THE FUTURE OF securing large-scale, legacy infrastructure IN THE public sector

BIO

Cecil McMaster

Deputy Commissioner – CIO NYC Environmental Protection

Cecil McMaster is CIO and Deputy Commissioner at the New York City Department of Environmental Protection. He was re-appointed in July 2014. Cecil had previously served a total of 13 years at DEP, including as DEP's CIO for seven of those years, from 2004 to 2011. Two years prior to his most recent appointment at DEP, Cecil was the Director of Infrastructure at Web.com, as well as the New York City Consulting Practice Manager for Microsoft. With technology continually changing and playing an increasingly important part of how we do our work, Cecil's range of experience and in-depth knowledge of the agency helps DEP fulfill its mission.

DYNTEK
DYNAMIC TECHNOLOGY SOLUTIONS

Today, many large organizations, especially in the public sector, operate a mix of new technology hardware and legacy IT infrastructure. All of those legacy computer systems must be secure, and can range from physical buildings to the custom software that supports aging infrastructure. Often, these systems are left in place because it is too expensive to replace them, but they pose a challenge for IT security professionals, because the legacy infrastructure was built and installed when security was not the first priority.

The New York City Department of Environmental Protection (DEP) is one such organization with a mix of modern and legacy information technology infrastructure. The New York City DEP is responsible for supplying over one billion gallons of clean drinking water, collecting and treating wastewater, and reducing air, noise and hazardous materials pollution for approximately nine million New Yorkers.[1] This means the DEP operates a massive network of pipes, regulators, pumping stations, treatment facilities and reservoirs. The responsibility for securing the information technology infrastructure, thousands of computer servers and desktops, tablets, wireless phones, sensors, PLCs, data, and networks, falls on the DEP's Chief Information Officer, Cecil McMaster.

For all these assets, including legacy equipment, to be truly secure, McMaster says security must be built-in from the beginning. Unfortunately, it is simply not the case with most legacy deployments, which can include infrastructure created before even the Internet was commonplace. McMaster believes in a holistic approach to securing the assets already in place. In other words, creating a secure organization based on legacy assets is not just about locking down hardware and software vulnerable to cyber or physical security threats, it's about considering the security of the entire organization, including the habits of employees. This perspective has helped him focus on promoting security best practices and education – engaging with employees across the board – when many other organizations are scrambling to lock down every device.

> **"Before you go out and spend a lot of money on an expensive security program with lots of tools and security controls, you need to make sure you get the basics right."**

STEVE STRUTHERS
VICE PRESIDENT OF SECURITY
DYNTEK SERVICES, INC.

[1] Mission Statement of the New York City Department of Environmental Protection: http://www.nyc.gov/html/dep/html/about_dep/mission_statement.shtml

A high-level approach TO security education

For enterprise-size organizations in the public sector, IT assets are rarely consolidated in a single location. This creates a very complicated task for IT teams charged with protection. For the New York City DEP, McMaster says the sheer scale, variety, and locations of the assets makes protecting everything in an organization nearly impossible – if taken as a single unit. The solution is to divide and conquer, identifying the most valuable assets and focusing on securing them first. McMaster also says it's important to break up the responsibilities among team members, making it reasonable for them to secure assets in their area of responsibilities.

Organizing a targeted approach to security, such as the New York City DEP strategy, should be addressed prior to making large security purchases, explains Steve Struthers, DynTek's Vice President of Security.

"Before you go out and spend a lot of money on an expensive security program with lots of tools and security controls, you need to make sure you get the basics right," Struthers says. "Have the processes and resources to ensure those are all happening efficiently and effectively and then start looking at your gaps and how to populate those gaps from a security perspective."

Other enterprise organizations can learn from this best practices example set by New York City DEP by focusing on visibility – identifying all data and hardware and categorizing it by importance. Clear visibility not only helps organizations understand the full scope of their assets, but it also helps with data protection and overall security.

A high-level approach to security with a focus on visibility and education helps address some of the common issues with large departments such as a lack of budget and can also improve communication between IT, operations, and the business. Communication is important because it helps business understand and address the full scope of IT's needs, including security, by setting budgets accordingly.

> **"People think cyber security is drastically different than securing other things. I would challenge them. I think the tools are different but the attitudes need to be the same."**
>
> **CECIL McMASTER**
>
> CHIEF INFORMATION OFFICER AND DEPUTY COMMISSIONER, NEW YORK CITY DEPARTMENT OF ENVIRONMENTAL PROTECTION

Education AND changing workforce habits

McMaster describes the challenge that many legacy organizations are facing today: "…most of the industrial control systems – including sensors and other infrastructure we monitor – were not manufactured to be secure. That will be achieved with the next generation of devices."

For enterprise organizations and public sector departments that cannot afford to replace all their existing equipment right away, that next-generation of infrastructure with baked-in security is still on the horizon. But waiting for more secure hardware to be implemented is not an option. The answer to properly secure a large legacy organization is to start educating employees about security best practices.

It is not only organizations with large legacy infrastructures that can benefit from an education-first approach. "People think cyber security is drastically different than securing other things," McMaster says. "I would challenge them. I think the tools are different but the attitudes need to be the same."

The proper attitude is to be always considering security in your daily activities, whether at work or at home, but even McMaster admits this often involves changing long-established habits. For example, when asked for personal information on a form, questioning how and where the information will be stored. He says at the New York City DEP, security best practices are a daily conversation. "It's about making sure that people understand we need to start changing our behavior," he says.

> **"It's about making sure that people understand we need to start changing our behavior."**

CECIL McMASTER

CHIEF INFORMATION OFFICER AND DEPUTY COMMISSIONER, NEW YORK CITY DEPARTMENT OF ENVIRONMENTAL PROTECTION

Optimism FOR A more secure future

As sensors and devices evolve, McMaster hopes manufacturers will emphasize security in their design. He stresses to other CIOs to carefully consider their security investments because of the fast pace of change in the industry. "There's a lot of false premises," he says of organizations that think they can spend their way to complete security. Instead he believes in a targeted security spend and a focus on training.

Despite the challenges, McMaster remains optimistic. "I have hope for the future that we're going to be in a more secure world," he says. In fact, Struthers says government departments are beginning to tie in physical security with IT security more than ever.

"Security Information Events Management (SIEM) systems can be interconnected with threat data from physical security like cameras and doors and alerts," Struthers says. "Security teams can see if there's a correlation between a physical threat and a cyber threat."

While it's clear the current generation of security professionals faces an uphill battle with security education and changing habits, McMaster believes the next generation will be much more comfortable with digital security, with behavior to match.

COMPREHENSIVE SECURITY SOLUTIONS

Optimize your enterprise through the convergence of business and IT strategy with DynTek

Request a free consultation, contact DynTek at 1-877-297-3723

DYNTEK
DYNAMIC TECHNOLOGY SOLUTIONS