, facilitating agreement on the plan and enabling implementation. She was also the face of the response to the attack, responding to media and City Council inquires, providing almost daily, transparent, honest updates until most systems were restored.

Process & Outcome

She immediately assembled her team, which included members of the Citistat (data-driven management system that monitors/improves City performance in real time) and Innovation Offices. Their first task was a full assessment of City services to determine which had been affected. Every application needed to be assessed before they could develop and implement a recovery and improvement plan.

They began by creating a template to collect hundreds of pieces of information and criteria to identify the areas needing priority restoration and quickly discovered that without manual intervention, many transactions would remain frozen. The attack had halted email access for City employees; disabled the City’s ability to process online payments; and disrupted computer access to multiple databases.

Individuals, for example, couldn't record real estate transactions or obtain lien certificates, which meant they couldn't buy or sell homes and other properties in Baltimore City.

Real estate transactions involve a number of City agencies as well as private title companies, lawyers and the courts, and they determined a manual workaround was needed until online services were restored. The team met with key stakeholders, mapped out the steps to manually recreate processes and proposed an action plan for those involved to agree to. They developed and implemented a solution within a week, processing paperwork manually about as fast as it was occurring online before the attack.

Sheryl supervised the City's Office of Information Technology's progress in restoring the citywide IT system. This required her to work with the IT leadership team and outside consultants to develop and implement a method to re-authenticate and restore email to 10,000 users. Together they created Cyberstat, an accountability program to document and track the progress of the Ransomware recovery, which would remain in place even after systems were restored.

This defined process, and the others Sheryl helped develop and oversee in the aftermath of the attack, facilitated a systematic approach to restoring services, improving IT infrastructure, solving problems and increasing accountability. Anticipating that there would be challenges, Sheryl brought teams together to develop proactive solutions. For example, when the parking ticket system was restored, it was programmed to automatically charge individuals late fees even though they couldn't pay tickets online. Sheryl worked with IT, Finance and other departments to keep those assessments from occurring.

A Plan for the long-term

Sheryl oversaw continuous progress during this recovery effort. Manual systems, where needed, were active within two weeks of the attack, and it took about a month for the 10,000 system users to be reauthenticated and obtain access to their email. The primary billing and online payment systems and most external facing systems were restored within three months. Atlanta, hit by a similar attack a year earlier, took approximately six months to restore comparable services.

Looking ahead, Sheryl partnered with the City IT Director to launch a citywide IT Governance Committee focused on long-term improvement of the City's IT infrastructure and implementation of security

features to protect against future attacks. This included upgrading equipment and investing in cyber-security and Cloud-based systems. The improvements and progress became apparent during the COVID pandemic, which could have paralyzed Baltimore City's operations. Less than one year after the ransomware attack, Baltimore City IT was able to support remote work for all employees approved for it.