CyberPro

November 2010

Keeping Cyberspace Professionals Informed

Senior Leader Perspective: Mark Weatherford

NSCI's Lindsay Trimble recently interviewed Mark Weatherford, vice president and chief security officer of the North American Electric Reliability Corporation (NERC). In this role, Weatherford ensures comprehensive threat information and evaluation of risk on cybersecurity is available to NERC stakeholders and serves as the single point of contact for the industry and government stakeholders seeking to communicate with NERC on cyber and infrastructure security matters. Prior to joining NERC in July 2010, Weatherford was appointed by Gov. Arnold Schwarzenegger as California's first chief information security officer after his success in this position for Colorado. He has also worked for Raytheon Company and is a former U.S. Navy Cryptologic Officer. Weatherford was awarded SC Magazine's *prestigious "CSO of the Year" award for 2010.*

NSCI: You've been with NERC since July. How has your experience with the California and Colorado state governments and with the U.S. Navy helped you transition to your new position?

WEATHERFORD: Like most people's careers, each new job has added something to my professional quiver of arrows. In the Navy, it was still the early days of what we now call cybersecurity and I remember the exact moment when I was introduced to this new thing called Mosaic and the World Wide Web. I was in graduate school at the time and didn't know then how the Web would change the world, but I knew it was pretty cool.

In Colorado and California, I obviously learned more about working in a political environment, but from a professional perspective, I learned to be more collaborative. In both of my state jobs, I was required to work with such a variety of different organizations with such a diversity of mission requirements that it was important to understand risk and that one size doesn't fit everyone. Because there are so many ways to achieve security goals, I learned to keep the end in mind and the path to get there was less important than achieving overall good security in an organization.

NSCI: Are there any major achievements you'd like to highlight from your first few months?

WEATHERFORD: Stuxnet was first discovered in June and then widely reported the week of July 12. I started at NERC July 19 and we issued the first Industry Advisory on July 22. That was a busy first week. An early priority was development of the Electricity Sub-Sector Coordinating Council's (ESCC) "Critical Infrastructure Strategic Roadmap" and the "Critical Infrastructure Protection Coordinated Action Plan," which we have completed and already begun establishing work groups. We were also active participants in the Department of Homeland Security-sponsored Cyber Storm

III exercise. Finally, and following a couple of years of technical research, we released the Aurora Recommendation to industry in September.

NSCI: How has the increase in cyber threats changed the way NERC protects the U.S. electrical grid?

WEATHERFORD: The NERC Critical Infrastructure organization didn't even exist a couple of years ago, so that says a lot about NERC's response to the cybersecurity issue. NERC and the electric industry have always been responsive to reliability issues, but cybersecurity requires a more dynamic way of thinking because the threats are different. Because of the interconnected nature of the grid, NERC has to think in more enterprise, or industry-wide, terms about the impact of cybersecurity threats. That requires a bit of an evolution in the culture.

NSCI: You mentioned that NERC recently participated in the Homeland Security Department's Cyber Storm III attack simulation. What are a few of the lessons learned for your organization in this exercise?

WEATHERFORD: Communication. Communication. Communication. The biggest lesson learned for us is that we need to fine-tune our communications protocols. Knowing who to contact and how to get in touch with them is always important, but during an emergency, it's critical. In our case, we have to manage flows of communications to both our large stakeholder community and with the government. We also learned that a major cyber-related event requires a true "all-hands on deck" mentality because so many areas of expertise are required to understand the various response options and so much is happening with such a high volume of information that it can be overwhelming.

NSCI: You recently said in an interview[1] that the Stuxnet attacks were a warning. NERC used this warning to create a Tiger Team to respond to serious malware attacks in the future. What progress has this team made so far?

WEATHERFORD: The Tiger Team was something of a loose and informal cabal of trusted security experts from around North America who all threw a shoulder-to-the-wheel of researching and understanding Stuxnet and how it threatened the bulk electric system. The Tiger Team was largely responsible for the technical background leading to the NERC Industry Recommendation on Stuxnet.

NSCI: Along with needing better defense procedures to respond to attacks on the electrical grid, you've also emphasized the need for more secure software. What can software-development companies do to ensure secure and reliable products?

WEATHERFORD: There's an easy answer and a not-so-easy answer. The easy answer is to hire good developers who understand how to write secure code and pay to keep their skills sharp. Understanding good security software development needs to become part of the DNA.

[1] http://threatpost.com/en_us/blogs/more-secure-software-needed-utilities-nerc-cso-says-100710

The second and harder answer deals with the supply chain for technology products. It's almost impossible to know where every component is manufactured these days and who wrote all the pieces of code, but for some important and strategic pieces of the nation's critical infrastructure, that might be critical information to have.

NSCI: You played a critical role in writing new cybersecurity legislation at the state level. What federal cyber-related legislation do you think is needed at this time? Does NERC have a role to play?

WEATHERFORD: Most of the legislation I was involved with at the state level was to solve gaps in state government. On the other hand, most cybersecurity legislation at the federal level targets the private sector, which requires you to think about other factors and unintended consequences. There are a number of pieces of legislation at different stages of the legislative process right now and we are staying involved as much as necessary.

NSCI: What processes and/or forums are in place to assist NERC in collaborating with government agencies and industry organizations?

WEATHERFORD: There are far too many different organizations, boards, commissions, councils and work groups to mention in detail, but for cybersecurity-specific issues in the electric sector, the Industrial Control System Joint Working Group (ICSJWG), the National Association of Information Sharing and Analysis Centers (ISACs), the Critical Infrastructure Partnership Advisory Council (CIPAC), US-CERT and ICS-CERT are very important. We also have relationships with organizations within the Department of Energy and the DOE laboratories, Department of Homeland Security, Department of Defense, National Institute of Standards and Technology (NIST) and with our Canadian partners, where we work together and share information on a variety of cybersecurity-related issues.

Thank you for taking the time to be interviewed.