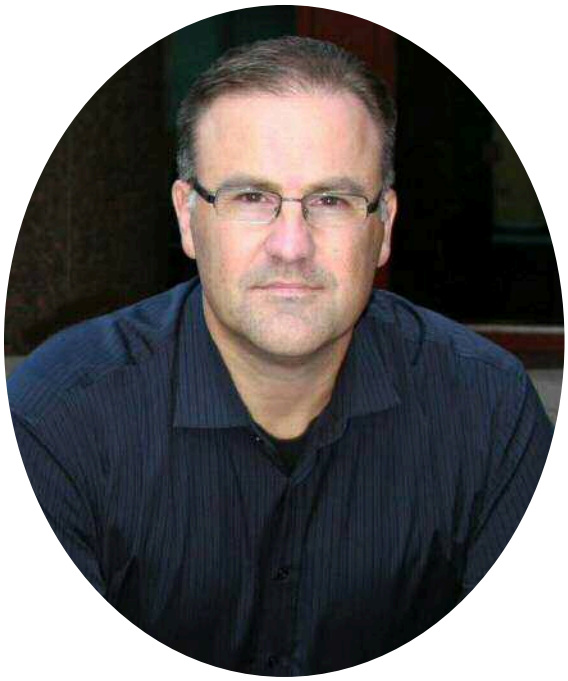
ceocfointerviews.com

Issue: December 25, 2017

CEOCFO Magazine

Q&A with Daren Klum, CEO and Co-Founder of Secured2 Corporation going beyond Encryption to Secure Data



Daren Klum
Chief Executive Officer & Co-Founder

Secured2 Corporation
www.secured2.com

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

CEOCFO: *Mr. Klum, what is Secured2 Corporation*?
Mr. Klum: Secured2 Corporation is an exciting new way to secure data beyond encryption. One of the things that we saw very early on with all of the security problems that were happening in this country was that we had to do something different. It has to be dramatic. It had to be innovative and new and it had to move past a binary type of encryption. Therefore, we basically run data through a process that shrinks, shreds and secures the data and protects it beyond encryption by taking all of the highly converted and highly randomized information and spreading it all over the place. Then as long as you can prove you are who you are you are able to reconstitute the data and bring it back together again to use. It is a really cool technology!

CEOCFO: *Would you tell us about the location? Is it your location? Is it cloud?*
Mr. Klum: What is really unique about this is that the customers can choose where those fragments live. I can be local. It can be hybrid where you have some of he shreds go locally in your own environment. Some of them can go out into the cloud in cloud locations or if you are working with a cloud vendor that you trust and choose, you can shred and spread, where shreds into multiple VMs within their environment or you can adopt what many companies want, which is a multi-cloud strategy can be shred and spread out into multiple different cloud vendors such as Google, Microsoft and Amazon. Also, what is interesting on the multi cloud front, is that you still get the benefit of all of their disaster recovery and business continuity and security for each individual shredded location. The only difference is that in our world even the cloud vendors cannot see what data you put into the network, because it is so converted, randomized and fragmented that they cannot see what is there.

CEOCFO: *How do you prove who you are to get it back or to use it?*
Mr. Klum: You prove who you are, and we are actually agnostic on the authentication front, although we do have a partner we recommend called TASCET. What TASCET does is they physically verify you, so it is not really authentication; it is physical verification, where we know that it is really you physically by facial and biometrics. Therefore, it is all combined into one solution. We are moving to a point where “I really need to know that it is you physically,” a point of authentication or verification and just really knowing it is you and then that will initiate the ability to restore.

CEOCFO: *If the recognition is good why do we need to have the data all over?*
Mr. Klum: Here is the analogy. When you are sending any packets over a switch network one of the challenges is that we send data sequentially. If you think about something that is encrypted today and how we are doing it today, you wrap data around with some funky math and you send it over the internet. You can capture those packets and then you can just pound on the encryption until you get in. Then, if you break into the data storage out in the cloud all the data rests in full,