ceocfointerviews.com

Issue: February 26, 2018

CEOCFO Magazine

Q&A with John D. Rome, CEO and Co-Founder of Intensity Analytics Corporation providing Behavioral Authentication Security Software that combines Advanced Mathematics and Machine-Learning Techniques to Assure the Identity of a User and Deny Illegitimate Access

John D. Rome
Chief Executive Officer & Co-Founder

Intensity Analytics Corporation
www.intensityanalytics.com

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

CEOCFO: ***Mr. Rome, what is the focus at Intensity Analytics Corporation today?***
Mr. Rome: The focus of Intensity Analytics is developing software and processes to change the security landscape, to bring technologies that we have worked on and developed and known about for many decades to the market, to help address the worldwide cybersecurity crisis.

CEOCFO: ***There are so many different ways of addressing security. What is your approach?***
Mr. Rome: My company, Intensity Analytics Corporation, has developed the capability to accurately recognize people's unique physical behavior by means of innovative, and now patented, advanced mathematics. Doing this is the best method to assure the identity of an individual in the course of commercial or personal communications without violating privacy norms nor requiring any special hardware. We have patented a unique set of mathematics to be able to characterize idiosyncratic human movements. Everyone has his or her own style of doing things, particularly for example, keying on a keyboard. Therefore, when someone makes those movements, they can be identified with the same certainty as happens with a photograph or a blood test or other kinds of identification methods. This has been a long-time quest of ours. We spent many years developing these capabilities, proving that it works and having it vetted by outside experts. Long story short, as the internet and communications proliferate around the world, critical to the success of that is going to be making sure you know who is at the other end of the wire, as they say.

CEOCFO: ***How do you assess a pattern? How long of a time, how much, how many different ways of doing something, do you have to look at to know? Would you walk us through how it works?***
Mr. Rome: As with all data subjected to any statistical analysis, there has to be enough of it in order to be able to draw meaningful conclusions. Let us use touching a keyboard as the example for our conversation, because almost everyone has one of one kind or another. If one were to touch a keyboard, but just a single key, let us say the letter K just once, the effort of doing that would be recorded but it would not be statistically significant. Not enough. That conclusion is based on the math of statistics. It is like going to a state to do a presidential poll and only talking to one voter. You may have a one hundred percent answer, but statistically it is not representative of the population. At the other extreme, having tens of thousands of movements is too much. You do not need that many. What you need is a reasonable amount. The definition of a reasonable amount varies a bit dependent upon people's individual habits. For example — and I will use analogies to help explain some of these things —if you are a fan of music and you play a short note or two sung by a singer, and if you know that singer's voice pretty well, and if the singer is pretty constant with what he or she does, then you can recognize that performer. Otherwise, it might take a line or two, or perhaps even a whole verse, to recognize that voice. For our purposes, building these mathematical models, take, for example, the effort of entering a password. You might have to enter it fifteen or twenty times, but the system we developed records all of that automatically. It does not take any special effort. We do not keep any of the text. We never even look at any of the actual password text. Again, we only look at the

timing of the finger muscle movements to identify relevant patterns. Usually, this can be done in ten minutes, but it can also be an ongoing process spread over a day or so. It is kind of like bringing a dog home from the animal shelter. It barks at you the first morning and a couple of mornings later it does not bark anymore because it knows you. That is how this works.

CEOCFO: ***Does it matter if you are using the same keyboard, if you are working on different computers?***
Mr. Rome: No, it does not. Now, having said that, we sometimes get asked, "Does it also work on the keyboard on a smartphone?" The answer is that could work, but people's movements are not repetitive enough to be statistically useful and trustworthy. However, it works on tablets with a glass surface and does works on almost all keyboards.

CEOCFO: ***What if someone is distracted? Is the core of the system sensitive enough figure out if someone took a little longer or was holding something in one hand, and so hitting keys differently?***
Mr. Rome: No, there are thresholds beyond which you can go. Let me give you some examples. If you normally type with two hands, but you are holding a drink in one hand, or if you have injured one hand, then your overall pattern of behavior has changed. There is nothing wrong with the different behavior, but it is different. It is sort of like if you are using a photograph of someone, but all of sudden they are wearing an enormous bandage over one eye, the picture is obviously different. Therefore, when keying, significant distraction can be a factor. Sometimes people who do not have a math background have asked, "What is the math used for?" Our simple answer is, "A measure of closeness." Here is another analogy. When you walk outside during the summer and look up to see a thunderhead; did you stop to think that there has never been a cloud exactly like that in the history of the world. Ever. Anywhere. They are all unique everywhere and across all time. Yet you immediately recognize, "That is a thunderstorm, it is not a normal raincloud." Why is that? That is because it looks pretty close to what it is supposed to look like. We have developed some pretty involved mathematics to measure "closeness." We can recognize people when they are tired or when they are enthusiastic — or perhaps angry or otherwise temporarily running with a different kind of mindset. However, there is, of course, a limit. Algorithms know about human variability's. We use machine learning. These days everyone uses that phrase. You see "machine learning" everywhere. It's the "in" phrase. You can hardly talk to a software person who does not "have machine learning." We have actually have it and have worked on developing and patenting it for years. The purpose of our machine learning technology is to figure out the answer to the question you asked, which is … "Is this John Rome and John Rome is tired, or is this somebody else, or could it be John Rome who is distracted, or typing with one hand?"

"My company, Intensity Analytics Corporation, has developed the capability to accurately recognize people's unique physical behavior by means of innovative, and now patented, advanced mathematics. Doing this is the best method to assure the identity of an individual in the course of commercial or personal communications without violating privacy norms nor requiring any special hardware."- John D. Rome

CEOCFO: ***How does the software pick up the touch and feel?***
Mr. Rome: When one touches any computer peripheral device — again it is easiest to picture a keyboard — when one touches a keyboard, the time of that touch recorded very, very precisely. Most computer systems record time increments in incredibly small values; one hundred nanoseconds. That is a tenth of a millionth of a second. Therefore, when you touch a given key it really sends out three timing singles. When I describe it to you, you will recognize what you do. When you initially touch a key it generates a "key down", meaning that the button is starting to travel down. When your finger hits the bottom of the travel, then that is a "key press." Then when you let go of the key and it comes back up, that is a "key up." So, there are three timing events involved in touching an individual key. And there are many, many timing events between keys. I happen to know the following numbers because we are asked this question all the time. When someone types, let us say, a twelve-character string, there are ten to the one hundred and twenty ninth power of possible timing pattern varieties. That is an enormous range of numerics measured, again, at a tenth of a millionth of a second. People tend to type in a very predictable pattern, but no one is ever identical to any other when typed by humans. In fact, as many times as you will type just your own name in your career, let us say tens of thousands of times, the metrics of you actually typing your own name has never been exactly the same to the millionth of a second. Therefore, an algorithm that can measure "appropriate closeness" is critical. This is where my company got its patents. Individual password-typing activities form little effort clouds. Massive collections of 1's and 0's. Everybody automatically, and without a plan or conscious effort, forms his or her own distinct effort cloud simply by the way they move. All clouds are idiosyncratic. They are just as indicative of who you are as is a picture of you. I know … it's a bit hard to believe at first because we are not used to thinking that way. But it's true!

CEOCFO: ***Are you commercialized? Are you still in development? Who might be using your services? Who should be using it? Where is Intensity Analytics today?***

Mr. Rome: Our technologies are fully developed. They have been independently tested and validated by some of the most well respected and best known independent professors — PhD's who do this kind validation work for the federal government. They are department heads at George Mason University in Virginia. Our products are done. It took us a long time to get there … about five years in development and a couple of years to get the foundational patent we are really proud to own. When people initially hear about what we do they sometimes say, "I have heard about that, or I have seen it, or that must be easy to do." In fact, it is very difficult to do. It took quite some time to develop the complex mathematics. We are a veteran entrepreneurial company. This is our third time at inventing processes and business and technologies. We are now entering the market. We have done many, many test installs. I cannot mention the names in a public interview like this, but some major government entities —we have fifty thousand seats in one of them for example — have been testing it for well over a year. Now, to answer the second part of your question, the most respected publication in our industry that has chronicled the extent of the worldwide cybersecurity disaster was published by Verizon. It's called the DBIR Report. Verizon's figure, which everyone kind of takes as gospel, is that eighty one percent of the world's cybersecurity problems all trace back to stolen credentials. Say you step away from your desk and an administrative assistant copies it, or say an unhappy spouse or a friend knows your password, or say they bought it on the Dark Web or whatever; however they obtained it, rightfully or wrongfully, when they type your password then they get in. Using our behavioral capability, they do not, because their typing, even though they accurately entered the requisite characters, does not match the behavior. There is an enormous market. It has been calibrated at around four hundred billion dollars by independent knowledgeable industry experts. Of course, market numbers coming from one's own company are less trustworthy than coming from independent people. It is a pretty big market and we are looking to develop various kinds of partnerships with companies to bring our solutions to the world.

CEOCFO: ***You offer TickStream.KeyID®, CV and Activity. What are the differences in your solutions?***

Mr. Rome: TickStream.KeyID is the product that guards the gate. When you go to a website you are almost always asked for a user name and a password. With KeyID®, if you do not type it both properly and with the "right effort," you do not get in. KeyID automatically measures the effort involved. Obviously, if your password is San Francisco and you type Los Angeles then the password itself is wrong, so the host would not submit it to our algorithms to do an effort check. We never see the text, so the host that is using our system must first make the "correctness determination." CV® is stands for Continuous Validation. Those algorithms work on any text. Building a reference library of effort metrics (again, not text) takes a little bit more text, somewhere between six hundred and one thousand characters; maybe half a page of emails, so later, when you type anything, your overall pattern of typing can be identified by matching against the pattern using our patented mathematics. The analogy would be to a singer. Say you happen to be fond of Willie Nelson. You know twenty or thirty of Willie's songs. Then you hear a new song by him. You would say, "I have never heard that song before, but I can recognize it as being sung by Willie Nelson." CV is designed to pick up and identify the author of a document. It has a great use inside organizations to establish the authenticity of a document. For example, one of the problems that is plaguing Facebook right now is the difficulty of making sure of who the actual author is. Is it a legitimate US citizen posting, with the (reasonable) right of freedom of speech to make a statement about controversial whatever, or is it somebody from another country who is pretending to be a US citizen, and therefore has tighter or different limitations. We would be able to tell the difference. We have a method by which people can ascertain the authenticity of the author of a document. Activity® is the third leg of the stool. What Activity does is keep track of what is happening on a computer in terms of context. For example, if you are typing numbers into a cell, that type of typing activity is not indicative of who you are or how you behave, because normally there is a lot of thinking and thought-filled entry involved. Activity communicates directly with the operating system all that is happening within the computer, again, without revealing any personally identifiable information.

CEOCFO: ***Is the world ready?***

Mr. Rome: Absolutely! The answer is … just look at all of the bad stuff that is happening now! For example, John Podesda's email being hacked and the government compromised — or any of the millions and millions of breaches. Ask Yahoo! A billion passwords of theirs are out! The world needs this additional measure of security. Here is my authority for saying that. One of the biggest legislative events in the world is happening this coming May; the GDPR, the General Data Protection Regulation, which basically sets standards for what is acceptable and what is not in terms of using PII, Personal Identifiable Information, to ascertain people's identity. Actually there is a great deal more about GDPR, but going into that now is too deep. But GDPR is a worldwide game-changer, and it's coming up this May 25. Blockchain is another example. Blockchain is a terrific way of detecting data in transit. However, the question is who started it rolling, and are they who they claim to be? One must identify the source with certainty. And who's at the receiving end? Not knowing those two makes a secure in-transit pipe incomplete, to say the least. Medical privacy. It is a requirement of HIPAA to

know exactly who the people are in the doctor, patient, pharmacy triad. The high-level label for this is called anonymous authentication, where you can know that somebody is legitimately a member of a pool, without having to know their name, their social security number, their address, and so on. The whole debacle with Equifax is another example. The world is more than ready! The reason our new anonymous authentication capability has not been out there is simply because it is extremely difficult to do.

CEOCFO: ***When you are talking to the right people do they understand the difference on a deep enough level to say, "This is the way we need to go?" Do technical people get it or is there a lot of convincing needed?***
Mr. Rome: Great question. The answer with the technical people is not so much. Sometimes there are feelings of pride or what the industry calls NIH (Not-Invented-Here), so you have to do without it, but that is a human emotion. The bigger issue is in the C suite; does management get it. These people generally are not technical but they sure are vulnerable. Given widely-recognized standards of due care, for example, when you check into a hotel and you give your name and your address and your credit card number, you expect that they are going to take good care of that information. When you give personal medical information to your doctor you expect that they are going to take good care of it. One of the challenges has been a general awareness of how to do the right thing in an affordable, proven, and convenient manner. Now, with all of the press about the extent of the cybersecurity disasters basically everywhere, and the countless millions of people affected by this, when combined with with the looming GDPR requirements and the enormous financial consequences of not meeting those; people really have no choice but to pay attention to the need for what we have. However, because the technology is new, there are always people who resist. However, for us, in terms of building a business, we are dealing with a potential market of well over one billion people who are affected. Even if people pick up on what we do gradually, we still can build a very strong business.

CEOCFO: ***What, if anything, might be missed when someone first looks at Intensity Analytics and looks at your solutions?***
Mr. Rome: There is not yet significant brand name recognition. We are small company. Many big companies like to deal with big companies, so they may not appreciate that although we are comparatively small in terms of revenue, some of us have far more experience than most scientists at big companies like IBM and Google — in my case, nearly forty years. Sometimes they miss the fact that an awful lot of the invention, innovation and creativity in our world comes from individual entrepreneurs — people who have dedicated their lives to creating helpful solutions and products and capabilities in the world. So sometimes we have to overcome that. But the good news from a business perspective … I do not believe that there is an executive out there who is not aware that there is a growing security problem … and that there are big consequences if they do not pay attention to it.