**Meeting Notes - NeoSystems Town Hall Meeting – July 14, 2021**

***Attendees:***

***Mr. Ed Bassett, CISO, NeoSystems Corporation***

*Mr. Kevin Garrison, staff member at the Institute for Defense Analyses (IDA)*

Kevin Garrison is a research staff member at the Institute for Defense Analyses (IDA). He previously worked as the Chief of Analytics for the DOD CIO, as well as holding several other senior analyst positions within the DOD. This all builds upon a career as an Army infantry officer.

Ed Bassett opened the discussion on the topic of zero trust, its evolution and its promise for the future - specifically - how it might intersect with some of the CMMC and other compliance preparations.

Kevin Garrison explained that the principal difference is that the perimeter model, which we've employed for years, includes a firewall, with another wall, and another wall, and security layers on top of security layers. There’s a theory that each layer adds (depending on what layer of the network you're at) adds another measure of security. The zero-trust model basically says you start with certain core principles as least trust and you only selectively give people access based on a certain set of rules.

“It's actually a different approach, which is more granular,” explains Garrison. “As a guy at work put it, instead of wrapping all your candy up in bulk, you individually wrap all the candies. That's a good way to think about it. So, every application running on the network must be enabled to do the least privilege and only give people access if they meet certain conditions. It's hard, very hard to do. So that's the big difference. There's a tremendous installed base of perimeter security vendors that will sell you firewalls that do X, Y, and Z. And the terminology keeps changing all the time and you have 20 sets of security stuff running on your network, but it's still designed to run on a model that the castle wall and the interior wall and the crown jewels are in the special vault. That's that model.”

Garrison adds that zero trust says you must assume every communication is from a bad actor and you would only let them in and communicate with them if they met your conditions to be trusted.

In a sense, he says, zero trust is a misnomer. It sometimes obfuscates as much as clarifies. And that's the basic difference between the two. “The core element of a zero-trust architecture is that you must know the identity of everything,” he says. “Every device connected to the network. That's an inherently hard problem that people struggle with all the time because devices get turned on, get turned off, get lost, get stolen. Or with an IoT device, they don't have any maybe security number or Mac ID or anything to identify exactly what it is. So that's a hard problem. You must have that stuff up to date. You must have the people part of it. The identity of people must be managed, which you can do with a credential or assert or some form of that. In the government, you have a common access card, which has a chip, and that's how we identify you. There are some roots of trust that says some identity system is issued you this credential that says you're Kevin Garrison. And if you put your magic code number in to prove that you're Kevin Garrison. We will trust that you are Kevin Garrison.”

Garrison then went on to explain two-factor authentication and other methodologies to identify the person on the network. He explained that a third component is you must have a rules engine that says, “if this is Kevin Garrison and it's Thursday, and he's in his office at the building, and I know where it is connected to that network, I will allow him access to system X.”

System X must know that set of rules. “You can do some of that centrally, but it really is a decentralized security model where each application implements zero trust. So, it's hard, because then you want to get scaled behavior or people are doing it the right way for every application across the network. So, it's very hard.”

Kevin Garrison mentioned that a potential shortcoming with CMMC certification is that it’s a certification based on a firm’s satisfaction of control requirements at a point in time. Then the same iteration is repeated in three years. There are possibly some shortcomings to that in that the actions may not be maintained and continuous. Ed Bassett then added that the gist is to achieve a maturity level that is more permanent. But Kevin Garrison replied that often the championing of requirements relies on continuity. If a key person leaves the company, much of the corporate knowledge could be lost and the maturity level may also be lost.

Ed Bassett then discussed CMMC and its relation to cloud adoption. It is a way to transfer some risk and the cloud providers are coming to the table with solutions that take care of a lot of the compliance requirements for them. However, they are moving now to these sorts of cloud only models, where the notion of perimeter defense starts to get shaky anyway. For some companies, a corporate network is just a collection of home office internet connections, and that enables remote workers to get to some cloud-based resources. Bassett asks how does zero trust as an architectural approach overlay onto that sort of architecture where a contractor leans on the cloud provider? How does zero trust intersect with that?

"Early on, there was a big flee to the cloud," says Garrison. “Then the big companies said, wait a minute, I got some stuff I don't want out in the cloud. I want to keep it in my safe deposit box in my house. Right? Because it's too sensitive. And I know the cloud people say they got it all secure, but I'm not taking that chance. Or it's my core financial application and I'm not moving that to the cloud. I'm keeping that in house. Well, then you got a problem of some of your data's over here and some of your data is in house, and now you've increased the complexity of your IT environment and your cybersecurity environment because you've got the stuff in house that you must secure and protect, and you must know enough about how the cloud vendor is doing it. In the cloud, it depends on whether you're doing software as a service, infrastructure as a service, platform as a service. And then your security responsibilities vary significantly, depending on what service model you're using to subscribe to the cloud. And that means you got to have people who understand that stuff.”

The conversation wound down with further discussion of cloud providers, security, ransomware and other related topics.