**Meeting Notes - NeoSystems Town Hall Meeting – June 30 2021**

***Attendees:***

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

***Mr. Chris Hughes, Co-founder and CISO of Aquia***

Chris Hughes previously worked as a principal security engineer at DevSecOps Innovator Rise 8. He's also an adjunct professor teaching courses on cloud security and is on the advisory boards of cyber resilience firm, Accurics, Inc. and audit management vendor, ByteChek. Chris Hughes previously worked for the federal government with FedRAMP jab, the Navy, and the Air Force.

Ed Bassett stated that we’ve watched and participated in CMMC as it is unfolded. One thing, he notes, that's been dominant is that it's driving a lot of IT transformation and cloud adoption. He says people are finding out that just overlaying security practices onto an existing IT footprint isn't always workable or the best solution. He asks why is the cloud such an important part of CMMC for most of us?

**C**hris Hughes says the cloud is an incredibly important topic for CMMC for a variety of reasons. Organizations of all shapes and sizes are increasing their adoption of cloud as part of their overall IT and business strategy. Larger organizations are adopting it to maximize the use of emerging technologies like artificial intelligence and machine learning for security and other purposes - data analytics and things. But small and medium sized businesses (SMBs) are also taking advantage of cloud to use Mac services, especially in cases where they don't have core competencies around some of the things they're consuming as they're leaning into the cloud service provider to make up some of those gaps.

“That said, there's also a lot of misperceptions on the topic of cloud and whether they're secure,” says Hughes. “I know this is something we're going to get into a bit more, but the reality is that cloud within government is basically assessed by an independent third parties against the same control, security control baselines that government systems are. These are the same security control baselines that are used within DoD and within the federal civilian community. That said, the overwhelming majority of cloud data breaches occur on the customer side of the shared responsibility model - which is another topic I know we're going to dive into as well. I think it's just a matter of customers understanding the shared responsibility model and how that dictates what the cloud service provider handles and what they as a cloud consumer are responsible for. It's something that's misunderstood by many. But it's such a fundamental topic. I know we're going to unpack that a bit.”

Circling back to CMMC, Hughes thinks that the cloud is an important part of CMMC, because it's being utilized by many vendors across the entire ecosystem, both large, prime companies, and small SMB, subcontractors. Not just one [cloud service provider] CSP either.

“They're using many as a service type offering, whether it's infrastructure as a service, platform as a service, and software as a service, a myriad of those basically,” says Hughes. “Those vendors are seeking CMMC certifications. They need to ensure that the services they're using based on DFARS and things comply with FedRAMP moderate, for example, or equivalent standards and that they understand what controls are met by the CSP, what controls are left to them as a cloud consumer, and then what controls are shared between those parties.”

Hughes adds that it's not only that, but it's also a topic [the cloud] that needs to be understood by other parties in the mix too. “We have three PAOs who are going to assess systems seeking certification," he says. “Then we also have registered practitioners (RP) who may be helping you prepare for certification. All these parties need to have a solid understanding of cloud going into this CMMC situation, so they can all perform their roles appropriately.”

Ed Bassett then brought up cloud providers, who, by and large, he says are doing a good job of security, and it's a great way to shift some of the compliance burden over to those CSPs. He thinks many people underestimate what's left for them to do in that shared responsibility model.

" I've seen some reports of large, scary numbers of cloud-based servers out there that are vulnerable and primarily because it was misconfigured,” says Bassett. “I think sometimes it gets lumped back on the cloud service provider, but it's really on the consumer who set that up and made those choices. Typically, they're self-managing the cloud environment and they may not have strong security expertise in-house. Tell us a little bit about infrastructure as code, those techniques, how they can help improve the security of cloud deployments, specifically for those kinds of companies that may, they may not have the extensive infrastructure management expertise, that's why they reached to the cloud in the first place.

Chris Hughes agrees with this assessment. “You're spot on with a lot of the things you mentioned,” says Hughes. “As I previously mentioned, there's a lot of benefit of shifting some of that responsibility to the CSP and inheriting some controls in that shared responsibility model, especially areas that are outside of your core competencies. “

Chris Hughes adds that this is true for SMBs. “They don't have robust cybersecurity and IT staff,” he says. “They definitely, in a lot of cases, don't have staff with skills around DevOps and infrastructure as code and things. Part of this is also since as organizations increasingly adopt and migrate to cloud, security, unfortunately, is an afterthought, if it's even a thought at all. That's always traditionally been the case with security in many cases, it's typically bolted on versus baked in, as we've heard so many times.”

Organizations, in some cases, don't invest in upscaling their workforce or hiring necessary skillsets, or even partnering with [managed service providers] MSPs or other organizations that have the skills to help them through a secure cloud migration and adoption journey.

“On the infrastructure as code front, I can definitely help on this front for a number of reasons," says Hughes. “Some of these benefits include expediting the migration to cloud environments. Now, if you start with utilizing pre-existing templates from cloud service providers or others, they can help you quickly get spun up into those environments, quickly provision the architecture that you need to utilize these cloud services, and they're aligned often with the compliance frameworks such as NIST853 and 80171 and CMMC, that you need to comply with as an organization. On the infrastructure as code front, you have vendor offerings from AWS and Azure. On AWS, you have AWS cloud formation for example, which is our native infrastructure as code format.”

Hughes explains that Azure has what it called blueprints. “It is the same thing, but from Azure - unless you use infrastructure as code to quickly spin up infrastructure in the cloud environment,” he says. “Then there's, of course, the leading vendor agnostic approach, which works across multiple cloud service providers, which is Terraform, for example. All these help in the case that they're already aligned with the compliance frameworks that you're seeking to use, says Hughes, and it helps speed up that activity, especially if you don't have the expertise on how to quickly and securely and, most importantly, set up cloud environments. “

The discussion wound down with more conversation about the cloud, cloud providers, Solar Winds and other topics.