ceocfointerviews.com

Issue: March 6, 2017

CEOCFO Magazine

Cyber Security Consultants enabling Executives to Become More Proficient Cyber Risk Managers

Kip Boyle
Founder, President & Chief Executive Officer

Cyber Risk Opportunities, LLC
www.CyberRiskOpportunities.com

Contact:
Kip Boyle
253-234-5474
Kip@CyberRiskOpportunities.com

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

CEOCFO: ***Mr. Boyle, would you tell us the focus of Cyber Risk Opportunities?***
Mr. Boyle: Our focus is on helping executives become more proficient cyber risk managers and by executives I am talking about middle market executives.

CEOCFO: ***Are many people looking to understand more or looking for someone to handle it for them?***
Mr. Boyle: I think they are struggling to get their arms around cyber security. A lot of companies really don't know how to manage it so they tend to treat cyber risk as a technology intensive problem and they tend to look for technology intensive solutions. I think they are finding that is not really helping them in the way that it used to because the people that are attacking them are using technology but they are not exploiting technology to attack them, so cyber risk is changing and they are trying to figure out what to do.

"We sell a managed program because we believe that cyber security is not something that you buy, like a firewall, it's what you do every day that makes you secure or not."- Kip Boyle

CEOCFO: ***How do you engage with a company to know what is right for them or to enable them to explain their situation?***
Mr. Boyle: First we try and help executives reorient themselves from seeing cyber security as a technology problem to seeing it as a management problem. When they are able to make that transition, it unlocks more options for managing cyber risk. For example, just looking at the data about breeches, today it takes over 200 days, on average, for a company to find out that they have had a data breech. Yahoo is a good example of a company that was hacked. It took them two years to acknowledge it. It also turns out that organizations find out that they have a data breach typically because a customer tells them, law enforcement comes to them, or a news media outlet finds out and then it starts to spread through word of mouth. This is a great example of how it is not a technology problem. The fact that people know that you have had a data breech and that your word of mouth is bad and your brand is under pressure. In a situation like that, if the executives are surprised then they are already behind the ball. Another thing we do is help them realize that they have to do some pre-planning around data breech response. That is all management work and there is not much technology involved. By helping them reorient towards cyber security being a management problem, it lets them be better prepared for when they do have a data breech.

CEOCFO: ***Would you walk us through an engagement?***
Mr. Boyle: Our approach is highly structured. We sell a managed program because we believe that cyber security is not something that you buy, like a firewall, it's what you do every day that makes you secure or not. We come in and once the customer subscribes to our managed program, we measure and score their cyber security so we have a framework and a methodology. We can score them depending on their size and how responsive they are, we can do all that within thirty to sixty days, a complete scoring. Then we use those scores to figure out what their top risks are, and that can involve anything from not understanding where all of their digital assets are, to not having the right technological preventions in place and maybe they are relying on outdated technologies. It also could be that they do not have an incident response program that spans the full breadth of the different activities that they are going to have to be involved in. Once we identify their risks and we give them priority, that is where it starts to become kind of magical. Executives understand scores because they are used to managing things by the numbers, so that helps and they understand and love priority so we have everything prioritized for them. Then we get into this great conversation about their risks and ask them what they want to do about them. We get into a great conversation about the full breadth of all the options they have. Going through those options can be a conversation, or some of our customers are data driven so they like us to do more data analysis to determine what exactly their problem is and what their return on investment will be. They want to know the business value of spending money on cyber security. We can help them with all that. Once they figure out what they want to do about their risk, we work with them throughout the year. We meet with them at least monthly and we have a quarterly meeting with them and update their progress and their scorecard. The scorecard is great for them because we print that out on an 8 ½ x 11 sheet of paper. We laminate it and give it to every executive. When they are out doing their work, if they should get prompted by questions from an investor or member of the board or anybody that asks what we are doing about cyber risk, they already have their story ready to go and they can tell it in about fifteen to twenty minutes. There are no more blank looks when they get asked that questions.

CEOCFO: ***Are insurance companies starting to require more in this area from companies they insure?***
Mr. Boyle: Yes, insurance companies are very much interested in seeing their customers take good measures to prevent a data breech and to minimize the damage should a data breech occur. The insurance companies are struggling right now because they do not understand the key factors involved. For example, when you go buy auto insurance, the insurance industry understands which factors affect automobile safety. They know the daytime running lights decreases the risk of an accident so you can get a discount for having daytime running lights, air bags, anti-lock brakes, collision avoidance. It is well understood so as a result their premiums are determined very accurately and all the forms are standardized. In contrast with cyber risk, they do not know any of that stuff. What I am seeing is premiums that they are charging are going to vary wildly from one carrier to the next. The questions that they will ask you when you apply for a policy will not look the same from carrier to carrier. They are struggling to find out what it is that we should be looking for and who is our best risk. That is a great place for us because what we can do is take that story about this organization and say these guys understand what their risks are and they have a plan for managing those risks and here are the numbers that show it. It is very persuasive because they do not have anything else to go on.

CEOCFO: ***How are you reaching out for clients and how would they find you?***
Mr. Boyle: It can be difficult to find us if you do not already know somebody who is working with us because usually executives are technology minded and so they think that they need to find an IT service provider in order to help them. That can represent a barrier for people looking for us and understanding that we work differently and that we can work more effectively because we are going to work at an executive level as opposed to a bits and bytes level but we can get down to that level if it comes to it. The way we are getting word out right now is referrals. We are growing organically at this point. The one thing we are doing in particular is we are starting to turn our attention toward the legal sector because what we did in our market analysis is we were looking for companies that had a high need for our services and a high awareness. We cannot afford to go out and educate the entire market on this. The way we accelerate that with attorneys is we have a legal education program that we provide for free. It is a one-hour program and attorneys that participate can get a legal educational credit which they are all required to do. We are getting tremendous traction through that and that is generating a ton of interest. We are starting to see some leads coming from that.

CEOCFO: ***What has changed in your approach over time?***
Mr. Boyle: I have been working in cyber security since 1992. I have seen a ton of change over the years. Since I have launched my company about eighteen months ago, I have even seen some change there. For example, when I first started my company I was not sure who the best buyer was and I was accustomed to the buyer being the person in charge of the IT program. Based on conversations and research, what I realized was that is actually shifting because there is a lot of downward pressure from boards of directors and investors. There is also a lot of supply chain pressure, so if I am a large company and I am using an outside legal firm, that outside legal firm has in their custody a lot of my very

sensitive information. I protect my sensitive information because I am a big company and I put a lot of resources into it but the law firm is not as big. They may not be protecting my data nearly as well as I would like them to so now I am going to start to put pressure on them to up their game. We also see this happening in the healthcare sector. You have a hospital for example that does not print its own explanation of benefit statements, it hires an outside provider to do that. But guess what? Whereas the hospital is under tremendous pressure to safeguard patient data, until recently, the printing company did not have commensurate protections because they were not required to and it was an enormous cost of doing business for them. Therefore, I am seeing a lot of my customers experience a ton of supply chain pressure from their customers and then they are turning around and looking at their third-party vendors and saying oh my gosh here I have Boeing telling me as a service provider that I have to do a better job. I am now a mid-market company and I am looking at my smaller vendors and I am asking them what they are doing because they are in here and part of my program. It has been interesting to see the shift in the supply chain.

CEOCFO: ***What's next?***
Mr. Boyle: We have to hire some great people. The good news is we do not have a tremendous amount of fixed cost so this is not a situation where we have to raise a lot of capital. We just need to take the methodology that we have and hire some great people and make sure that as we grow we are able to keep our promises so we do not grow in an out of control way.

CEOCFO: ***What, if anything, might people miss when they first look at Cyber Risk Opportunities?***
Mr. Boyle: When they first encounter us, their mind is typically in the IT space so they think that we are a traditional security consulting firm and that if they work with us that we are probably going to offer to do an assessment and we might ask for a five or six figure fee to do that. They might be concerned that when we come in and find out what their issues are that we will pressure them to find more services. That is not how we operate at all. Our major focus and only focus is to support executives and their decision making. Inevitably it always turns out that they do need more work. We have partners that we typically will bring in to do that work. We do that because we want to maintain the executive's confidence that we do not have a hidden agenda and that our only agenda is to serve them and to make sure that they are becoming more proficient in managing their cyber risk. We are focused and that's how we are different.

CEOCFO: ***Final thoughts?***
Mr. Boyle: Many executives are surprised when they find out that the things that they need to do really do not cost a ton of money. Many of them assume that once we tell them what their cyber risks are, that now they are going to have to expend a lot of capital because they are accustomed to buying firewalls and computer servers or whatever. It turns out that there are many things that executives can do that do not cost a lot of money but rather is the result of shifting people's attention. For example, cyber hygiene is a concept that we talk about. It is kind of a hand-washing paradigm. While you are on the internet and you are doing work every day, you have all these germs coming at you whether it is malicious code or phishing attacks. There are a lot of things people can do at their computers that can significantly decrease risk. Executives do not know what those things are. We can shine a powerful light on those things and they can train their people and they can drive down the risks that they are going to get compromised by 70-80% just by changing the way people do work. These are not that disruptive of changes. That is often a big surprise for them, and of course it is a very pleasant surprise.

Cyber Risk Opportunities