Countering Cyber Threats

An Interview with Joseph J. Grano Jr.,
Chairman and Chief Executive Officer, Centurion Holdings LLC, and Premier Alliance Group, Inc.

EDITORS' NOTE *Joseph Grano was previously the Chairman and CEO of UBS Financial Services Inc. (formerly UBS PaineWebber). Prior to joining PaineWebber, he was with Merrill Lynch for 16 years, holding various senior management positions, including Director of National Sales. He is former Chairman of the Board of Governors of NASD and a member of the NASD's Executive Committee. He was appointed by President George W. Bush in 2002 to serve as the Chairman of the Homeland Security Advisory Council. He served in this capacity until August 2005. Grano holds honorary Doctor of Laws degrees from Pepperdine University and Babson College, as well as an honorary Doctor of Humane Letters degree from Queens College. Grano also served in the U.S. Special Forces (Green Berets), and he is the author of the book* You Can't Predict A Hero.

Joseph J. Grano Jr.

COMPANY BRIEF *Premier Alliance Group Inc. (premieralliance.com) is a leading provider of cyber security, energy, and business advisory solutions. Headquartered in New York City, Premier Alliance has been delivering results that improve productivity, mitigate risk, and maximize profits since 1995. Clients range in size from Fortune 100 companies to mid-sized and owner-managed businesses across a range of industries, including local, state, and federal government agencies.*

Centurion Holdings (centurionh.com) was founded in 2004 by Joseph Grano. Centurion has advised over 20 companies across numerous industries over the past ten years, helping companies grow from nascent stages of raising seed capital to becoming industry leaders. Centurion currently advises and owns equity stake in over 12 companies headquartered around the world, including New York, Seattle, Colorado, Toronto, and London. Their representative market sectors include technology & social media; security; "green" and sustainability; and technology transfer.

When you decided to lead Premier Alliance, what excited you about the role?

After leading UBS, I never imagined that I would get involved with a company trading below $1. Then I saw who was on the board. I asked Harvey Pitt, former Chairman of the SEC and one of the board members, what he was doing on the board. He said he had checked out the company thoroughly and was encouraged by its prospects.

After being there for six months, as non-executive Chairman, it became clear that the company had two value propositions: one in energy and one in business consulting with a focus on regulation, neither of which could be categorized as a growth engine and both of which had low margins.

In December, I convinced the company to buy a cyber-security firm. My biggest corporate and national security concerns right now are the vulnerabilities from the cyber side.

I interviewed several companies and found root9B to be the best in class.

They convinced me that U.S. corporations, as well as the government, have gaps in coverage and are seeking technologies to better defend their platforms and data. They further convinced me that if you don't understand the attacker, you can't defend.

We bought the company and the board of directors asked if I would be willing to lead it over the finish line. I agreed to become CEO primarily because I was impressed with the people throughout the organization and because it gave me the opportunity to contribute towards the defense of our nation.

What did you see in the company that made you feel it was a good risk?

The cyber-world has its own culture and you cannot underestimate the intellect of these people. There are three categories to be concerned with: state-sponsored groups, like those in China, Russia, and Iran; hackers themselves, who can be segmented as well; and disgruntled employees.

This group, root9b, has true subject matter experts as its leaders, mostly from the NSA, who understand the attack side because, for the government, they were tasked with protecting us from multiple adversaries.

They do a vulnerability assessment like anyone else, but they drill deeper into your source code. They will tell you that you need, in many cases, your own customized tools to combat your vulnerabilities, and those tools are expensive and unique, and you need to have that experience to create them.

The company is doing that and we are in front of some major corporations. We are training the Air Force, and members of the NSA and Homeland Security. We are close to cyber-command. What makes this unique is that when we are training an officer or programmer from the Department of Defense, they come in and say, we have just found a new attack. What do we do to counter it? So we stay ahead of the learning curve, based on our connectivity with government.

The point I would make is that anything is penetrable in time. Anyone who thinks that they don't have to worry because they have a firewall is wrong.

When the SEC went out to companies asking questions such as if they were PCI compliant, I called them and introduced them to root9B because I care. I wanted to show them what to look for and what questions to ask.

We created a virtual investment bank in 15 minutes. It blew them away. I'm going to do the same thing with FINRA.

Our guys truly understand the mentality of the attacker and they don't underestimate his or her intellect.

Is the target market solely large global institutions?

The solutions are very human-intensive – there is no do-all automation. This means your subject matter experts can only handle so many clients. I'm targeting the largest corporations, governments, and municipalities out there. I am told there are approximately 35 journeymen who would be considered experts – seven of whom work in this company and we project it will be 12 by the end of this year. No one else has been able to amalgamate that level of talent in one place.

How high up does that relationship need to be within the corporation to be effective?

In the pit of their stomachs, every board and every CEO has concerns about regulation, cyber, and social media.

Twenty years ago, in more cases than not, you would have a seasoned experienced business person as head of an audit committee in a public company. But because of what has happened on the regulatory side, businessmen and businesswomen now understand that it's difficult to do that job unless you are on site at least a few days a week.

So that function is being replaced by prominent men and women from academia. They are forced to rely on internal and external auditors. However, with the new regulations and the cyber threats, the head of the audit committee inherits a whole new level of influence and responsibility. If he or she walks into the CEO's office and wants to hire root9B to ascertain vulnerability and create a defense, the CEO is more than likely going to say yes.

A corporation's intellectual property (IP) today is probably 60 to 80 percent of its overall value. So you have to protect it.

Many equate Premier with financial services, but isn't it much broader?

Absolutely, in terms of the utility industry in particular. There were 150 cyber-attacks last year against utilities. Those are attacks on the power grid and this is a basic element of defending the U.S. It's also critical that any institution that ultimately gets access to your identity and your bank account protects itself in the best way possible. It's a much broader issue and it's multi-industry.

How extensive does your investment in training need to be?

We believe we are the only integrated cyber-security firm that provides unique, in-depth training, which is a differentiator. We're training the specialists for many national agencies.

The package includes vulnerability assessment, PIN testing, and a mitigation strategy. Not only do we train an entity's top 10 people who need to have this expertise, but we will come back every six months and update them.

Does this mean you're not a threat to the IT people in companies but rather a partner?

Yes, because if you come in bottom-up, the Chief Technology Officer may believe you're going to put a target on his or her back. They fear that the CEO may want to know why the CTO didn't know about the firm's vulnerability.

The appropriate entry-level is at the C-suite, where you partner with the CTO and the head of the audit committee in evaluating the system. You want to make sure that the firm understands their attackers. Most of our systems professionals were never trained for defense; they were trained to create code and to process transactions. Robert Mueller III, the former Director of the FBI, recently stated that there are two kinds of corporations: those that have been hacked and those that are about to be.

How far can the safeguards go and is this about mitigating the damage or preventing it?

It's both. Corporate America is going to have to spend more money than it is spending on this defense. If you step back and determine the intrinsic value of your company, you will find the vast majority of it is IP.

So a higher percentage of your revenues are going to need to go toward protecting that IP, and protecting your clients and their identity therein.

How do you measure success in these efforts?

Is it any different than with an insurance policy? You have to think about it from a preventive perspective and protecting the assets of the corporation. When you have state sponsors like China attacking and trying to steal your IP – and they are – you have to monitor it and fund it at an appropriate level to get adequate protection.

It will require a higher allocation because we need to apply a higher level of expertise. It starts with a different approach in recognizing that you can't defend if you don't understand the attacker. Target was PCI compliant when attacked and was penetrated through the HVAC system. I am quite confident that in retrospect, they would have gladly funded additional mitigation strategies.

Corporate America is going to have to spend more money than it is spending on this defense.

Did this venture require a lot of learning on the job for you?

After 9/11, the old uniform didn't fit. Thank goodness, President Bush tapped me to be Chairman of the Homeland Security Advisory Council so I could contribute to the defense of our nation.

In that Council, we were looking at different vulnerabilities and we interviewed multiple think-tank groups – one group told us that we're all looking at the interdependencies above ground, but no one is looking underground. I gave them Manhattan and Charlotte to work on and you would have been surprised at how vulnerable we were under the ground.

As I got into this space and became more aware of the vulnerabilities through my interaction with this group, I went through a learning curve, because I'm not a subject matter expert, but I know that at Premier we have the best-in-class in terms of subject matter expertise, and that is a differentiator I can proudly associate with.

Has true change occurred on Wall Street and has enough been done to safeguard against another recession?

A lot has been done, but on a regulatory front, it's been an overreaction and is probably causing more harm than good.

You get to a point where corporations don't invest in growth because of uncertainty and lack of clarity.

There has been consolidation with the commercial banks primarily, so the bulge-bracket firms, as we knew them, aren't there anymore.

Also, the markets have become much too fragmented. The worst thing that happened was when Elliot Spitzer's foolishness cost us Dick Grasso, the leader of the industry, and the best advocate for the quality of markets and the protection of the individual.

In the banks, the tier 1 capital positions are much better but I don't believe they're lending enough. If you ask me what the problem is today versus 2008, it's the government and its lack of cohesiveness, leadership, and clarity. We're getting slam-dunked on a foreign policy front. Corporations are reluctant to invest in their own businesses because of the lack of clarity and overregulation. Look at what is happening with the fines. What was a $500-million fine in the past may now be $9 billion. Everyone is raising the bar and that causes a shake-up in confidence. Plus, there are now criminal indictments, which they never had before. It's overkill.

Do you often reflect on your accomplishments or are you always looking for the next challenge?

When I'm climbing the mountain I struggle like most people, but when I get to the top, I look down and say it wasn't bad, where's the next mountain? You need ambition and goals, always. What motivates me are those four interns sitting in that conference room that I'm helping to understand the real world, or getting 1,000 employees to drink the Kool-Aid to help improve their business as well as their lives.

It's psychic income, not dollar income, and the best leaders thrive on psychic income. That's the differentiator between a good leader and a great leader. A good leader has to be a good manager, and not all good managers are leaders. Great leaders have an intrinsic respect for the individual and are driven by psychic income. That passion for people is key – the interest in helping improve their lives.

When it comes to running a public company, you have three partners: the shareholders who subsidize the business; the clients you choose to serve; and the employees. Every major decision has to be fair and equitable to all three. If you overly favor one partner, you conversely are stiffing the other two.

It's not an issue of popularity, but if each partner can say, that's fair, then I know I have done the right thing. ●