EXECUTIVE VIEWPOINT
A Conversation with
DOMINIC CUSSATT

DOMINIC CUSSATT
CISO, Department of Veterans Affairs

The chief information security officer at the Department of Veterans Affairs talks about how VA is creating a resilient cybersecurity ecosystem

How do you prioritize where to focus VA's cybersecurity resources?

In alignment with Executive Order 13800, VA established the Enterprise Cybersecurity Strategy Program (ECSP), which uses an enterprise-level approach to determine risk and prioritize programs and resources. The ECSP creates a proactive approach to manage cyber risk at VA and institute a transparent program that spans from government statutory requirements to the information system level.

The ECSP is a holistic program that enables VA to identify risks at the earliest point possible and make prioritized, defensible decisions related to cybersecurity activities, providing the department with the means to create a resilient cybersecurity ecosystem.

How do you avoid complacency and stay ahead of threats in today's ever-changing cyber landscape?

At the enterprise level, VA continuously monitors the threat landscape and then infuses the latest and greatest technologies into our environment to mitigate threats and stay one step ahead of the adversary. We focus on being proactive, not reactive.

We also stay ahead of threats by sharing information and lessons learned with other agencies. From this perspective, VA is persistent in its approach to pursue state-of-the-art technologies — such as advanced behavioral analytics, endpoint detection, and security information and event management — to provide pervasive and ubiquitous awareness of our posture in real time.

We recently created the Office of Cybersecurity Workforce Management to address the critical need of acquiring, developing and retaining the skills of our cybersecurity workforce. Advances in technology may lead to more automation of routine system monitoring, but VA will always need talented cybersecurity personnel to perform high-level threat analysis and keep our systems safe.

If you were to write a guidebook for other agencies, what lessons would you include?

When VA began its modernization, we struggled to bring the right people together to address cybersecurity needs. We have learned how to correctly identify and engage the right stakeholders as we modernize our cyber capabilities and will use the team we now have in place to shape our policy and strategy moving forward.

One lesson learned is our employees can be a weak link when they unknowingly click on malicious links or browse malicious websites and consequently download malware. In a guidebook for other agencies, it is important to convey that traditional manual approaches to cyber defense are no longer sufficient, so automation is critical in incident response.

There are myriad tools from different vendors that can be deployed, but there is no silver bullet, and tools that do not communicate or integrate easily can add complexity and slow incident response. We should strive for predictive networks that can automatically detect and isolate new attacks, then self-heal to prevent similar future attacks.

Finally, agencies need to work together and combine our strengths to defeat adversaries.

This interview continues at Carahsoft.com/innovation/cussatt-VA