Cyber resilience is a national problem

Jan Kallberg, University of Texas at Dallas
The biggest challenge for American cyber resilience right now is to disseminate knowledge within the nation. The federal sector, the financial institutions, and the defense complex are on top of the game to a high degree.

The asymmetric way cyber conflicts are and will be fought exposes the whole government structure of a country. The sheer numbers entities that form local government are staggering – just as examples I mention that in the US there are 6,000 counties, 15,000 police departments, and 50,000 public utilities.

The immediate reaction is natural – then let us take the federal knowledge and ensure that local government become up to par with their cyber security and there are several efforts to do so. The National Science Foundation supports cyber education where research institutions spread their cyber knowledge to local communities, the FBI-sponsored INFRAGARD public-private partnership, and online both FEMA, CERT, and other public entities provides excellent information and resources.

My concern is that the effort is speaking to those who already care. If I work in a county in rural America as an IT-manager it is less likely that my county judge and county executives would put pressure on me to kick up cyber security to the next level. Why? Local politics tend to follow traditional routes addressing local matters and a full-blown cyber-attack from a foreign nation is not business as usual. How do we fix this? The awareness that cyber security is a major challenge and might require more resources allocated is likely to be known to the IT-staff, but how do they sell it to the next level? What will convince a county executive that cyber security needs more money from a cash-strapped county budget?

I have been thinking down the lines that the federal government should be more active contacting local government but then I remember Ronald Reagan’s quote: The most terrifying words in the English language are: I'm from the government and I'm here to help." The key question – would local government be willing to cooperate with DHS, NSA, DOJ, or who gets the job to disseminate knowledge?

My take is that to be able to strengthen American cyber resiliency local government needs to play an active role and they vehicle to disseminate knowledge, support them as subject matter experts, and give guidance it has to come from an organization that they already trust. Local people trust local people – that is almost a natural law.

I have arrived at the conclusion that American cyber resilience would require that the states are the active vehicle to support local government cyber security. We can just run a test. You are a plant manager in McAlister, Oklahoma. One person shows up: “My name is John Doe and I am from the NSA, we would like to help you with cyber security” and another “My name is John Doe and I am from Oklahoma Air National Guard, on behalf of the State of Oklahoma, we would like to help you with cyber security” – who will you pick?

To ensure American national cyber resilience a top down approach all the way from Washington D.C. is not a workable model. The states are likely to be the most efficient way to disseminate knowledge, support and ensure cyber security at the local level.

Cyber resilience is a national problem