ceocfointerviews.com

Issue: September 12, 2016

CEOCFO Magazine

Supply Chain Cyber Security Solution for Critical Infrastructure and Enterprises

Yossi Appleboum
Co-Founder & Co-CEO

Sepio Systems
www.sepio.systems

Contact:
Mrs. Allyson Ruscitella
(571) 230-0157
media@sepio.systems

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

"The supply chain is a big unknown. When you buy hardware, you have no ability to know how many hands there were between the vendor and you. This unknown is actually full of threats. It starts with the 3rd party sub-contractors to the vendors; the ones that manufacture the hardware. It goes to the distribution channels and then to the store or the courier that delivers it to your organization."- Yossi Appleboum

CEOCFO: ***Mr. Appleboum, what is the concept behind Sepio Systems?***
Mr. Appleboum: Saying "Cyber Security" is speaking about so many problems under one umbrella. There are more than 600 companies, just in Israel, which is known as a cyber country. In addition, there are couple of thousands cyber security companies in the US. However, Sepio Systems is dealing with something that is different than most, if not all of these other companies, which is the hardware supply chain that is used as a new attack vector of organizations, enterprises and governments critical infrastructures. What Sepio is actually doing is helping customers to recognize that while securing most of their entries, internet connections, and file handling processes, they actually pushed the criminals, to find new attack vectors, and one of them is the hardware supply chain. Therefore, this is what Sepio Systems is focused on.

CEOCFO: ***What are some of the challenges unique to the supply chain in terms of security?***
Mr. Appleboum: The supply chain is a big unknown. When you buy hardware, you have no ability to know how many hands there were between the vendor and you. This unknown is actually full of threats. It starts with the 3rd party sub-contractors to the vendors; the ones that manufacture the hardware. It goes to the distribution channels and then to the store or the courier that delivers it to your organization. All of these are unknowns, which makes it a very scary world, because it is being used in order to harm your organization. In each one of these hands I can harm you by switching a keyboard, for example, or planting something into it, and the keyboard is just a simple example. The same is true of everything an organization purchases, and the criminal uses this to attach your organization.

CEOCFO: ***Would you tell us what you have developed? What is your approach to keeping organizations and their supply chain safe from cyber attacks?***
Mr. Appleboum: A common practice to deal with a supply chain was created and developed by the government. The idea was to clean everything before it was installed in a facility. However, that was proven not to be working. Our approach is different. We ask organizations to consider that an attack is in place, then we need to take the poison out of the attack. Just like the keyboard example, we just were informed recently of malicious barcode scanners that are used in warehouses or selling points. All of these are used in order to attack you, and what we say is that we will take the poison out, so that you can allow the device to keep doing what it should do, and the other influences will be isolated before they can attack you.

CEOCFO: ***How do you take out the poison and isolate those influences? What is your solution?***
Mr. Appleboum: We have a simple to install and use appliance that isolates between what we call the exposed side of your infrastructure and trusted side. Let's assume that your data center is the trusted side, and someone is coming in to install new hardware, our appliance is sitting in-between forever, making sure the data is first going in the right direction. It starts from the keystrokes and up to the keyboard. If someone is actually hiding a cellular modem inside of your keyboard

or other devices, which can really happen, as they are not fiction stories, what Sepio does is stops the cellular modem from getting any data. Data should get in and not out. This is the first thing. The second thing is that we actually monitor the data that gets in to make sure t it is valid. With the keyboard for example, the keystrokes are being done by a human being. In addition, we are using similar methods like “Captcha” in website to make sure a human being sits behind the keyboard you installed and is not running some malicious trick, trying to look like a human being.

CEOCFO: ***Security is important, but many people see an overload of information and approaches. How do you garner interest for a totally different approach? Does it make it easier as it is a new concept?***
Mr. Appleboum: You are right. Most organizations are exhausted hearing every second day about new solutions and new versions, all coming from a long list of vendors, but eventually they will have to reach a balance between their budgets and the threats. There is no one way to solve that problem. Our approach is a bit different in the way we go to the market. We are actually trying to convince and have been successful in our efforts, in that what they are doing is great and they should keep doing that in a way that should keep them secured. However, they need to address something that as long as they do something great, they are creating a new problem. In your home, if you have a burglar alarm, and you put many sensors and gates around your home, eventually you will leave one door open in the back and the thief will go through that door. That is an analogy. Organizations have done such a great job with cyber security that the criminals had to find new attack vectors and one of them is the hardware supply chain, and that is what we are addressing.

CEOCFO: ***Where are you in development, commercialization and usage?***
Mr. Appleboum: The first version of our device is already ready for installations, but we keep further developing it all of the time, because with cyber security you need to keep running because the other side is always trying to find better ways to get inside of an organization. However, in terms of development and commercialization, we have one version that is ready for shipment. We are actually a very young company that is trying to build relationships with potential customers. We are hoping that within the coming weeks we will be able to announce our first customers.

CEOCFO: ***What changed in your approach as you were developing and improving on your system? Why is it better today than when you started development?***
Mr. Appleboum: First you must listen to you potential customers and try to understand their pains, then based on that you may make slight or major changes in order to adjust your solution based on their feedback. A good example of that is that we have met so many Chief Security Officers that were exhausted from installing more and more security devices and then had to manage them. Therefore, we wanted to do something that was a close to plug-and-play as possible, and that was one of the best feedbacks that we received from the market. Another one was in terms of how to deploy that on large organizations, because they do not always have enough manpower to go to each one of the workstations install each by themselves. This meant that we had to do something that could be installed by a common employee and not just an engineer. This allows the network engineer and the security engineer to see after a while that all were in place and then just deal with the problems.

CEOCFO: ***Are you funded for the next steps?***
Mr. Appleboum: Yes! We have very good investors, who are committed to the company. We have enough funding for more than a year ahead and as a young startup company, we are in contact with potential investors all of the time for future moves.

CEOCFO: ***Have you considered the competitive landscape? Are other companies looking at this arena or are you really ahead of the game?***
Mr. Appleboum: I’ve spentsix years in Army Intelligence in Israel and I was taught to never underestimate your competitors, although in those days they were the enemies. Therefore, we are not sitting idly by waiting for the money to get into the company. We know that even though the vendors are not pushing in that direction right now, we feel that some companies are starting to realize that their solutions are not solving the problems that we are seeing.

CEOCFO: ***Put it together for our readers. Why pay attention to Sepio Systems today?***
Mr. Appleboum: Because the harm that can be done on an enterprise or organization by a supply chain attack can take the organization down. I do not want to frighten anyone, but it is serious enough to pay attention to. Sepio Systems is offering a solution, so people should recognize that there is a major problem, start facing it, look for solutions and consider us.