ceocfointerviews.com

Issue: October 20, 2014
The Most Powerful Name in Corporate News

Cyber Security and IT Assurance Services

About Enterprise Risk Management
Enterprise Risk Management, Inc. (ERM) is a cyber security and IT assurance services firm. With over 16 years of focused experience in information security and breach investigations, ERM offers the full range of services to help organizations meet the continually changing and complex demands of cyber security. Enterprise Risk Management was recently featured in the Miami Herald - "Taking on the Hackers" and in the South Florida Business Journal - "Data Security: A Big Job for Health Care Providers."

Interview with: *Silka Gonzalez -* *President & CEO*
Conducted by: Lynn Fosse, Senior Editor, CEOCFO Magazine

CEOCFO: *Ms. Gonzalez, what was the vision when you started Enterprise Risk Management, and what is the vision today?*
Ms. Gonzalez: The vision has always been to be able to provide excellent cyber security services and to become a worldwide leader in this area. This vision remains intact. ERM is able to provide high quality at a fair price. Together with our clients, ERM can accomplish our mission, which is to provide protection to our clients, their customers and to society in general. Cyber security is a big concern today, and with the growing threats, it is going to continue to be very important.

CEOCFO: *This is a topic that everyone is familiar with and many companies claim they have the solution. What do you understand fundamentally about cyber security that perhaps others do not?*
Ms. Gonzalez: I know it is a huge problem, and it is a problem that is affecting us here locally, nationally and internationally. It is a problem that affects all industries and sectors of society, and we are just at the beginning of this problem that keeps becoming more complex and affects all areas of our life, including national security. Until recently, many people were not paying much attention to this topic. It is now becoming more of an issue that people are aware of. I still believe that most organizations, especially small to medium sized ones, do not understand the severity of the problem. I think the biggest problem is insufficient awareness, due to a lack of education about this problem. Many people do not comprehend how severe the problem is and the ramifications that it will have.
What sets ERM apart is that we have found a way to provide the best quality of services at a price that fits the needs of each organization. Not a lot of firms have been able to find this balance. You either have high quality service providers who are extremely expensive or you have very inexpensive service providers but they often don't know what they're doing. Also, we understand, in great detail, the regulatory compliance aspects of information security and we help our clients jump through those hoops as well.

CEOCFO: *Who are your typical clients and how do you work with them?*
Ms. Gonzalez: We serve 16 different industries, banking being the largest industry because it is highly regulated. We serve the public sector and the private sector, and in the public sector most of our clients are in the federal government, like agencies of the Department of Defense, Homeland Security and Department of State, and the Department of Treasury. In the private sector, we have clients that are large institutions that need help, or are regulated. In the banking sector we work with Banco Santander, Credit Agricole, Banco do Brasil; in the healthcare sector we work with Mount Sinai Medical Center; in the airports space we work with the Metropolitan Washington Airport Authority; in the insurance sector with large multi-national organizations like Assurant Solutions – these are some examples of the large ones. We're now also seeing demand from mid-sized and smaller organizations that are calling us for our services.

CEOCFO: *Is there a particular time when a company is likely to turn to you?*
Ms. Gonzalez: When they have a breach, they call immediately. When they have a big problem on their hands and they need to find out how it happened, who did it, determine what the next steps are to contain the problem, and to gather and preserve digital evidence so that it is admissible in court. I also advise them to make sure that they hold a "lessons learned" session to ensure that their response to incidents undergoes a continuous learning cycle. We also hear from a company very fast when there is fraud. We also hear frequently from the organizations that are highly regulated like banks, healthcare institutions, publicly traded companies, or those that process credit card because they're all governed by one regulation or another. Based on their typical regulatory compliance cycles, they get in touch with us. We are now also getting many requests from airports and federal agencies for services such as security awareness training programs

and physical security training (for instance, to protect against active shooters) for organizations besides all the other services that we provide.

CEOCFO: *Why are they turning to Enterprise Risk Management specifically?*
Ms. Gonzalez: I think the level of trust that comes from the fact that we've been doing just this – cyber security – for over 16 years now and counting makes a huge difference. It gives a clear message that we're not a fly-by-night company. We are a well-established company with very large clients. This has to be a reason for that big client list we have. We also have offices at multiple locations - in Coral Gables, Florida as well as Washington D.C. We also have operations in India. We have a very good reputation helping our clients, and our retention rate of clients is over 95 percent. We get many client referrals and I think that's a testament to the quality of service they get for reasonable fees. Our professionals are very high in caliber - similar to the ones you can find in large organizations like IBM or Big Four firms with practices similar to ours. We compete by keeping our overhead costs low. As a lean operation, we are able to provide clients with value in terms of the knowledge that we have, the quality of service we provide, and the fees that we charge.

CEOCFO: *How do you evaluate the new technologies?*
Ms. Gonzalez: I think technologies keep changing all the time and we like that. It shows we're making progress. But the security-focused brain and the way of thinking about information security remains the same. If you approach the security problem in the same way every time, you will never be bogged down by changing technologies. The thing is that after doing this for 30 years and having people here who are seasoned professionals, when you look at the problem of cyber security it is not only an IT problem. It is a more comprehensive problem involving the logical side of the security inside computers as well as the physical aspects, the awareness, training and software side, the policies and procedures, and so on. Every organization, whether public or private sector, large or small, they all have the same areas of problems and concerns. The scale might differ. The key thing is to make sure those key areas of concerns and issues from the cyber security perspective are addressed diligently. It is just like if you have a small kid, a teenager or an adult – each needs to be examined by a doctor in different ways but with the same central theme. They know what they need to do in the human body for a child, teenager or adult because there are certain things that they should be checking for. It is the same thing.

"Over the past 16 years, we have seen several ways that organizations get attacked and we've figured out ways to help organizations protect themselves against those threats. We've provided clients with the value proposition of having the highest quality at a fair price." - Silka Gonzalez

CEOCFO: *How are you able to accommodate all of the clients in busy times?*
Ms. Gonzalez: So far, we have been very successful in assisting our clients and scaling the business accordingly. Not everybody is having breaches and are calling here every day, although we have seen a significant increase in breaches over the past couple of years. When you are dealing with this kind of service, decisions must be made by many different people from senior management up to the Board of Directors. It is not something that happens in a two-day period, but a longer period typically. We usually have people asking for things, but they don't necessarily need you on-site the same day. You can pace yourself, and good project management and scheduling is the key. It is like a law firm that answers calls for different cases and different clients. Some cases can take longer and some less – not all of them are so easy that they can be resolved the same day. There are some situations like that, but it is more complicated in a majority of situations.

CEOCFO: *What might you look at when you are evaluating for a client that perhaps others do not realize is important?*
Ms. Gonzalez: I think many people and organizations invest a great deal of money, people, and effort in implementing a secure infrastructure. We have seen that breaches and people who are attacking organizations are using more creative ways of getting into systems and technologies and methods that were not foreseen or addressed by organizations as well. For example, many times they have not paid enough attention or put sufficient controls in place for their third-party vendors who have direct or indirect access to their systems. Poor vendor management creates a risk and is often a source for security incidents. It could even be something as simple as physical security – simple but often ignored. Sometimes, not enough attention is dedicated to training internal employees. How you educate your own employees on what is good behavior or bad behavior to protect the data of the organizations is critical and most effective when they understand the implications of their behavior. These are some examples of areas that we see are not addressed properly. Also, sometimes the education needs to go all the way to the top executives and the people in the board of directors. Now they face all this pressure that they have to deal with securing their data, and sometimes they do not understand all that is involved with this and the ramifications of not dealing with this correctly.

CEOCFO: ***It is so overwhelming for many people that know they should but really do not want to look at the problem!***
Ms. Gonzalez: It is frightening, and the thing is that technology is essential for running an organization and is here to stay. Society needs to take advantage of technology and move forward for progress, but I also think that the implementation of state of the art technology comes with a price. One of the prices of using technology is that you are dependent on the hardware, software and all the networks and connections you bring with it; which then takes the problem of inadequate controls, privacy and protection to a completely different level. As we get into new technologies, we see that it opens the door for more issues that are coming in the future.

CEOCFO: ***You were recognized as a 2014 Florida Company to Watch. Tell us about the significance of this recognition?***
Ms. Gonzalez: We feel very proud that we were selected as one of the companies to watch and grow in the next few years. We have obviously been working very hard for many years, and it is not something that we have done overnight. Especially for me, I started this many years ago and I am the founder of the company with a vision that sounded almost impossible. Many people were telling me it was a big mistake in my professional career, that I should not do it and that I should stay in corporate America in a good, well-paid position. But my vision was completely different. To see the effort and sacrifice that you put in over the years bearing fruit makes you feel good and positive.

CEOCFO: ***What surprised you as the company has grown?***
Ms. Gonzalez: What has surprised me in the last few years is the magnitude of how this problem is evolving in society, and sometimes I feel it is becoming like the "wild, wild west" once again. It is hard to keep up with everything that is happening because just like the cyber security industry is very large and many organizations are in the industry, the problems in cyber security and the hackers who create problems in cyber security keep growing too – for instance, hackers and malicious individuals online are now like an organized crime group. It is surprising to me how fast this has evolved, and I cannot imagine what will happen 20 years from now with technology and all the issues related to cyber security.

CEOCFO: ***Put it all together for our readers. There are many companies in your industry, why Enterprise Risk Management?***
Ms. Gonzalez: Over the past 16 years, we have seen several ways that organizations get attacked and we've figured out ways to help organizations protect themselves against those threats. We've provided clients with the value proposition of having the highest quality at a fair price. Our significant client list, which has grown year after year, and our high client retention rate shows the considerable confidence many organizations have in ERM's services and ERM's cyber security expert's.

BIO: Silka Gonzalez founded Enterprise Risk Management in 1998 with a select group of expert information security and risk assessment consultants. True to her vision, Ms. Gonzalez has built an information security advisory and assurance company that provides high quality and cost-effective information security risk management services for organizations worldwide operating in multiple industries. Ms. Gonzalez has more than 25 years of experience in providing value driven IT assurance services. Prior to founding ERM, Ms. Gonzalez was a consultant with Price Waterhouse, where she was the Manager of IT and Business Services. Ms. Gonzalez was also Manager of Information Systems Auditing for Diageo, PLC, and Manager of Information Systems Security for American Bankers Insurance Group, now known as Assurant Solutions.

Ms. Gonzalez holds a Masters degree in Accounting Information Systems from Florida International University in Miami, Florida, and two Bachelor's degrees, one in Accounting, and one in Computer Information Systems, from Xavier University in Cincinnati, Ohio. She also successfully completed the Entrepreneurial Masters Program at the Massachusetts Institute of Technology. Ms. Gonzalez also holds professional certifications and licenses, including Certified Information Systems Security Professional (CISSP), Certified Information Systems Manager (CISM), Certified Information Systems Auditor (CISA), Certified Information Technology Professional (CITP), Payment Card Industry Qualified Security Assessor (QSA), and Certified Public Accountant (CPA).

Ms. Gonzalez is also active in professional organizations. Among other things, she is a past President of the Miami Chapter of the Institute of Internal Auditors, and a Board member of the Information Systems Audit and Control Association (ISACA). Ms. Gonzalez has also taught a graduate level IT Audit course at Florida International University, and is a coach for the University of Miami's Entrepreneur Program. Ms. Gonzalez has also published articles and is a regular speaker on a wide range of IT and cyber security topics, including regulatory compliance in the banking and health care industries, security awareness, vulnerability assessments, identity theft, hacking, security breaches, and computer forensics.

Enterprise Risk Management

Douglas Entrance
800 Douglas Road
North Tower, Suite 940
Coral Gables, FL 33134
305-447-6750
www.emrisk.com