PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

MICHAEL DENT
CISO, FAIRFAX COUNTY, VIRGINIA GOVERNMENT

LOCATION: Fairfax County, VA

EMPLOYEES: 12,000

ANNUAL REVENUE: $3.8 Billion

VETERAN CISO CREATES PROGRAM TRANSFORMATION

Michael Dent has held the CISO position at Fairfax County, Virginia for fifteen years, making him a veteran and far outpacing the average tenure of most CISOs. He offers a historical perspective on the position, a long track record of success and an established reputation among the County employees.

Dent describes his start at Fairfax County, “In 2002 many places were not concerned about security incidents. The fact that Fairfax County leadership was hiring a CISO put them ahead of the curve. However, there were a lot of questions that did not yet have answers. At the time, the County did not have a documented IT Security Policy, and had no clear separation between IT and information security. Again, this was typical of County governments across the United States.”

Through Dent’s tenure, security awareness became one of his biggest priorities. Dent initiated the County’s annual security awareness day for employees. During this day, employees learn and develop cyber security tactics applicable to their personal and professional lives. The speakers and break-out sessions cover topics such as protecting children online, using IoT safely, and best practices for secure banking. “Employees love the day. We provide them very useful information in a high energy environment, and we make it fun,” says Dent. “While this is a service to help them in their personal lives, it improves the County’s overall security posture. As a result of these sessions our incidents have decreased, employees are more knowledgeable about security, and they are more willing to work with me and my team to create secure processes.”

The security awareness training helped Dent integrate himself with the staff of the County agencies, as they adjusted to working with a Security Officer for the first time. Dent says, “At first, the agencies did not understand why security was needed, or why we needed to document our processes. Some worried that my goal was to prevent or delay their IT initiatives as most implementations would be delayed when my office was included initially.” Today, after years of training, security understanding in the County is much higher and the working relationship between Dent’s team and County employees is strong.

Dent and his staff worked hard to rid themselves of the reputation as the “no” people. Dent comments, “Now,

> **The Next Generation of Security Experts**
>
> I had the honor and privilege of speaking with 30 High School students two weeks ago at a summer outreach program. I spoke about a variety of career pathways in cybersecurity and answered many questions around what happens in a cyber security organization and what a CISO is expected to know and do. This program is a partnership between Fairfax County Public Schools and Systemic Solutions (NOVA's college-wide STEM education outreach program).

employees know security has to be the first call at the beginning of the project. They realize this makes it easier for us to get it right from the beginning and build out a technology or process that works for them, and is secure."

DILIGENCE IS REQUIRED TO MAINTAIN A LEADERSHIP POSITION

Fairfax County has a reputation as one of the best counties in the United States, both in terms of size and government services, especially information technology and cyber security. Employees work hard to provide services to citizens quickly and efficiently. Dent's role is to make sure these services are delivered securely, with protections in place for citizen and employee data.

The County is comprised of more than 50 agencies, and the majority have multiple types of businesses within the agencies, including public safety, parks and recreation, and libraries, among others. "We are a centralized IT security team, so security for each agency falls under me and my team," says Dent.

"The simple fact is we are not going to maintain our image as the top county in the country if our data gets compromised. Our leadership has led the way through investments in the Cyber Security Program and has ensured that cyber security stays at the top of their lists of concerns. We can never say 'don't worry about it' to the board. In my option, all of the recent (within the last 10 years) major breaches we have heard about in the news were caused by negligence amongst leadership up and down the latter." Dent points out, "We need to be diligent and remain so to be successful."

Dent's two main goals are to protect data and privacy, and to educate employees and keep leadership informed to increase security awareness. "Our sole mission is to allow business to be conducted in a secure manner. I tell my team to never say 'no.' Instead we focus on giving employees and agencies multiple secure options to accomplish their goals. Therefore, we need to be involved from the beginning with internal IT folks and agency teams."

Fairfax County's environment is large and distributed across agencies, and Dent is realistic about what his team may uncover in advance. To keep threats at bay, they conduct yearly and quarterly vulnerability and risk assessments. He says, "I used to think I knew everything on the network. Now I realize that's not feasible. The assessment identifies the risks and unknowns that occur between assessments, then I have to take action to bring it into compliance."

Dent works closely with the Senior IT Steering Committee, comprised of the County executive and his deputies, and includes the Director/CTO and Senior IT leadership, to identify and report on critical cyber security programs. Dent shares, "At those meetings we talk about current programs, and I do a status review of the security program. We review multiple facets of cyber and cyber risk along with any mitigation strategies we may need to take to ensure we have no compromises."

As most in the IT Industry, the County deals with the challenges of legacy systems that remain critical to agency operations but are difficult to secure. "We need to work to get those agencies solutions updated and/or upgraded with minimal down time that would affect services to our citizens. It is a delicate balance to make sure those systems can serve their purpose yet not be compromised. These legacy systems require additional measures to mitigate and create exceptions to IT Security Policy eventually becoming burdensome to IT and Security staff.."

Dent suggests these legacy systems are an example of how leadership in County agencies and IT should partner with the security team to improve the County's overall security posture. "Today, business decisions need to be made that factor in both security and efficiency," says Dent.