martinwolf

Executive Perspective®

Unique Viewpoints from Industry Leaders

June 2017

Rich Fennessy

CEO, Kudelski Security

Editor's Note: *Rich Fennessy is the CEO of Kudelski Security, where he leads the global cybersecurity business. Rich has a proven track record as a successful Fortune 500 CEO with 30 years of international management experience in the technology industry. After 17 years at IBM, where he held various sales & marketing executive roles, he has been a successful President and CEO of several technology companies. Most recently, he served as CEO of Fishnet Security, one of the largest providers of information security solutions in North America.*

When we last spoke, FishNet had just merged with Accuvant. Today, the company is Optiv, and it notably was acquired by KKR shortly after filing paperwork to explore an IPO. What are your thoughts on the company today?

Optiv continues to be a strong company with a large client base and a great group of people focused on supporting their customers.

How has IT security evolved since we last spoke? What new challenges are we facing?

The adversaries of enterprise security continue to increase in both numbers and sophistication. Despite record high investments by client organizations, and an amazing array of new products and companies addressing various cyber challenges, we don't seem to be making an impact. Organizations are under constant attack, breaches are harder to detect and risks are as high as ever.

The fact is, what we are doing today as an industry is not working. The bad guys are winning and causing pain to our global economy. It's time for a new approach, a different paradigm in the fight to protect our companies.

When I say that things are not working today, you just have to open up the newspaper to see what I mean. Every day you see new breaches from the largest brands and governments around the world. And this is all happening, while at the same time 83

billion dollars is being spent on new technologies and services to prevent and detect breaches.

Again, something must change, especially with our ability to reduce the amount of time between breach and detection. This new approach to cyber security that truly challenges the status quo is what we are focused on delivering to the clients of Kudelski Security.

What are the potential implications or effects of the cybersecurity climate on today's enterprises? Are there added precautions that CEOs and business owners need to be aware of?

Business leaders – not just IT – need to understand the threat landscape and realize the business implications associated with managing cyber risks. Business leaders need to keep security in mind as new applications, services and business strategies are deployed, and ensure that appropriate planning and investments are made to minimize risks as much as possible.

"We have to also focus on translating highly technical plans into outcome-oriented business decisions."

As security professionals, we also need to do a much better job in communicating to our peers across the business what cyber risks require the focus of the business. We need to set up security programs that can be described in business terms, and we need to create measurements that highlight our actual preparedness in a way that business leaders and boards of directors can understand and appreciate.

Security control frameworks like NIST and others provide some levels of management and measurement, but translating this to the business in a meaningful way is a challenge, and these frameworks are typically manually managed which chews up a lot of valuable manpower. One of our focuses has been to create a new approach to building a security program – which is called Secure Blueprint – that works with all the viable control frameworks, takes into account important business parameters, and can be rapidly updated to easily measure and show the current state of a security posture. Always with business context in mind.

The famous statement about you can't manage what you don't measure is absolutely applicable. But with the complexities associated with enterprise security, we have to also focus on translating highly technical plans into outcome-oriented business discussions.

Tell me about Kudelski Security. How has your past experience shaped how you approach your role as CEO?

As I mentioned earlier, Kudelski Security is focused on challenging the Status Quo of cybersecurity. We are the cybersecurity division of the Kudelski Group, which is a Switzerland-based organization that for over 65 years has been applying Swiss engineering and expertise to produce market-changing innovation.

"We need to address old problems in a new way."

I was hired in 2015 to take a Switzerland-only cyber business and transform it; reshape the focus and build it for scale to ultimately be a global solutions provider and recognized leader in the industry.

The result of this transformation is a business that combines world-class consulting, technology, managed security services, and innovation to minimize the risks and ultimately help protect the businesses of our global client base.

As for my past experience, it is all coming to play in this new venture. I think the combination of strong IBM management roots, combined with the entrepreneurship I learned from running IBM.com and several startups, along with the experience gained by leading one of the United States' premier security solution providers (FishNet Security), all helped me shape a strategy that is designed to challenge the status quo.

We need to address old problems in a new way. I think my background helps me understand what we need to do, and the great team we have at Kudelski will help us to successfully deliver on our strategy with our clients. At the end of the day, we are trying to help clients be more secure. We have lofty goals, but I'm confident in our approach.

How is it operating as a division of a Swiss company? Is the Swiss management culture different than the American management philosophy?

Being a part of the Kudelski Group has been a fantastic experience. As you know, the Group is publicly traded on the Swiss exchange and has about one billion dollars in revenue. The company views cybersecurity as a key part of its long term success and has been very supportive of the investments we need to make to execute on the strategies we have put in place. The company is well run, profitable and, with its deep engineering roots and history of innovation, has assets in talented people, facilities, and technical expertise that are huge advantages to us. Unlike the startup mentality, we're afforded the luxury of a company that is willing to take a long view – focusing on how we can make an impact on the industry and establish a market leading position.

"Unlike the startup mentality, we're afforded the luxury of a company that is willing to take a long view."

Today, enterprises of all kinds are incorporating the cloud and turning to the Internet of Things. What cybersecurity implications does that carry?

We have spent a tremendous amount of time over the past year on both cloud security and IoT. It is clear the cloud is here to stay, which has tremendous implications on how cybersecurity is engineered, operated and managed. We work with clients everyday on strategies to secure applications, data and assets that exist in a new paradigm that includes a mix of on-prem, private and public clouds. We're also working with our manufacturer partners on business strategies for selling, provisioning and supporting cloud based services. We believe, with our specific skills, we're in a position to provide value to both constituents.

As for IoT, this is a huge focus for both Kudelski Security as well as the Group. Earlier this year we launched the Kudelski IoT Security Center of Excellence, which applies our Advanced Labs and Cyber expertise to assist our clients in architecting secure IoT solutions. It is very clear to me that security is an after-thought today for many IoT device and platform providers.

As an example, we will be launching in the fourth quarter a security chip that we have developed, that has a very small form factor and very low power consumption, that is perfect to include in IoT devices. We are currently working with our clients to embed this security chip into their IoT product roadmaps and expect this to be a growing part of our business in the future.

Again, our focus is to design Security in on the front end in the next generation of IoT devices and platforms.

How has the business climate changed since we last interviewed you in 2014?

There continues to be a strong appetite for investment in the industry – in new products, companies and ventures. And I think business leaders are more focused on the risks facing their organizations. Big breach data losses and massive ransomware attacks have captured the attention of organizations and driven the need for change, a new approach.

This creates opportunities for companies like Kudelski Security, but as stewards of cybersecurity, we need to be hyper-focused on helping make sure clients have a comprehensive view on what it will take to increase enterprise-wide security.

What is your M&A philosophy at Kudelski Security?

"So far we've focused on acquisitions that add critical talent in key geographic regions."

So far we've focused on acquisitions that add critical talent in key geographic regions. We acquired Milestone Systems and added over 100 people in the North Central and Southeast U.S. In January of this year, we acquired M&S Technologies, which added 50 people and some very strong client relationships in the TOLA (Texas, Oklahoma, Louisiana, Arkansas) region.

Looking ahead, I can envision additional acquisitions that either launch us in strategic geographies or add to our technical capabilities.

What geographical areas have the biggest growth potential for Kudelski Security?

We are very much a global organization and support clients today throughout EMEA, Latin America, and the United States. With this said, we will continue to grow the resources and strengthen the capabilities we have within each of these three regions, as well as potentially extend our focus to Asia Pacific overtime.

What's a piece of advice someone gave you that has stuck with you throughout your career?

Growing up within IBM, I learned that success in business is based on having clarity in direction and outstanding people leading strategy into execution on a daily basis. Great businesses are built by having great people. I am fortunate to have a great team within Kudelski Security that share a collective vision of making the world a safer place.

"If you are not learning every day, then you are not moving forward."

You're the first executive we've interviewed twice for this piece. Are you continuing to learn new things in your career? How is the Rich Fennessy of 2017 different than the Rich Fennessy of 2014?

I am a firm believer that if you are not learning every day, then you are not moving forward. Over the last three years, I have focused a lot of my professional learning on understanding the evolution of the cybersecurity landscape and most recently on identifying ways to approach the problem, differently. As I referenced earlier, change in our industry is required and it's fun to be on the front end of delivering that change, globally.