Q&A

With Shivaji Sengupta

Member and CEO of MAGNUS Management Group LLC and founder and CEO of NXTKey Corporation. He also is an adjunct professor of cybersecurity at Delaware State University.

How are cybersecurity and innovation intersecting, and is it a positive or negative development?

As technology advances, so does the realm for hacking. When cloud computing and storage was released, hackers rejoiced as more valuable details were accessible on the Internet, making their "jobs" easier. All these recent technology innovations have led to the considerable increase in the attack surface in a relatively short period of time and provided new gateways for hackers to exploit. This business of cybersecurity is all about continuous innovations both on the defensive and offensive side to ensure our information assets continue to be protected.

What must a small business do to implement effective cybersecurity, especially if it is serving as a sub to a large prime?

Attackers are benefiting from every vulnerability, and we can all agree that 2020 brought many to our table. The big challenge for small businesses in this environment is constant evaluation of security posture by implementing NIST 800 171 requirements, locking down corporate information assets, instituting compartmentalized secure storage solutions, and ensuring end-using computing and connectivity is secure by ensuring team members segregate personal/corporate usage, continuous cybersecurity awareness training, and most importantly, securing any flow of data down from the prime contractor.

With the supply chain currently under siege, is its cybersecurity going to fall by the wayside?

The supply chain has received a lot of attention the past year with newsworthy breaches across critical infrastructure, automotive and software companies, to name a few. President Biden's executive orders on America's Supply Chains dated February 24, 2021, and Improving the Nation's Cybersecurity dated May 12, 2021, put our federal agencies on notice to make this a priority. The supply chain is only truly secure when all entities throughout it carry out effective and coordinated security measures to ensure the integrity of supply chain data. Because of that, the term supply chain is fast becoming synonymous with cybersecurity in the federal marketplace.

What is the future of cybersecurity?

We are experiencing the peak of cybersecurity technological disruption, and this is expected to last long into the future. The next decade is going to bring about cybersecurity advances in artificial intelligence, virtual reality, cloud computing, strategic automation, the Internet of things, robotic process and blockchain, among many. Some of the immediate advances will be made in the areas of unsupervised machine learning, artificial intelligence and process automation to find patterns and detect anomalies and then spot potential attack attempts. The future of cybersecurity will be all about unsupervised automation to detect and mitigate cyber threats across our networks and environment.

What do you think is the next great information technology trend?

The next big technology trend will be a solution that enables innovative tools and technologies to be more efficient and provide faster computing for the ever-evolving world of cybersecurity. This trend will be all about quantum computing, which will perform tasks quicker and more efficiently than the current generation of computing. Quantum computing will take machine learning, process automation and artificial intelligence to new heights, thereby significantly impacting cybersecurity functions. Quantum computing will dramatically change the face of innovation and will be the next big leap in the evolution of information technology.

To share or comment on this article go to http://url.afcea.org/February22