ceocfointerviews.com

Issue: April 16, 2018

CEOCFO Magazine

Q&A with Thomas J. Miller, CEO of ClearForce LLC. providing a Workforce Assurance Solution enabling Organizations to better Manage Employee Risk with Post Hire 24/7 Event-based Alerts of Misconduct and High Risk Behavior Outside the Workplace

Thomas J. Miller
Chief Executive Officer

ClearForce LLC.
www.clearforce.com

Contact:
Tom Miller, CEO
908 500 3000
tmiller@clearforce.com

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

"ClearForce is built on a foundation of employee consent and transparency, placing privacy at the forefront of enhancing organizational security."- Thomas J. Miller

CEOCFO: ***Mr. Miller, what is the concept behind ClearForce LLC?***
Mr. Miller: ClearForce focuses on helping organizations better manage employee risk on an ongoing basis and achieve an appropriate balance of privacy and security for their organization.

CEOCFO: ***Would you give is an example of what people are looking at day-to-day, as far as employee risk?***
Mr. Miller: In most organizations we typically find that employee risk is managed with a pre-hire background check. Beyond that, ongoing risk management becomes very technology centric. Organizations are looking for aberrations in network behavior. You can think about cyber monitoring and cyber technology solutions that are looking at the activities of employees on their company's computer network, including their use of company email. Therefore, what exists today is a gap from pre-hire screening with a focus on the human side of risk to cyber technology monitoring. That is where ClearForce comes in. ClearForce fills the gap by helping organizations understand individuals who may be under a form of personal or financial stress that is creating risk within the organization.

CEOCFO: ***What is the range of the solutions you provide?***
Mr. Miller: We deliver real time event based behavioral alerts, activities that are occurring outside of the organization, and make those behavioral alerts actionable inside the company through a legally compliant business application and workflow. We solved the big challenge and legal regulatory hurdle of how to consistently handle external behavioral information in a way that makes it legally compliant, standardized and transparent from an employee perspective.

CEOCFO: ***Would you give us an example?***
Mr. Miller: If you go back to the pre-hire background check, most of those checks are looking for criminal activity; criminal convictions that

have occurred in the past. Probably the most common alert that comes through our system would be real-time arrest information. If someone is arrested of a crime, based on their role and based on the severity of the crime that may be something that the organization needs so know about. Therefore, we will deliver a criminal alert, typically in real-time or with same day notification.

CEOCFO: ***Does an employee need to consent to this at some point? Do they recognize that they are agreeing to it when they are hired?***
Mr. Miller: Yes. Consent is the foundation of our solution. Much like a company obtains employee consent for an initial background check, consent would enable the organization to be able to look again, to look on a regular basis, an ongoing basis, at specific sources of information. Yes, consent is a big deal. We are really unique in our approach to insider risk, because we are not looking at it as a big data problem per se. We are not trying to find negative information about employees, because that is not a very palatable solution in most corporate cultures. Rather, we are working in a way where the employee understands specifically and exactly what information is necessary for the company to know about in order to provide an appropriate level of security.

CEOCFO: ***What other risk factor might you review?***
Mr. Miller: Again, back to the initial background check, in some positions it is appropriate to evaluate individuals that are under financial stress. Therefore, we will look at leading indicators indicative of financial stress. If you are in a job that requires direct access to financial transactions with cash or perhaps very sensitive trade secret information, it is important for employers to understand whether there is financial stress of the employees. Beyond we can alert on an employee's presence on a wanted or watch list. If someone shows up on the Sex Offender Registry or shows up on an FBI or Interpol or sanctions list; if you are in a regulated industry and your job is sensitive in nature then those types of alerts may be appropriate. Another really important aspect is that nothing is defined for the overall company. All the alerting and all of the policies are configured and customized for each company and for each specific job role within that organization. That is essential because not every employee represents the same level of risk to the organization.

CEOCFO: ***Do you help a company decide what level, what positions and what they want looked at or does a company tell you? What is the interaction when you initiate your system?***
Mr. Miller: It can be a little bit of both, but typically we predefine policy within the system. We will make recommendations on job roles and we will make recommendations on appropriate policy given the experience we have in the marketplace and our experience in risk management. Then we will train our customers how to configure and adjust policy, so it can be specific and appropriate for them. Policy tends to be a collaborative working session with the organization. If it is a large enterprise organization and they have multiple functions and lots of job roles there is nothing that requires them to have an all or nothing approach. They may start with higher risk functions or roles within the company, apply policy and then expand usage to other functions and other roles.

CEOCFO: ***How is the information protected within the company so that only the appropriate people have access?***
Mr. Miller: We have security at all of the layers that you would expect and maybe then some. All of the data is encrypted in transit and at rest.

All the employee information and any of the alerting and proprietary data of the company are not accessible to us. It is not viewable by us. Access is limited to those with permission-based roles from within the company. Customers set administrative roles that are typically managed by someone within human resources or an internal investigation or potential legal function. All with secure access into the system. We created a variety of automated checks and balances so as customers adjudicate issues through their permission-based roles, and no data ever leaves our system. Therefore, everything is retained and secured and centrally archived.

CEOCFO: ***Who is using your services today? What types of companies?***
Mr. Miller: We sell into public and private sector businesses and organizations. Today, we have customers that represent financial services, legal services, insurance, government contracting and real estate, as examples. Today, all of our customers are in the United States, but we are actively working to deploy in a select international markets, with a strategy to support our multinational customers in the markets where they have significant employee presence and significant risk.

CEOCFO: ***What relationships have you developed on your end to get the information? How are you able to add additional information or perhaps be in touch with different jurisdictions if is related to criminal activity?***
Mr. Miller: We work with a variety of data partners that provide various forms of alerts within our system. I mentioned that we tend to align to the pre-hire background check, because that tends to represent the balance of privacy and security for many organizations. That said, we have an open API to incorporate other alerting sources based on different customer requirements. That becomes another collaborative point of our engagement with customers to really understand the specific information they believe will best fit that balance. We also have the ability to incorporate internal alerts. We have an ability to have a very seamless integration with cyber technology and digital activity alerting applications as well.

CEOCFO: ***Are companies or government agencies aware that they need to go further; that they need to institute a system or is there an education component to what you are doing?***
Mr. Miller: Many companies have contemplated how to bring an external view into their employee risk management infrastructure. I think the main challenge they have faced is they have not had a legally compliant application to ensure standard actions under EEOC or FCRA rules and regulations. However, that is exactly what ClearForce has been designed to do, to solve that regulatory problem and make external behavioral information actionable.

CEOCFO: ***How do you stay on top of the regulatory issues that may change from time-to-time?***
Mr. Miller: The more regulation, at a federal, state, and local level, the larger the value we deliver as we provide automation and an ease of use to apply policy, not only for risk management, but for legal compliance. We work with some of the nation's leading law firms, in their labor, privacy and FCRA practices to ensure we stay up to date. We communicate information proactively to our customers, so that they are aware of updates as we become aware of them.

CEOCFO: ***How are you reaching out to prospective clients?***
Mr. Miller: Today, we sell direct into the key market verticals, which includes the government, financial services and energy. We have started to establish partnerships in a few other verticals; including transportation and education. We also connect through our experienced advisory board, board of directors and customer referrals.

CEOCFO: ***What have you learned as people have started to use ClearForce? What has changed?***
Mr. Miller: We first began this business assuming the predominant risk would be information risk, cyber risk, and that continues to be a core component of our value proposition. However, what is interesting and a little surprising is that we are doing quite a bit in physical security as well. Physical security represents employees with secure access to restricted areas, or risk of physical harm from an employee to a customer or another employee or infrastructure. We add a lot of value to physical security. Again, it goes back to the fact that most organizations are running a single background check at the time an employee is hired and then no ongoing evaluation or vetting of any sort thereafter. Therefore, we become a logical extension to the pre-hire background check.

CEOCFO: ***How is business?***
Mr. Miller: Business is good! It is busy and we are really excited. There are so many different companies where we can deploy and add value very quickly. It is the kind of solution that integrates easily within their existing infrastructure, so we are not ripping and replacing or displacing systems. We tend to complement and enhance existing investments that have been made.

CEOCFO: ***What is the competitive landscape? Are other companies looking to get into this arena?***
Mr. Miller: We have competitive threats at a general level with those performing analytics and data aggregation to solve insider threats, but their common approach is to solve insider risk as a big data problem from outside the organization and without employee consent. In many ways I think those organizations represent good partner candidates for us as we integrate third party analytics and more data solutions as components of our platform.

CEOCFO: ***What, if anything, might people miss when they first look at ClearForce that should show through and is important to understand?***
Mr. Miller: ClearForce is built on a foundation of employee consent and transparency, placing privacy at the forefront of enhancing organizational security. Privacy is the essential element. Unless there is balance of privacy and security and unless an organization is able to achieve a shared security objective with its employee base, it becomes very difficult to solve insider risk. We have taken a very unique approach to privacy and transparency and it serves as one of our most important differentiators in this marketplace going forward.