CEO
CFO

ceocfointerviews.com
All rights reserved!
Issue: June 5, 2017

CEOCFO Magazine

LAZARUS ALLIANCE IS PROACTIVE CYBER SECURITY
IT AUDIT & COMPLIANCE - IT RISK ASSESSMENT & MANAGEMENT - IT GOVERNANCE & POLICIES
POLICY MACHINE
CYBERVISOR
YOUR PERSONAL CXO
SECURITY TRIFECTA
HORSE PROJECT
AUDIT MACHINE
POLICY MACHINE
CONTINUUM GRC

With a Mix of IT Audit and Compliance Activities, IT Risk Assessment and Management, Governance and Policies and Cybervisor Services, Lazarus Alliance is enabling Organization to be Proactive in Cyber Security

Michael Peters
Chief Executive Officer

Lazarus Alliance
www.lazarusalliance.com

Contact:
Michael Peters
1.888.896.7580
Michael.Peters@LazarusAlliance.com

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

CEOCFO: ***Mr. Peters, the tagline on the Lazarus Alliance® site is Proactive Cyber Security. How are you able to be proactive effectively?***

Mr. Peters: The primary thing is that it really involves doing things to eliminate problems before they become problems for the organization. We arrived at that situation by providing a very comprehensive mix of IT audit and compliance activities, IT risk assessment and management, governance and policies and Cybervisor services for our clients world-wide. As an audit and compliance organization we are accredited with various authorizations for the major industry standard assessments out there. For example, we are a FedRAMP 3PAO. There are actually only about forty organizations in the world with that designation. We performed the AICPA's SSAE 16 SOC 1, AT-101 SOC 2 assessments. We are a PCI QSA. We perform a multitude of NIST based assessments such as HIPAA and CJIS and a variety of others listed on our website that we assist our clients with. Within the realm of risk assessment activities; those are all about assessing risks that threaten a company's core business assets. Some of those threats are natural while others are adversarial. We assist with the identification of potential problems before they actually become problems protecting business value, customers, and shareholders.

> **Our advantage is very deep industry knowledge and experience, internationally awarded and recognized professionals who are all well credentialed… Cyber security, audit, compliance, and risk is a cyclical activity. The bad guys do not take breaks. They do not take holidays. They are always working to try to circumvent your controls to steal the essence of your company or do damage. We add tremendous value added because we remain vigilant for our clients around the world."- Michael Peters**

CEOCFO: ***Is there are particular point in time when a company would turn to you?***

Mr. Peters: Again, along the same theme of proactive cyber security, just about all organizations have some sort of regulatory requirements that they are faced with, so there are cycles that they have to comply with. Therefore, ideally before things are due, but on an annual cycle that is definitely when organizations will retain us for services and assistance. All organizations really should be concerned with risk management and risk assessment. It does not matter what industry they are in. Risk is pretty universal in applicability so our services should be engaged at really any time. However, certainly smart companies are doing this, again, proactively rather than reactively, after, “Gee, a breach has just occurred, now what”; that type of a scenario.

CEOCFO: ***Do you see much movement in people being proactive?***
Mr. Peters: I definitely think that we have seen a significant uptick or increase in organizations looking for answers, looking for a better way, looking to get ahead of the threat. A few things that have occurred over the past couple of years; probably the Target breach about three years ago, that was the seminal shift, the big paradigm shift, in the industry. The reason I say that is because that was the first time that a corporate CEO of an organization lost their job as a direct result of a cyber security breach. There have been others along the past couple of years since then. However, cyber security has now risen to the board level, the very top level of the organization. It is now pretty universally identified as a business risk. The risk is real and there is not a day that goes by where organizations are not reporting breaches. To your point about an overwhelming head in the sand type of a situation; in the larger organizations we do not really see that so often. We do see it in the SMB space. Therefore, the small/medium business space and generally smaller shops are a little bit less knowledgeable about what needs to be done and what the threats are, even if they may be small to the point where the regulatory compliance demands are not really being enforced on smaller companies, like they are on the larger. However, they are no less still responsible for these things. Therefore, there is a lot of knowledge that certainly needs to be improved upon out there, awareness of what the threats are and what you do about it, but that is also why we do what we do. We advise our customers and potential customers. We have had long meetings with potential customers, just trying to help them get educated on what they need to look for. They may not always become clients, but we still try to do what we can to raise some awareness out there.

CEOCFO: ***With the long history of Lazarus Alliance and the experience, what might you find in doing an assessment that less experienced companies would not realize?***
Mr. Peters: There are really several things that come to mind. Probably one of the bigger items is that it is really a skill gap, a knowledge gap if you will. To give you an example, statistically the industry tells us that forty to forty one percent of organizations are doing risk assessments. In our business risk assessments are fundamental things that you should do. The sad thing is most of those are actually doing them incorrectly. The business of audit and compliance risk assessment, particularly risk assessment, is a very complex subject to begin with. It is not all about technology. It is also about the physical world; policies, physical security and operations. These are skills that are much larger, much more comprehensive than what a single technologist for a company might be skilled at or adept at or exposed to. Therefore, many times, because of the complexity, they really do not know what they do not know and they are basically missing the bigger picture. They are unfortunately on the Titanic and while they saw the tip of the iceberg, what is hidden underneath is ultimately what caused the problem. I suppose if there was an analogy, maybe that was a good one. However, I really think it is an expertise gap. Our advantage is very deep industry knowledge and experience, internationally awarded and recognized professionals who are all well credentialed. They do not get there without the appropriate training and the appropriate experience and things of that nature. Even if a company does not have that expertise, they can certainly retain it and be a heck of a lot better off for it. We also have the Cybersecurity 500 ranked IT Audit Machine (ITAM) which is our proprietary SaaS governance, risk, and compliance (GRC) platform. It is quite unique, loved by our clients, and that helps to sustain the work done over the long haul. You have to start somewhere and it is a great place to be when you finally arrive there. Cyber security, audit, compliance, and risk is a cyclical activity. The bad guys do not take breaks. They do not take holidays. They are always working to try to circumvent your controls to steal the essence of your company or do damage. We add tremendous value added because we remain vigilant for our clients around the world.

CEOCFO: ***How do you help with the basic information such as, “passwords should not be “password,” do not click on links, watch out for phishing and spear phishing”? How do you help a company pass that along to their workers so that on a very basic level they are at least doing their best?***
Mr. Peters: Part of my answer is in a review, if we are effectively auditing or reviewing an organization, it really does not matter what sort of regulatory or compliance framework we happen to be focused on, whatever is applicable for that business or it is just a risk assessment; pretty universally there are some fundamentals. The password, for example, is of course one of them that you mentioned among some others. However, part of that evaluation includes an examination of these controls. When we find gaps, we make recommendations for how to remediate those items. In some instances clients will retain us to help make those changes. It may be a training program, workshop or policy development. Even at a higher level many of the things we do are freely available on our website. Every week we have awareness content that goes out applicable to businesses, end users, individuals, detailing what is current in the threat-scape out there, what are

businesses faced with, individuals face with and with suggestions for how to avoid those threats. This is part of our outreach, our contributions to the global community. Those are some things that we do.

CEOCFO: ***How do people find you? How does Lazarus Alliance standout?***
Mr. Peters: There is a variety of things that we do. Obviously, marketing and advertising; that of course is always part of the mix. However, at the end of the day you are not going to attract recognition or you are not going to get new clients and people are not going to find you if you have nothing valuable to offer. What we offer and how clients find us is typically that they have a specific need. Maybe they have a regulation to comply with. Maybe they want to be proactive about cyber security so they want a risk assessment, etc. We have very specifically defined service offerings. If an organization is interested in being proactive about their cyber security, audit, compliance, risk and so on, we are easy to find. We target this niche and we work diligently to support our clientele. Our clients endorse us and provide testimonials and referrals and things like that. We are published in this space, in books, blogs and other industry materials. We are consistently recognized as thought leaders or industry leaders in our space. We have the right credentials that people will reference. Many times they are looking for something specific and there are certification bodies out there that maintain a list of all of the organizations that are authorized to perform a particular assessment. We are part of that community. As another significant difference here, we compete all of the time with other providers. Invariably we tend to earn the clients business because we work smarter and not harder. We have a wonderful platform that we use that is called ITAM, otherwise known as the IT Audit Machine. This is a SaaS platform that we conduct all of our assessment through collaboratively with our clients. It is drag and drop easy. It takes the complexity out of these very complex assessments and activities. It is great for sustaining the work that the teams do over the long term. It provides lots of automation and ease of use and things and our clients really, really like that! We have cutting edge tech, industry standard service offerings and much of this helps to reduce the price, the labor involved and the time to deliver it. We are agile, innovative, and collaborative which really resonates with clients out there.

CEOCFO: ***What has changed in your approach over time? How is Lazarus Alliance a better company today than two or three years ago?***
Mr. Peters: I could definitely tell you that as our unique technology and our methodology continue to improve, we get faster, more efficient, less expensive and more effective. Part of it is through gained experiences. Part of that is just the product and service life cycle. I'd be remiss if I overlooked the softer skills. We frequently hear that we have an excellent bed side manner, so to speak. The point is that a lot of assessment experiences with some of these big 4-6-8-whatever firms are that they are tend to be adversarial relationships in nature. As if their customers are going through an interrogation! It is uncomfortable, it is unpleasant, and it is all done with antiquated tools and ill-suited technology. The biggest tool out there is still the humble spreadsheet which is terrible for this type of work! It is one of the drivers for why we created ITAM to begin with. We like working smarter and not harder, and we have changed the whole paradigm for the industry. It enables us to build meaningful and collaborative relationships with our clients, instead of those traditionally adversarial relationships that really resonate. Let's face facts here; Customers are concerned. Businesses are being threatened. Many businesses are going out of business because of cyber security breaches. The common statistic right now is that sixty percent of small/medium businesses are out of business within six months after a breach. The stakes really could not be any higher. Business owners are already nervous. They feel like they are not prepared. They do not have much hope and they want to trust someone, so the last thing they need is some sort of environment that is antagonistic or not conducive to solving problems and developing a partnership. We have really been delivering on that for a very, very long time and that really resonates with our customers.

LAZARUS ALLIANCE IS PROACTIVE CYBER SECURITY™
IT AUDIT & COMPLIANCE - IT RISK ASSESSMENT & MANAGEMENT - IT GOVERNANCE & POLICIES
POLICY MACHINE
CYBERVISOR
YOUR PERSONAL CXO
SECURITY TRIFECTA
HORSE PROJECT
AUDIT MACHINE
POLICY MACHINE
CONTINUUM GRC