ceocfointerviews.com

Issue: May 16, 2022

Conquest Cyber: Providing cyber resiliency to America's critical sectors

Jeff Engle
Chairman & President

Conquest Cyber

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

CEOCFO: ***Mr. Engle, what is the overall vision behind Conquest Cyber and what are you focusing on right now?***
Mr. Engle: The overall vision is to achieve cyber resiliency for the sectors critical to our way of life. As we are seeing play out on the world stage, our critical infrastructure sectors, which includes everything from the industrial base to healthcare and financial services, energy, oil and gas, and others, are in danger. Those sectors are now being more consistently leveraged in an ongoing geopolitical conflict. Those sectors, along with global connectivity provide a way to harm Americans on US soil, without having to escalate to full scale military conflict. It has hampered our ability to protect our friends and allies and project power around the globe. Therefore, our view is that critical infrastructure sectors have become the new frontline for freedom in this hyper-connected world.

Our organization was established in the recognition that the US government was not going to be able to protect the hundreds of thousands of organizations that make up the ecosystem that enables our way of life, and would need more mobilization from private sector, via public/private interactions, the cyber security, cyber resiliency industry and the organizations themselves.

CEOCFO: ***What is your approach to protecting people and companies?***
Mr. Engle: Our approach is really demand generated. We have found that different sectors, from the largest most well-funded government entities down to the small community banks, were having a consistent problem. The challenges that are known lack skilled resources. A lot of transitions are happening at an incredible pace. Cyber security talent, engineers, IT, and risk people move jobs frequently but the speed at which that is happening has become a national security challenge. Then, there is a reality that the adversaries are consistently focused on us, and we typically only have defenders in place during working hours. Those are the problem statements that I think are the most recognized. The bigger concern are the challenges that go unrecognized.

When we looked at it a little bit deeper, we found that when it comes to building a solution for those problem statements there were a couple of key needs. The dots needed to be connected for the operators of the program. For example, we needed to connect the risk analysis activities to what is happening within security operations and general IT operations management. Similarly, we need, as an ecosystem, to connect things like compliance standards to the actual objective of that compliance standard as an overlay to good cyber posture and hygiene, rather than just treat compliance as an objective in and of itself. Therefore, connecting those dots for the operators and making sense of what they were doing was a critical portion of our approach. The second part of it is providing transparency and context to decision makers.

Ultimately the risk executives, the board members; they are the ones that are responsible for maintaining their business risk analysis, which includes cyber as an element, and managing that in alignment with their fiduciary responsibilities. Up to this point, they have not had the context needed to really execute on that.

CEOCFO: ***Do you see board members, in general, becoming more aware of their responsibility, taking it more seriously, or is it still where people know breaches exist, but throw up their hands?***
Mr. Engle: I think that we are on the front edge of the wave that is driven by a couple of different dynamics. One, is simply what is happening in the world, and the other is the regulatory environment shifting to a more aggressive posture on holding them accountable. However, we are still on the very front of that wave, where the vast majority have not changed their approach to taking a more in-depth, hands-on path to understanding their cyber risk in relation to business risk.

SafeRX Pharmaceuticals

It has been typically sourced by their existing board teams, where they say, "Now you three are part of the cyber committee," rather than bringing the necessary expertise into the board with a seat at the table. Therefore, do I see a positive trend, both from government and from recognizing that cyber risk is business risk, and ultimately the boards responsibility? Yes. However, I do not think we have seen an aggressive push towards the "not necessary" knowledge skills and abilities to be able to manage risk at board level or placing it as a priority that would rival things like PNL reporting.

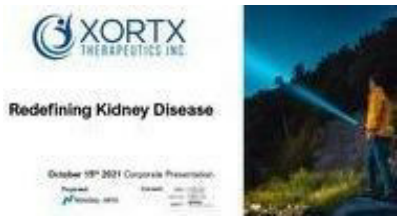
There are positive trends, but I think we have a long way to go. Unfortunately, there is not enough downside risk for a board member if they do not prioritize their responsibilities overseeing the cyber security programs in their organization.

"The overall vision is to achieve cyber resiliency for the sectors critical to our way of life. As we are seeing play out on the world stage, our critical infrastructure sectors, which includes everything from the industrial base to healthcare and financial services, energy, oil and gas, and others, are in danger." Jeff Engle

CEOCFO: ***Would you tell us about the different solutions you have available? How do you work with your clients?***
Mr. Engle: We provide an integrated cyber resiliency platform, and ultimately enable that platform, based on the customer's vertical that they operate in. In some cases, we will see customer organizations having a fairly robust internal capacity, and we may co- manage their environment and augment it with our integrated cyber resiliency platform. In other cases, they are very nascent, and we can go in and provide our platform, and help them understand where they are today in relation to where they want to be, and work incrementally towards achieving cyber resiliency as an organization.

In the traditional IT cyber security world, what our platform does is cyber posture management, compliance management, attack service management, managed enhanced detection response, third party risk management, and ultimately connects all of those different capabilities together in a way that makes the insights actionable, provides that context to decision makers, and connects the dots for the operators of the program, so they can prioritize the right things.

CEOCFO: ***The Conquest Cyber site offers 2 solutions: Armed and SCyOps. What are the differences and who might be using either of those services? What types of companies?***
Mr. Engle: Armed is designed for federal clients in the defense/industrial base. It is aligned to the National Institute of Standards and Technology's standards, for both risk analysis and for underlying frameworks to organize the data. SCyOps, on the other hand, is designed for all of the other critical infrastructure sectors. The way we approach risk, the underlying platform that it is hosted on, the compliance standards that it is aligned to; all of those elements between Armed and SCyOps are different. However, the underlying approach to integrated cyber resiliency within the two platforms is the same. The different versions and branding just provide greater contextualization and different approaches to compliance, risk analysis and prioritization of threats.



XORTX Therapeutics

CEOCFO: ***Where do you see the greatest weaknesses in protecting from a cyber threat? Are there certain areas that people just seem to miss more than others?***
Mr. Engle: Yes. I would say that understanding the assets that are on your network, and how those assets impact your attack surface is both the first step and the one that is the most challenging for most organizations. Though maintaining an accurate asset inventory for software and hardware, understanding what is actually on your network in relation is what is supposed to be on your network; that is a difficult task for even small organizations.

It becomes nearly impossible, the way that we, in industry, have been trying to do it up to this point. We have to start thinking about assets in the broader spectrum, not just physical assets, laptops and things of that nature, when you get into data assets, that is an element that is critical.

That sprawl that happens makes it really difficult to maintain an accurate attack surface management program, understand your system boundaries, and where your communication and data flows ultimately can escape to in the event that there is a nefarious insider, an adversary gains access to your systems.

CEOCFO: ***How do you reach out to potential clients? What do you understand about working with the government?***
Mr. Engle: The way we engage our clients is typically through industry groups, direct engagement with our alliance partners, we have a number of technology alliance partners, and the going directly to those technology leaders who have security responsibilities through direct outreach. The way that we have a unique capacity relation to the government is that most of our leadership team has a significant amount of experience working with the government at all levels. I was an acquisition program manager, trained in the Department of Defense, and spent my formative years in special operations.

Most of our leadership team either served in the military and ultimately in some element of an acquisition or R&D role or worked directly with the government for a number of years, at the federal DOD state, local, and education levels. Therefore, we have a great deal of experience in identifying the right contractual mechanisms and navigating through the government regulations. We do that, both directly with the government and indirectly by helping our clients, who are highly regulated giving them a lot of risk exposure to government requirements, navigate through those processes and ultimately enhance their business outcomes.

CEOCFO: ***Do you work with MSPs as well, or through MSPs, or is it strictly one on one with your clients?***
Mr. Engle: We work through channel partners. Many of them are managed services providers that provide things that augment the cyber resiliency program and provide services such as patch management and penetration testing, and vulnerability management. Being that we are an integrated cyber resiliency platform company, there are many things that we could do, but it would cause us to merge over to being more of a hybrid services provider. In those cases, we work with our partner ecosystem to be able to augment any of those underlying capabilities that a client needs to achieve their cyber resiliency objectives.

CEOCFO: ***How is business at Conquest Cyber?***
Mr. Engle: Business is great! Obviously, there are impacts from Russia's invasion of Ukraine, the public recognition that our critical infrastructure cyber security are in need of help, and that those sectors are going to be attacked by advanced adversaries, even if it is not for our full-on war, as a geopolitical tool.

We have seen an uptick in urgency from our critical infrastructure sectors that otherwise only becomes urgent when you see the government take significant action towards more regulatory oversight and accountability. Therefore, both things happening at the same time, the defense industrial base getting hit in the CMMC 1.0 and then 2.0, as well as, the critical infrastructure sectors being publicly exposed as a target to our nation's data adversaries, have both driven demand for the offering that we specifically provide.

CEOCFO: ***What, if anything, has changed in your approach over time? What have you learned?***
Mr. Engle: Over time, we have adjusted our primary customer target. Most cyber security organizations sell to security engineers, so those are the ones that are expected to be the buyers that are evaluating tools and capabilities against other items that they have purchased. Therefore, we have changed our buyer personas to being security leadership, where they see the value in eliminating unnecessary technology sprawl, simplifying their architectures, and maximizing the automation.

Ultimately, they are the ones that have to manage the risk, and they get much more bang for their buck by having a technology stack that is seamlessly integrated, than buying all the technologies with individual capabilities that might be best of breed. That is why best of breed outcomes is what we are driving towards, and I think that is what our buyer personas are looking for, whereas the traditional security buyer is looking for best of breed individual technologies, and that really does not enable the management of that attack surface the way it needs to be done.