ceocfointerviews.com

Issue: January 21, 2019

CEOCFO Magazine

Q&A with Jim Libersky, President of Barrier1 using AI-Deep Learning to Block Cyber Threats within Sub Second Time protecting Organizations, Infrastructure and Individuals in Banking, K-12, Colleges, Ski Resorts, Electric Companies, and Government Agencies with Extreme Accuracy

Jim Libersky
President

Barrier1
www.thebarriergroup.com

Contact:
Jim Libersky
763-230-1041
jalibersky@thebarriergroup.com

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

CEOCFO: ***What is the idea behind the Barrier1?***
Mr. Libersky: The basic premise of Barrier1 is to solve the cyber problem. In other words, stop today's and tomorrow's cyber-attacks of all types, names and strains before they enter your network. Therefore protecting our organizations, infrastructure and individuals with extreme accuracy and speed.

CEOCFO: ***Would you explain how?***
Mr. Libersky: Early on we recognized that cyber-attacks are really based on a process. We break down the cyber events from 1. Those we have seen before and have fixes for and 2. Those we have not seen before and there are no fixes for. We take what we have seen before learn from them and then apply it to those cyber events that have not been seen before. Next, every cyber-attack has attributes. These attributes can be how they use a protocol as just 1 example. Barrier1 identifies these and puts them in context using AI-Deep learning. We then block them within sub second time. Our latest was from having an ethical hacker try and hack through. He was unsuccessful and Barrier1 blocked him in 12-20 microsecs.

- Here is the link to the article we posted for you:
- https://e-channelnews.com/ethical-hacker-gets-stumped-by-barrier-1-technology/

CEOCFO: ***Why can you do this and others cannot? What is that you have figured out?***
Mr. Libersky: Barrier1 can do this simply because we looked at the problem differently than everyone else.

Barrier1 figured it out that cyber-attacks are a process.

CEOCFO: ***What are you physically providing to organizations? Are people, in general, understanding the need for a physical component in security?***
Mr. Libersky: Barrier1 solutions are available in both hardware platforms and VM/Software platforms. Our Barrier1 hardware based "Intelligent Threat Management" platforms fit at the individual user level to a multi-location Fortune 500 type of customer. At the low end we have Barrier1 Mobil. B1 Mobil is an app developed for the Android smart phone and tablet market. Next is our Barrier1 Model 15. This is designed and priced for the SMB market. Third is our Models 50- 75. They focus on the mid enterprise markets. Next the Barrier1 model 100-200-300-300 scale up to large enterprise organizations. Last, Barrier1 cloud is a software VM version designed for a number of VM platforms. All of our platforms

will protect all vertical markets. As an example, we have banks, k-12, colleges, ski resorts, electric companies, government agencies, book store and others.
So, a direct answer to your question, yes all understand the need for cyber security. However, some value the protection or need to protect differently but it does touch everyone.

Viruses go back many years. Much like the networks at that time, they were simple and slow. As networks grew cyber-attacks grew and changed. Computer networks touch everyone and everything about our way of life. Computers and networks control our electricity and distribution, our personal communication, our banking, our manufacturing, our entertainment, and soon even our transportation. Networks are involved with everything including this interview because once finished with this on my computer, I will forward it on to CEO Mag. electronically.
Cyber-attacks have grown in complexity, sophistication and speed as well. What was once just an inconvenience or a few organizations and maybe individuals can now disrupt countries and societies. People are realizing they have to pay attention to cyber.

"Barrier1 can evolve as fast as the cyber criminals do without changing the hardware or system architecture. Thus, delivering a solution that is more Effective, Accurate, Faster and Affordable."- Jim Libersky

CEOCFO: ***How do you gain attention? When you are talking with a prospective client or someone is assessing Barrier do they understand the difference: Are people skeptical? How do you get the facts across so that people understand this is different?***
Mr. Libersky: Gaining attention is always a challenge. I think cyber is probably the most challenging. It is challenging because to many these cyber seems foreign and abstract. The very conversation can come with a lot of terms and concepts people might find difficult to either learn or understand. Second, cyber has over 20 sub markets under the umbrella of Cyber Security. Each one has a unique technology behind it but if someone just focuses on just one of those categories alone you will be hacked. One has to have a deep understand where you audience is in terms of understanding cyber-attacks. IT requires a conversation that will resonate with your audience. One of the real differences with a Cyber is that it is multidimensional. In addition, you have to prove your value or really the ability to identify and block all cyber-attacks. That will lead to trust and that will lead to greater attention.
Anytime there is a new process people are skeptical. However to solve the cyber problem you have to look at it differently. We had to bust a lot of myths. One of those myths is to get out of the mindset that you focus totally on 1 part. I constantly state that "people look to solve independent problems independently". In cyber you have a virus, spam, malware, APT, Trojans, DDoS. All with their own process. Then compound that with today's cyber-attack process are using parts of a DDoS, APT, and Viruses as part of the new wave of cyber-attacks and rapid change. In cyber that term is referred to as "Polymorphic Events" or rapidly changing. So, you really have to look at them all. An example is Trick Bot.

In discussion with prospects one first has to understand where the prospect is at in terms of education, understanding, technical awareness/understanding, need and overall risk. In short, what value do they place on their digital assets If you share how cyber-attacks are working and then your solution in their terms, people can understand the difference. I think the skeptical part comes in because they have been bombarded with cyber-attack information for years. To add to that, this massive information blast keep coming bigger, louder and more frequent. It seems that there is no end in sight. In reality people just want to be protective.
Everyone has either an opinion or experience of cyber. Generally when people are going through their due diligence and education they look for someone they trust. Since cyber is really sometimes complex and bizzar people rely on trust more than ever. Building trust is important. The hard part for people is cyber is changing so fast and innovation is coming from organizations that are new. The large organization they have heard of are no longer innovators. Thus we see large organization purchasing the same old solutions from the same large organization. It is these organizations that are showing up in the news paper are being beached. IN addition, in order to stop cyber in a holistic method, you have to bust the myths. It is these myths that established organization continue to hammer on to the public. All of this has to be taken into account so people will listen to a new set of facts, understand them and implement them. So, the delivery method and style is to bring a technical discussion down to a common understanding for each party. Then use examples. One of the examples I use from time to time is Football. I compare cyber to football and other sports.

CEOCFO: ***Are there particular industries of focus for the The Barrier Group? Do you find certain groups understand a bit better and are willing to make the choice?***
Mr. Libersky: Barrier1 focuses on 5 vertical markets. They are Government, Education, Finance, Health, Utilities.

Each group is at a different stage in the adoption curve. I rank the interest in cyber based on the value the organization places on digital assets. However, that is changing. The change is really the realization that building, factories, stadiums and etc. are run by networks. We had the opportunity to be at Levi Stadium for Super Bowl 50. Like all stadiums, it is run

by a network. Anything from the jumbo tron, ticket sales, POS systems, heating air, and etc. All can be compromised via a cyber-attack.

CEOCFO: ***How is business?***
Mr. Libersky: Business is good. We are replacing a lot of well-known brands simple because we show what they are missing and can react in real time with extreme accuracy. People are just now starting to understand and feel more comfortable with AI/Deep Learning. The quality of questions are always rising. Although being 3 generations ahead of the market can be tough. However, we were able to show for years that we had a better solution and that the Barrier1 solutions not only scaled but were able to stop new cyber-attacks without having to replace. That is important in building a brand.

CEOCFO: ***Do you find it personally frustrating that you can make such a difference and everyone is not jumping onboard?***
Mr. Libersky: Yes, I think all innovators feel that way regardless of their product market. I also understand why. Education is a key part of that adoption. The more complex or away from what is known the more education will be needed. IN cyber everyone was used to just being told "You have been infected by a…. Virus or malware". Not many look at how cyber-attacks worked.

CEOCFO: ***Then it is a good thing we have Barrier1?***
Mr. Libersky: Yes, and Barrier1 can evolve as fast as the cyber criminals do without changing the hardware or system architecture. Thus, delivering a solution that is more Effective, Accurate, Faster and Affordable.