Tackling Cyber Security Challenges in an Obama World
Local Government Agency Culpeper County is Already Ahead of the Curve

From foreign policy to the automotive industry to healthcare, President Obama has rapidly and systematically begun tackling the nation's biggest problem areas in his first 100 days in office. High up on this list is cyber security, a top priority for Obama who stresses the importance of making the nation's digital infrastructure a secure, national asset. In a recent speech on the topic, Obama honed in on the importance of local, state and federal government agencies to create strategies that will "deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage."

What President Obama has pointed out is not only a problem for homeland security, but a daily headache for local government agencies -- from 911 call centers, to the county attorney's office, to local sheriffs' offices, all of which are subject to network vulnerabilities and cyber attacks. Although many are still unaware even of the concerns that are facing them, some have recognized the challenges and have begun to innovate in their responses. The steps that they are taking to adopt mission-critical security technologies such as network access control – and the results they have demonstrated – are a promising sign ... for the small local government as well as the world's most powerful country.

Identifying Holes and Gaining Control: The Case of Culpeper County
The Culpeper County Government in Virginia is a local county body that supports the government offices for a population of about 43,000 people. Systems Administrators Todd Frazier and Anthony Soucek are responsible for the IT infrastructure for over 500 users, nine hardwired offices and another five remote offices. This network includes both desktop and mobile users that span the county agencies including the 911 Emergency Center, EMS, Airport and Sheriff's office.

Like many local government bodies, Culpeper County's network is spread across a variety of rented historical buildings and older buildings where they share space with other government agencies and private businesses. Many local government agencies share space with other offices. Prior to shoring up network security, it was possible for any Culpeper County government employee to plug into random wall jack and unknowingly create a bridge with the network of another organization. This was causing significant vulnerability and also problems with network performance.

"Culpeper County has network infrastructure and users spread across multiple buildings in the county of varying levels of physical security. This provides a variety of network security challenges," said Anthony Soucek, Network Administrator of Culpeper County. We needed the ability to see any and every device on the network, their interconnections to other network devices, and the ability to control how that device is being used − in real time."

Changes to the Freedom of Information Act (FOIA) also required that Culpeper County evolve its approach to network security. Recent amendments now require local governments such as Culpeper County to keep public records on all correspondence to and from any government office including email, chat sessions and peer-to-peer communications. This is a huge challenge to manage, when one cannot see or control the use of non-sanctioned communications such as instant messaging or POP email accounts.

The Culpeper County team quickly realized that they did not have sufficient visibility as to what was going on across their network and little ability to control or enforce IT policy. The need for a network access control system was clear.

The Solution
After a looking at a variety of options including wireless intrusion prevention and other NAC solutions from Cisco and others, Frazier and Soucek decided to move forward with CounterACT, a network control platform that promised to provide both visibility and control of devices across the Culpeper County network. CounterACT provided the network security team with the ability to shore up its network perimeter, adhere to FOIA compliance regulations and protect critical government agencies from malware, viruses and cyber threats. Part of the reason for this decision was that CounterACT was the only solution that didn't require rip-and-replacing the existing infrastructure, and provided bolt-on intelligence that helped raise the IQ of Culpeper's intelligent switch.

The Results
Using CounterACT, Culpeper County was able to identify points of vulnerability and shore up the perimeter of their network. Furthermore, CounterACT was able to detect and disable rogue wireless access points deployed across the county, effectively eliminating an additional vulnerability in the network. Culpeper County is using CounterACT alongside antivirus protection from WatchGuard, and has found CounterACT helps to ensure the AV system is "always on".

"Working with our existing infrastructure, ForeScout has provided Culpeper County with a single powerful device to shore up our network perimeter, adhere to FOIA compliance regulations and protect critical government agencies from malware, viruses and cyber threats ... 24/7/365, " said Todd Frazier.

CounterACT also enables Culpeper County to restrict the use of instant messaging, SMS chat and disable peer-to-peer (P2P) file-sharing programs so that accurate records can be kept and Culpeper can ensure FOIA compliance.

Impact
"Using CounterACT we have gained the ability to see any and every device on the network, their interconnections to other network devices, and the ability to control how that device is being used - in real time," said Anthony Soucek. In the future, the Culpeper County team may use CounterACT for locking down USBs and as a supplement to group policy management.

With ForeScout as the sledgehammer in the back office enabling them to stamp out any threat which hits their network, Culpeper County is confident that they are prepared to tackle the threats that Obama warned against in his recent speech. "This is our first line of response," said Frazier.

Culpeper County Contact:
Todd Fraizer
Systems Administrator
Culpeper County Government
Email: TFrazier@CULPEPERCOUNTY.GOV
Tel: (540) 727-3416
http://web.culpepercounty.gov/CountyInformation/AbouttheCounty.aspx