ceocfointerviews.com

Issue: June 25, 2018

CEOCFO Magazine

Q&A with Kyriakos "Rock" Lambros, CEO and Founder of RockCyber, LLC strategic consultants aligning Cybersecurity to Enterprise Business Strategy, reducing Enterprise Risk through Strong Governance and Compliance Programs while delivering Operational Excellence

Kyriakos "Rock" Lambros
Chief Executive Officer and Founder

RockCyber, LLC
www.rockcyber.com

Contact:
Rock Lambros
844.729.2730
info@rockcyber.com

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

CEOCFO: ***Mr. Lambros, RockCyber, LLC launched this month. Why do we need another security company? What can you bring to the table that is not available now?***
Mr. Lambros: We focus on Cybersecurity strategic consulting; almost like a management consulting company from a Cybersecurity perspective. We specialize on aligning security strategies to enterprise business goals. That means that we really want to work with businesses who are looking to grow in a competitive environment, that may have both traditional IT and/or Operational Technology environments that may leverage cloud, industrial control systems and/or Internet of Things (IoT) technologies, and with individuals who are open-minded, are prepared to be challenged and are amenable to change. We do this in order to proactively address both business market demands and changes to the threat landscape, to leverage Cybersecurity to develop and maintain sustainable competitive advantage over existing and new competition and to also leverage Cybersecurity to drive high-growth and revenues. We do this by suggesting and implementing strategic plans focused on achieving desired business outcomes, aligning cybersecurity strategy to enterprise business strategy, reducing enterprise risk through strong governance and compliance programs, and delivering operational excellence and process improvement.

CEOCFO: ***Why is now the time? Why do you feel that people are ready to look at security from your perspective, as an overall and a strategic arena?***
Mr. Lambros: It is in the media almost every day. It is getting more coverage by the day, so therefore there is awareness of the actual risks. Organizations have to realize that Cybersecurity risk is a business risk, not just an IT risk. A Cybersecurity attack can impact you company's bottom line due to spending time and resources from recovering from damages and/or from lost revenue. A disruption in service to your customers directly impacts your revenue. Some small or medium sized businesses simply cannot absorb that. They are more and more becoming targets because they do not have the resources to dedicate to a full-time Cybersecurity program. That is where we at RockCyber can jump in. Per Verizon58% of breach victims in 2017 were small businesses. 76% percent of breaches were financially motivated and 68% of breaches took months discover. Then, McAfee and the Center for Strategic and International Studies released a report that said that cyber crime cost between $445 billion and $600 billion globally in 2017.

CEOCFO: ***What is your plan to reach out to potential clients?***
Mr. Lambros: Doing interviews such as this, trying to evangelize the need for Cybersecurity and also, to evangelize that the perspective that RockCyber is taking on Cybersecurity is not to be that department of "no", but rather the department of "how". We have gotten the reputation in the Cybersecurity industry of being that department of "no" and being a cost center to the business as opposed to being a department that can help the business actually grown and generate revenue. We are taking a stance that that is absolutely not the case; that we can absolutely leverage Cybersecurity to give you a better advantage in the market. I have been doing Cybersecurity for almost 20 years in the corporate world. Cybersecurity is a ubiquitous problem across all industry verticals and sizes of companies.

CEOCFO: ***When you are looking at a company and what they are doing, their vulnerabilities and what would be the best solution, what might you consider that less experienced people do not take into account? What have you learned from all your experience that puts you ahead of the game in crafting a solution?***
Mr. Lambros: Oftentimes what some of the larger consulting organizations would do is that they would come in and they would have their methodology of doing an assessment and will try and really fit a square peg of a company into their round hole of a security assessment. What we want to do is absolutely the opposite of that. We pride ourselves on being more of a boutique type of shop. We will come in and say, "Oh, you want to be ISO 27001 certified? Well, we really don't think it's right for your business. If you at least want to align your security program to ISO 27001, then there are 114 security controls, and I am going to sit here and tell you that you do not need to be a high maturity level in each of those 114 controls. I am going to sit here and tell you that for your company and your business goals, that is overkill. Maybe you need to be a high level of maturity in only 20 of these controls, a medium level of maturity in 70 of these controls, and a low level of maturity in the rest. Let's prioritize and allocate funds and resources accordingly." There is much more money is me saying "Sure, no problem, we'll get you ISO 27001 certified", but that wouldn't be right for the client.

"RockCyber is an important company because we are pivoting the focus of Cybersecurity risk from being an IT risk to being an enterprise business risk."- Kyriakos "Rock" Lambros

CEOCFO: ***Do you recommend certain programs? Do you put in a personalized solution? After the advice or after the consultation, what are you providing?***
Mr. Lambros: Absolutely. Each engagement is different. Although we primarily focus on strategic consulting, If the client wants us to do a technical evaluation of specific security technologies and recommend to them which one is the best one for their environment, we can do that. If the client decides they would like to move on with implementation services, we partner with the right people to provide those implementation services to the customers. For instance, a client may say, "We want to deploy a new firewall solution, so, RockCyber, we want you to evaluate the top players in the market and give us a recommendation on what fits our business." We will conduct a product evaluation, make our recommendations and work with the client to pick the right solution for their business. Then we have a list of strategic partners that we work with to provide the implementation services.

CEOCFO: ***How do you help a client understand that it is not a static situation, that what they put into place today, what you recommend, may change?***
Mr. Lambros: Fortunately, that is an easy sell, because of everything that you see in the media. The media jumps all over data breaches, financial losses and privacy impacts that we have seen in the United States over the past several years. This includes everything from Equifax, to the recent Facebook/Cambridge Analytics scandal. The threat landscape is constantly changing. Individuals and organizations are more and more aware of that fact now. Having a Cybersecurity program is just that. It is a program. It is not a project that you stand up, walk away from and rinse your hands of. It is an ongoing program with continuous improvement throughout the program. There are governance, risk and compliance processes that have to be put into place to monitor the effectiveness of your program and to ensure that your program is mitigating the risks of your company appropriately and down to the level of your acceptable risk posture. Every organization has a different risk posture. Some organizations are risk averse. Some organizations are really risk accepting. That risk posture may change as your business goals change. You have got to tailor your Cybersecurity program accordingly.

CEOCFO: ***How do you know when someone is just picking your brain and when someone may really have an interest?***
Mr. Lambros: That is a great question. There is a challenge to qualifying a potential customer; however, everybody is a potential customer, right? We are based in Denver and I am involved in the local Cybersecurity community here through different industry organizations, so I am okay with giving "free" advise. We have a strong tech community here and we

share and collaborate with each other constantly. I certainly wouldn't have gotten to where I am today without the "free" help of others. However, there comes a point to where it is up to me to say, "This requires more of an in depth analysis of your organization and your business goals and we should discuss something maybe a little more formal." If we are having just a conversation over a couple phone calls or some coffee or lunch, to spread the wealth if you will, I am okay with that, but when it gets to beyond the point of cursory, advisory type of stuff, talking about point specific strategies or point specific solutions for your organization, then we need to discuss having a more formalized engagement. That is because I need to get NDAs in place, because I am going to start asking some very probing questions.

CEOCFO: ***Who is the right person to speak with at an organization?***
Mr. Lambros: That is different in every organization. It could be anywhere from whoever is running the IT organization all the way up to the CEO and even the board. As I mentioned earlier, Cybersecurity risk is not just an IT risk. It is an enterprise business risk. However, some smaller businesses still punt it off to the IT organization. With many of the larger businesses we are seeing more engagement from the C-Suite. It is really about understanding the organization and understanding the market that they are in. For instance, I have an oil and gas background, and in the Oil and Gas industry, perhaps the CIO or the CISO (if there is one) is the more important individual to target. However, I also come from an ecommerce background as well. With ecommerce, it is absolutely a CEO, CFO, COO or CTO type of discussion to have and the corporate boards are much more engaged there than maybe they would be with a more traditional, less progressive, company.

CEOCFO: ***What has changed in your approach from the time you thought about launching RockCyber to the actual launch? What did you recognize as you were developing the concept for the company?***
Mr. Lambros: Really focusing on business outcomes verses technology risk. Quite frankly, technology risk is the easier sell. Spreading fear, uncertainty and doubt and saying, "Yes, you have a Cybersecurity risk; look at everything that is going on in the media. We can implement all these silver bullet types of tools to help you 'become more secure'" is a much easier sell than taking a step back and really defining what "more secure" means for your organization. Most importantly, how do we leverage that to drive the bottom line? I have tried to do that in my corporate world life, but it is really easy to fall back to playing with the shiny bells and whistles of security technology. Now that I am putting on the CEO hat, if you will, of my own organization, it is about aligning Cybersecurity to enterprise business goals.

CEOCFO: ***Are you looking for investments, partnerships, any kind of funding as you go forward?***
Mr. Lambros: Not at this time. We are in a fortunate position to where we do not need investment. My goal is absolutely at this stage to grow the company organically. My focus is on leveraging my relationships and bringing on customers one at a time, and I want to maintain that. We keep very customized, very personalized types of engagements, and I believe I taking on investment potentially leads us into a situation to where we have to focus on volume, which means focusing more on standardizing my engagements and going back to fitting that square peg into the round hole that I talked about earlier.

CEOCFO: ***You like what you are doing!***
Mr. Lambros: Yes, I do like what I am doing. Absolutely! It has been a passion of mine.

CEOCFO: ***Why is RockCyber, LLC an important company?***
Mr. Lambros: RockCyber is an important company because we are pivoting the focus of Cybersecurity risk from being an IT risk to being an enterprise business risk. As long as data is worth money, cyber attacks and data breaches will continue to escalate. However, not all attacks will be financially motivated. More and more attacks, I believe are going to be politically motivated, especially attacks against critical infrastructure. Whether that be in the financial sector or the energy sector, or the healthcare sector, etc. Attacks will increase as traditional IT and operational technologies start to converge. Then there is one of today's buzzwords, IoT; the Internet of Things. One of our niche plays is in helping organizations secure their IoT deployments. Honestly, that market is so new that there is not a standardized approach in doing so. The proliferation of IoT is undeniable, though. IoT are all those types of things in an environment that allow items like your refrigerator to talk to the Internet and automatically reorder eggs when you are running low. They are your smart watches and your personal assistant devices. Having said that, IoT is gaining most traction in enterprise environments. From an oil and gas industry perspective, digitizing the oil field, putting sensors along a pipeline, leak mitigation are all things that bring business value and save costs.
Another concern I see is the change in the regulatory landscape. High profile breaches such as Equifax, Uber and Verizon, and the privacy concerns raised by the Facebook/Cambridge Analytics scandal, have lawmakers calling for stricter regulations to protect user data and to minimize the impact of such incidents. In the U.S., Congress has failed to pass any meaningful comprehensive Cybersecurity regulation, so organizations have to contend with a hodge-podge of

overlapping laws and standards at both the industry and state level. For instance, HIPPA regulates the healthcare industry and the FERC/NERC CIP standards regulate the power grid (via the Energy Policy Act of 2005). At the state level, just about every state and the District of Columbia have passed their own data breach notification laws. Finally, at a global level, there is now GDPR, the legal framework that governs data security and privacy for EU citizens. Although GDPR is a European based regulation, every company that collects data from an EU citizen, regardless of whether or not the company is based in the EU, is in scope. With all of these different laws, regulations and standards flying around, it is just about impossible for an organization to keep track of them all. Unfortunately, I do not see a consolidation of these laws and regulations in the near future. That is why we are an important company, because we are going to help you stay in front of it all.