CEO CFO

ceocfointerviews.com
All rights reserved!
Issue: April 14, 2014
The Most Powerful Name in Corporate News

DIGITUS BIOMETRICS
Access Security Solutions

Secure Biometric Access Control Technology

***David Orischak** - CEO*

Digitus Biometrics was founded on ground-breaking biometric fingerprint recognition and encryption technologies with a single purpose: To create the most secure access control solutions possible.

The Company focused early, on development of its “next generation” technology and is now a market leader in access control solutions via the application of its highly advanced fingerprint recognition technology, operating software, and unique system configurations.

Years of continuous development and feature/function improvements have led to what is today the industry’s most complete set of biometric access control solutions, capable of securing entire enterprises from the front doors of multiple buildings to the doors of individual cabinet doors in the data center, all on a unified platform that delivers an indisputable audit trail across every protected access point.

Today, the Company’s fourth generation fingerprint recognition technology provides unparalleled access security solutions in various high-profile installations including government, military, healthcare, educational, and commercial facilities.

The Digitus team continues to focus on engineering and design breakthroughs that extend its own product lines and deliver application-specific, private label solutions to customers seeking to serve their own industries with the most secure access control solutions possible.

Interview conducted by: Lynn Fosse, Senior Editor, CEOCFO Magazine

CEOCFO: ***Mr. Orischak, what is Digitus Biometrics?***
Mr. Orischak: Digitus Biometrics is a biometric access control company. We offer our customers a technology platform that allows them to secure access to buildings and highly secure areas within those buildings. We got into the access control business in 2005. Our legacy products enable our customers to secure things like the front door to buildings, reception areas, hallways, offices, interior doors and interior rooms and so on. About four years ago, we entered into the business of securing server cabinets in the data center. Today we are the only company in the world that has biometric access control technology that secures server cabinets and data centers. The biometric that we use is the fingerprint. I tell everyone that we decided on the fingerprint, because it is highly reliable, as it is a high integrity biometric. It is economical to deploy across a wide range of applications. There are other good biometric authentication devices out there. You have probably heard of facial scanners, iris scanners, palm scanners and the like. They are all good technologies, however the fingerprint enables you to economically secure more access points than does the palm scanner, as an example. It is very difficult to put a palm scanner on a row of server cabinets in a data center.

CEOCFO: ***Would people believe a fingerprint just because everyone believes they are unique and maybe not everyone believes that a palm will do it?***
Mr. Orischak: As you know, law enforcement has been using fingerprints forever. It has been highly reliable. We have built a major portion of our legal system around authenticating people through fingerprints. Much of our judicial system is based on that. Since 2005 we have installed thousands of these products and we have had zero false positives and zero security breaches in that time. We secure some pretty high profile clients; people like the US Air Force, the Army, Duke University Medical Center, Wake Forest University and the Center for Regenerative Research. We secure NORAD, the nuclear missile facility out in Colorado. There are many prominent organizations that trust us with their access control needs.

CEOCFO: ***Have people not thought about securing data centers? Are there particular challenges? How did you get to be the only one?***
Mr. Orischak: There are other folks in the physical security business with regards to data centers. However, they all use proximity cards or card access control systems to do that. Card access control systems are the technology most people

are familiar with. They are often used to control entrances to buildings and parking lots and sensitive areas within a building. Card systems have been around since the early 1980s, so they are widely accepted and almost everyone is comfortable with card systems. The problem with card systems is that the cards are easily lost, stolen or copied. With something as important as server cabinets in a data center, you cannot afford to have someone with a lost, stolen or copied card granted access to that data center and the equipment and information that lies within. We like to use the term "indisputable audit trail", because with a biometric at the server cabinet level, it truly is indisputable as to who went into that cabinet, what day, what time and how long they spent there. With a card there is always something called "plausible deniability". I could say "it was not me, I was out of town that day, but maybe someone who stole my card went into that cabinet that day or copied my card and went into that cabinet that day. There are literally hundreds of documented cases where cards have fallen into the wrong hands and the wrong people have be given access to data centers, resulting in a data security breach. Therefore, cards are very fallible, biometrics are not. Ours is a patent pending technology. We developed the concept a little over four years ago and we have been refining it ever since.

CEOCFO: ***Are people coming to you looking for a better solution? What is the state of the industry? How do you get the attention that to me seems obvious, but I am guessing it is not as obvious as I think it is?***
Mr. Orischak: The way that I like to describe it is we are an emerging technology in an emerging marketplace. When you start talking about data center security, most people think you are going to have a discussion around cyber security. It is protecting against hackers that are getting into your systems somewhere, stealing passwords or hacking into a data center or a given website. There are a great many high quality companies that are focused on cyber security and they have built some strong solutions. However, there are very few of us that are actually focused on the physical aspects of security within the data center. As we go down the road, there are more and more documented cases of people physically leaving data centers with thumb drives or hard drives that do not belong to them. There has been a heightened awareness in the marketplace that facility managers need to consider physical security as important as cyber security. We are on the doorstep of the mass acceptance phase of this technology. I think we are just on the early stages of that growth curve. People are now very much attuned to the fact that people can walk out of data centers with hard drives with equipment and that cyber security is not enough. If you look at the people that make the server cabinets that go in the data centers, the cabling, the power distribution units, the heating and cooling, the uninterruptable power supplies. Those companies already have relationships in that marketplace and are partnering with us to help their customers physically secure data centers. We do not have a single direct sales person on staff. We do this all through our partners.

> **"We have, far and away, the most secure access control platform on the planet and the strongest warranty in the business. If an executive chooses to secure his data center with our technology, we guarantee that data center will be compliant with all of the government and industry regulations." - David Orischak**

CEOCFO: ***Are there industries that are more receptive than others or that are more aware than others?***
Mr. Orischak: There are. I guess one way of answering that is that there are three key market drivers to our business. One is the ever growing list of government and industry regulations out there. You are probably familiar with HIPAA. Most everyone has heard of HIPAA, which is the Health Insurance Portability & Accountability Act. If you are a data center and you are storing medical information and medical records and individuals medical records, you need to make sure that that information is secure, both from a cyber perspective (secured from hackers) and secured from a physical perspective. There is another set of regulations called PCI DSS, which deal with personal credit card information. Therefore, if you are a data center and you are housing someone's name, address, social security number and credit card information, you are subject to PCI DSS regulations. Both HIPAA and PCI DSS have specific line item descriptions of the need for physical security in data centers. Industries that are most in need of our technology include the managed healthcare industry, hospitals, banks, credit card companies, anyone that does a financial transaction over the internet, which is just about every company today that accepts credit card payments. They are susceptible to PCI DSS audits. There are some big Fortune 50 companies out there today that are not able to pass those PCI DSS, physical security audits in their data centers. That is what is driving them to our door, for our solution.

CEOCFO: ***When someone is buying and they are not buying directly from you, do they know the name? Does it matter?***
Mr. Orischak: Today we do not have any of what I would call "private label" agreements in place. Therefore, every product that goes out, even though it is sold by someone else, still has the Digitus name on it. Therefore, we are becoming quite recognized in the marketplace. We are developing brand recognition. We front all of our product names with the initials DB, which is the acronym for Digitus Biometrics. It is funny, when you talk to people in the marketplace they shorten our name to DB; this is a DB product or this is a DB solution. As a strategic goal and objective, we did not think it was necessary for us to build brand recognition, but in fact we have, because of the overwhelming popularity of the product.

CEOCFO: ***What is your geographic range today?***
Mr. Orischak: We just came out of a meeting pertaining to our installed base of products and it is worldwide. We have units installed everywhere from Australia to Singapore, Malaysia, Europe, South America and of course here in North America. Therefore, it is truly a worldwide product. We do not have any product in Japan yet. We have not broken into the Japan or the China market yet.

CEOCFO: ***Do you find it is about the same as far as interest, acceptance, knowledge and need, or do you find many differences in the different geographies?***
Mr. Orischak: The government and industry regulations change from country to country. The European Union has different regulations, focused on data center security, from the United States. The tie that binds though is that you are a public data center and providing a service for a Fortune 500 company here in this country, you are subject to the same government and industry regulations as that Fortune 500 company, no matter your location.

CEOCFO: ***Therefore, at the end of the day everybody needs Digitus!***
Mr. Orischak: Yes! In a server cabinet, many folks do not realize there could be upwards of a quarter million dollars worth of IT equipment in those cabinets. Therefore, the next key driver in our business is that folks want to make sure that what is in those cabinets stays whole; that no one walks off with a server. That is second market driver; they want to protect the IT, the hard assets that are in those cabinets. Then, the third market driver is down time. There are a number of organizations that publish statistics that say that the majority of downtime at a data center is caused by human error. What our technology does is help to reduce human error by making sure that the right person is in the right cabinet. What happens after that, we cannot insure, but at least we make sure that the right person is in the right cabinet.

CEOCFO: ***What has changed in your system over time?***
Mr. Orischak: That is a great question! You should be writing our marketing literature! This technology platform of ours has been around since 2005. We have thousands of successful installations and we are constantly receiving feedback form those customers. We tend to incorporate that feed back into our technology… always trying to improve the product.

It was the US Air Force that helped us get into the data center security business. We were securing most of Dover Air Force Base, helping them secure what they call a communications closet. There are over three hundred of those on Dover Air Force Base alone. We were using our traditional access control products to secure those communications closets. A communications closet is a bit larger than what you might picture as a janitorial closet. Inside there may be one, two or three server cabinets, all with voice servers installed in them. As you might imagine, communications for any military base are important to day to day operations. We were securing access to those closets with our building access control technology and we were approached by a ranking officer at the Air Force who explained he had server cabinets that were not located in closets. He asked if we could install our technology on these rogue cabinets, standing in the rear of cafeterias and reception areas. That launched us into the server cabinet security business or the physical data center security business. Over the past four years (since that conversation at Dover Air Force Base) we have listened intently to customer feedback. Our customers have led the way to the point where we are today, where we think we have hit the bull's eye in terms of securing server cabinets and data centers.

CEOCFO: ***Why should people pay attention to Digitus Biometrics?***
Mr. Orischak: Every company around the globe should be concerned about physical security in the data center. One reason is that the average cost of a security breach in a data center is well above seven million dollars today. That does not include damage to brand. If you look at some of the recent security breaches like Target, Michaels Crafts Stores and Health Net the damage to brand resulting from those security breaches has been astronomical. An executive has to ask himself and his management team, "Can we afford the damages, the financial damages and the damage to brand associated with a physical security breach?" If the answer is that you think you can, then you should not be concerned with Digitus Biometrics. If you are like most executives, you believe your company cannot afford a security breach and damage to brand. You want to be compliant with all of the government and industry regulations. If that's the case, then you need to pay attention to what Digitus Biometrics is doing. We have, far and away, the most secure access control platform on the planet and the strongest warranty in the business. If an executive chooses to secure his data center with our technology, we guarantee that data center will be compliant with all of the government and industry regulations. If the data center fails a compliance audit for whatever reason, we will gladly refund the purchase price of the technology. That, is in a nutshell, is why people should pay attention to DB.

BIO: David Orischak, CEO and Chairmen at Digitus Biometrics, has over thirty years of experience in corporate and entrepreneurial businesses. Digitus Biometrics is a biometric access control company with a patent pending technology to physically secure the data center. The Digitus biometric platform is based on fingerprint authentication and it allows Digitus customers to secure everything from the front door of a building to the server cabinet door in the data center, with the same IP based platform. The company has recently announced two new products for the data center and we are receiving phenomenal feedback from our customers. Customers are able to centrally manage, monitor, alert and produce an indisputable audit trail for every access point on the network.

David is also a Partner at Penn Valley Group, a Philadelphia based business advisory firm. From strategy to planning to execution, Dave has an established track record of successfully growing businesses. His clients rely on his judgment and the practical application of his knowledge to assist with planning, funding and executing their business strategies.

Dave has been successfully raising capital for businesses since 1985 when he financed the growth capital for PC Concepts, a training and software development company he co-founded. Dave planned for and managed the execution of an aggressive growth strategy for PC Concepts that culminated with the sale of the company to Ziff-Davis in 1991.

Much of Dave’s success is a direct result of his ability to draw on seven years of experience at IBM. While there, he worked in a number of progressively more responsible sales and marketing positions in the Philadelphia Region.

Dave earned a BS in Economics from Wilkes University and is a member of Omicron Delta Epsilon, an international honor society in Economics.

DIGITUS
BIOMETRICS
Access Security Solutions

Digitus Biometrics

2 East Bryan Street, Suite 502
Savannah, GA 31401 USA
912.231.8175
www.digitus-biometrics.com