ceocfointerviews.com

Issue: August 21, 2017

CEOCFO Magazine

Professional and Managed Services for Enterprise Security providing Protection from External and Internal Threats with the Tools Needed for Extraction while Preserving All Data

Rajiv Jolly
Chief Executive Officer
Principal Consultant and Founder

SourcetekIT
www.SourcetekIT.com

Contact:
Raj Jolly
647 818 4646
rjolly@sourcetekit.com

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

CEOCFO: ***Mr. Jolly, what was the vision when you started SourcetekIT and what is the vision today?***
Mr. Jolly: When we started SourcetekIT quite a few years ago we had the vision of providing professional services where we thought we could fulfill their extended network bench, which is a term that is commonly used for all of those engineers. Therefore, we thought we could have that extended team on their behalf and fulfill their high end engineering and extend it. That was a good start, but then we realized that most organizations already have a full bench. Therefore, this is what changed us and we got into getting more and higher engineers, the fully qualified engineers with ten plus years experience.

CEOCFO: ***On your site, big and bold, is "Protecting your data, securing your future." What do you understand about security that perhaps others do not?***
Mr. Jolly: That is a good question. Many large organizations have changed their practices, where they used to be just a firewall for protection, now it is totally different. There are more firewalls plus the content based security. It was easier before to break into the firewalls by opening or trying to open a port and getting through the application. Now, each application has to be further secured on its form for internal or external threats. Most threats are now internal rather than external where the firewall is in protecting the data. What we understand about security now is I do not think that many people know is that when any company gets hacked or if someone has access to a PC or a laptop, they may think they have viruses or if they have software that can provide them with remote access or copy data, but this is beyond that. What they have been doing is they have been coming in and having something installed in the memory of the hardware. It is impossible to detect and sometimes very difficult for any antivirus software to catch it and indentify this as a threat. Therefore, security in general has changed so much more than what it used to be three, four or five years ago.

CEOCFO: ***What happens if there is something in the hardware? How do you fix it? Or is it just throw the computer out and start over?***
Mr. Jolly: Once it is in the hardware we take the memory dump to extract data from the memory of the hardware. Most security technicians are becoming aware of this. They will install something on the memory of the hardware, but it only until you reboot your device. However, once you reboot that portion of the memory byte is gone. The trick for us is to get in without rebooting, capture what is in the hardware, how it was installed through the random memory and extract and figure out what was taken from the hard drive without them knowing that anything was taken. They will say, "We had our