CEOCFO Magazine

ceocfointerviews.com

Issue: December 11, 2017

Q&A with Scott Totzke, CEO of ISARA Corporation providing Quantum Age Security and Next Generation Cybersecurity keeping Companies using Cryptography Safe

Scott Totzke
Chief Executive Officer

ISARA Corporation
www.isara.com

Contact:
Scott Totzke
1-226-339-1201
scott.totzke@isara.com

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

CEOCFO: ***Mr. Totzke, what is the vision at ISARA Corporation today?***
Mr. Totzke: Our vision is to allow our customers to take advantage of all the wonderful technological advances that we are going to see from quantum computers in areas like material design and pharmaceutical research, without them being exploited by quantum computing. Within the decade, there will be a large-scale general-purpose quantum computer that will break all of the cryptography that protects so many of the things we do online today. As an industry, we must move towards quantum-safe security solutions; at ISARA we are developing the next-generation of cybersecurity.

CEOCFO: ***What do you and ISARA understand, on a very fundamental level about security, that others miss?***
Mr. Totzke: It goes all the way back to the formation of the team. Myself and Mike Brown, our CTO, started this company two and a half years ago. We have spent thirteen years together building the security practice at BlackBerry, so we have got a fairly extensive history in how to build security in constrained environments, as well as to implement complex cryptographic solutions in a way that is easy for the end user to use; in fact, invisible to the end user. It does not interfere with the activities that you undertake on a day to day basis. Over half of our company comes from that pedigree. Therefore, we have built a very strong organization on a fundamental belief that our past experiences, building of security solutions in the mobile world, translate into how we deliver this next generation of cybersecurity. Another way that we differentiate ourselves from how others attack the problem is that we are very focused on standardization. We think it is absolutely critical, that even as a small organization, we actively participate in the standardization of not just cryptographic algorithms themselves, but the implementations and protocols required to ensure that systems are able to communicate with each other in a completely transparent and compatible manner. If you do not have good standards, systems will not work well together. Look at your phone. Your phone works in one hundred and ninety different countries because we have excellent standards in the GSM standards body, which allows for interoperability. As the industry migrates into this next generation of security it is not just about getting the math right, that is really important, however, it is the foundation that will allow us to interoperate that is absolutely critical.

CEOCFO: ***Why is it taking so long?***
Mr. Totzke: None of this is easy. We have an installed base of millions or billions of end points that have to communicate and authenticate with each other. When you look at that, you can make the case that the most successful thing the technology industry has done over the last six years is embed strong encryption into everything we do. Even a non-technical user uses strong encryption thousands of times a day: checking your email, signing onto your carrier network, signing onto your Wi-Fi network, checking your bank balance, making a purchase on Amazon; we just embed it into everything that we do and we do not think about it. We have built a basis of cryptographic assumptions for the last forty or

fifty years that has served the industry well. But now we are looking at a threat that can be argued to be eight years out, around 2025 / 2026; which is when we will need to have new quantum-safe cryptography. The challenge today is a lack of urgency and recognition that we need to change the way we do security. If we do not, we are going to have a catastrophic failure. While eight years seems like it is a long way out, it really is not a lot of time to move these millions or billions of connected devices to a new type of encryption and this is essential to ensure that we have long term protection in everything from ecommerce, to protecting the operational speed of the government.

CEOCFO: ***Would you tell us about ISARA Radiate? What is your solution today?***
Mr. Totzke: ISARA Radiate is a toolkit designed for developers. It is the embodiment of our IP and our research in a set of software functions that can be used to implement quantum-safe cryptographic solutions in a variety of different products, such as mobile devices and enterprise data center solutions. It's essentially a set of building blocks that OEMs can use to migrate their solutions from where they are today to a quantum-safe solution. It has been on the market in commercial release for about two years now. We are on version 1.3 and we continue to iterate and build more functionality into it so that we can better serve the development community.

"Within the decade, there will be a large-scale general-purpose quantum computer that will break all of the cryptography that protects so many of the things we do online today. As an industry, we must move towards quantum-safe security solutions; at ISARA we are developing the next-generation of cybersecurity."- Scott Totzke

CEOCFO: ***What is different about the offering today than it was two or three years back? What have you added? How have you been able to do the improvements?***
Mr. Totzke: We started with the basic leading quantum-safe candidates for algorithms and implemented some of the core mathematical primitives, offering the core math functions in the initial release of the toolkit. In our first release, we had three or four algorithms covering some of the very basic and essential pieces of quantum-safe cryptography. Our second release focused more on developer integration tools by adding the OpenSSL connector. About fifty percent of cryptographic solutions that you use today rely on OpenSSL as a way to provide security for your transactions. Therefore, we thought it was really important to find a way to make sure we integrate our toolkit into the OpenSSL stack. In our most recent release, we rounded out the algorithmic base, so that we have all of the leading quantum-safe candidates included. Throughout our process, we continue to refine the performance of the algorithms. Essentially, we look at how we could improve the underlying performance of the cryptographic functions without compromising security. We want to make sure that we are providing solutions that, from a use perspective, preserve the user experience that you have today. We could not deliver a solution that would take you twenty minutes to sign onto your online bank account, that transaction has to take three or four hundred milliseconds. So, we are continually looking at how we can reduce the time it takes to perform mathematical functions that are equivalent to the tools we use today. That is our emphasis now and going forward. We will continue to look at how we can improve the performance quality of the algorithms, and the usability from a developer perspective so that it is easier to integrate our solution into existing products.

CEOCFO: ***Who is using your solution today? What types of companies and are there groups that really should be and have not paid enough attention or should every company have some integration with what you can provide?***
Mr. Totzke: Every company that relies on cryptography should be looking at quantum-safe security. Our solutions are the best in the industry, in terms of commercial solutions, to do that. That is a very broad statement when you look at how much cryptography is used without you being aware of it. Cryptography is built into everything, from the connected thermostat in your home, to your mobile phone and now we're seeing connected vehicles. Therefore, we are very much targeting the OEM base of technology providers. The automotive industry is quickly becoming a big technological player, so you can see where that is an interesting area for us. From there, you can diversify and start looking at things like mission critical control systems in critical infrastructure and other areas. A big part of what we do is making sure that we optimize our solutions for all different types of use cases.

CEOCFO: ***How do you work with your clients in using Radiate?***
Mr. Totzke: It depends on how you look at it because there are two sides. On one side, we work with the end user communities, such as the large banks or financial service institutions who need to be aware of the types of risks that they are being exposed to. Therefore, we do a lot of education and a bit of consulting on the risk and how much it manifests itself and where they need to focus their efforts in order to engage with their supply chain to provide the quantum-safe solutions for the future. Right now, much of that is in building awareness and setting the timeline, because even if they had the technology in place today, it is still going to take six or seven years to complete the migration, so they really need to start now. Then when it comes to the OEM communities that are deploying their solutions, we have integration services

both in architecture and implementation. In some cases, we'll build custom solutions because there is a specific process or a specific environment that we need to integrate into. Therefore, we offer a whole range of services, depending on who the customer is.

CEOCFO: ***How do you reach potential customers? How do you stand out? What might someone search for if they were looking for the area that you address in security?***
Mr. Totzke: They would probably search for quantum-safe cryptography. When you look at the investments that have gone into quantum information science over the last decade or couple of decades, in Waterloo, Ontario where we're located, there has been over two billion dollars invested in private and public funding. There is a lot of excitement about who is going to build the first quantum computer and it is only recently that people have started to pay attention to what sort of security risks that may pose. Therefore, if you are searching for quantum computers and quantum information science, you will increasingly start to see some commentary about what goes along with the advancements of quantum computing. Customers looking for protection from the quantum threat, will see solutions from ISARA.

CEOCFO: ***What is your global reach today?***
Mr. Totzke: Pretty much everywhere! We work in Europe and Canada and the US, as well as in Asia. However, we are primarily focused on North America, we are in Waterloo, Ontario, Canada and have a small office in California. I expect in the next twelve months to have folks in Europe and Asia.

CEOCFO: ***How is business today?***
Mr. Totzke: It's exciting and really starting to pick up. We have got a couple of early adopters. We have had product announcements with some smaller Canadian companies talking about integrating our tool kit into their products. What we have seen in the last three or four months is a real change as some of the coverage has shifted away from scientific journals. We have gone away from, "Is this a science fiction threat that we do not have to worry about," to "This has really become much more crystallized." In the last few months the discussion with a variety of different OEMs has really started to accelerate and intensify in terms of how many people are looking at this type of solution. I would say that by the end of the year we are going to hit this threshold where Google, IBM, Microsoft or some other large research company is going to come out with a quantum computer that is fifty qubits or greater. What that means from an industry perspective is that we will reach "quantum supremacy", meaning we'll have a quantum computer that can outperform the most powerful supercomputer available today. That should be a real signal, especially for anyone in the industry that has not been taking this seriously, that the threat is real and that the timeline to implement solutions is rapidly shrinking.

CEOCFO: ***What is the competitive landscape? Are many people taking your approach, somewhat?***
Mr. Totzke: We are the largest company of our kind. We have been around for two and a half years and we are thirty plus people. About twenty five percent of our staff are active in Big-R research. Today, there are a lot of smaller companies that are largely based in academia, such as professors looking at how they can commercialize their academic research. There are a lot of companies that are specializing in quantum physics to solve the problem such as quantum key distribution. Then there are the larger traditional ICT organizations where within their research groups there are two, three or maybe a handful of resources that are looking at this problem. There are the big tech companies such as the Microsoft and IBMs of the world. They are very focused on building quantum computers and achieving quantum supremacy; the bulk of their R&D is based on building quantum computers because they create such a great economic advantage from a technology standpoint.

CEOCFO: ***Does something like the Equifax breach that seems to be getting worse every day trigger interest or is that not on the level of ISARA's services?***
Mr. Totzke: Looking at this from a historical perspective, what I can say is you have never really seen a large-scale failure of cryptography in the past. The issues we see today are caused by human error, the unpatched system and similar situations are the cause. It has never been cryptography and that is what makes this problem we are dealing with so interesting, because now we are at a point where even if we did everything right and you did not have human error and you eliminated any of the variables like poor design or poor implementation, the cryptography cannot be relied on. That is what is going to be directly attacked and that is what is going to be vulnerable once there is a quantum computer. We as a technology industry have never had to deal with that. We have always been able to make little changes. We made our keys a little bit bigger and we have been able to use that as a hedge against the advancements in computing. With the advent of quantum computing, we can no longer rely on the same field of mathematics we've been relying on today. This is a much different threat. We need a completely new approach to security. With Equifax and other breaches, the cause is not cryptography. Therefore, I think that this is the first time that we can say with confidence, that we are on the cusp of seeing broad failure of our cybersecurity infrastructure if we do nothing.