PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

SHANNON RAMSAYWAK

CISO, KIND

HEADQUARTERS: New York

EMPLOYEES: 800

ANNUAL REVENUE: $727 Million

"Security was one of many risks to the business the board identified, and made it a point for the business to address. So, it was clearly a board-sanctioned directive to start a security program."

- SHANNON RAMSAYWAK

OFFENSIVE TO DEFENSIVE SECURITY

A little over two years ago, Shannon Ramsaywak undertook the first-ever role of CISO at KIND, the healthy snack and granola bar company based in New York. Two pivotal things drove Ramsaywak to join the rapidly expanding organization – building a program from scratch and the full support of KIND's board. Ramsaywak says, "Security was one of many risks to the business the board identified, and made it a point for the business to address. So, it was clearly a board-sanctioned directive to start a security program."

In an incredibly brief period of time, KIND successfully expanded their global footprint and significantly grew their product offerings, yet lacked an established security program. He says, "I was brought in to bring the business from an all offensive approach, to expand and include a defensive cyber strategy. KIND grew so large, so quick because it was mainly concerned with growing the brand. However, after achieving such high growth, we found that we had many imitators and aggressive competitors we had to fend off. My role was to provide them with the defensive strategies they previously lacked."

During the interview process, Ramsaywak shared his thoughts on what type of data he planned to protect at KIND. He answered with a clear-cut description of five levels of data, as he sees it. He explains, "The first level is open data such as sharing our latest bar with the public. Second level is internal communications. Third is sensitive corporate information such as stock valuation. The fourth level is regulatory, so anything that requires a mandate or law like PCI or HIPAA. The fifth level is the formulas of our bars, including our supply chain, from the initial purchase to our end product. That's very sensitive, so those are the things that we're looking to protect most."

BUILDING BLOCKS OF A SECURITY PROGRAM

Ramsaywak's first phase of security initiatives was the "black and white" phase, addressing the most critical items. He determined the risks to the organization, then discovered the risk exposure level. These levels included critical, high, medium, low and very low risk. He next approached the business and laid out the risks, and how they correlated to a specific risk exposure.

"What's your risk tolerance posture? Are you risk adverse or are you risk tolerant? Once we found that, we married those two ideals into how we remediate. The very first directive I got from my boss was that we are very open when it comes to our user-base and our team members going to the internet and using tools to collaborate. But we are extremely risk adverse when it comes to the things that matter most to us," explains Ramsaywak.

He says, "Segregation, segmentation, antivirus, endpoint protection, firewalls, VPN, all of the black and white stuff is complete." He originally anticipated the first phase to take up to three years, but due to diligent work and board and C-Suite support, completed it in two.

The next phase for Ramsaywak includes transforming a security operations and security hard-line approach into a risk program. He comments, "Last year, we started the risk program and we're doing an assessment of all the departments and systems. We started with our critical departments, our New Product Development (NPD), HR and Finance departments."

UNDERSTANDING COMPANY CULTURE

The dynamic, young culture at KIND represents a "plugged in" workforce, who work off laptops and mobile devices. Ramsaywak realized it would be challenging to protect his employees and company data in this type of environment, which is a stark contrast from the highly risk adverse and "locked down" state government agency he came from. He explains, "What I had to do was understand the culture and then take a step back from the technologies. I had to come up with a concept of protecting the organization while still allowing the organization to keep its' ethos of the way it does business. And in that, I discovered that everyone wants to collaborate in real-time around the world which means work in the cloud, Google Docs, Dropbox, etc. It's not really the idea of Google or Dropbox, it's the idea of a tool that people can use anywhere to transfer information and get things done instantly."

After an initial discovery phase, Ramsaywak began to build out concepts to fix and enable, without limiting his employees. He comments, "I needed the concept to solve the issues the company had, and do it securely, so it wasn't a matter of coming in and implementing only what I knew. I think we have to allow ourselves to grow and be a little bit vulnerable in order to be better and to deliver better to the organization."

Not only did Ramsaywak implement policies and technologies that properly aligned with the company culture, but he started a heavy security awareness training campaign. Beginning with executive support, he achieved buy-in by emphasizing the criticality of their users being more educated and better aware. He says, "Our awareness program paid off in dividends because our end user infection when I first started was 6.7 a month, out of a group of 400 people full time and another 400 part time. Our infection rate has dropped to .15 a week or .5 per month. So, we've dropped from seven people per month to one person every two months."

Ramsaywak continues, "Focusing on where you have the greatest needs, whether it's your end user, your configuration or your vulnerabilities is very important. I found focusing on the end user in this day and age, with everything being open and bringing your own device, is one of the most effective ways."

FOCUSING ON FUTURE GROWTH

Once per quarter, Ramsaywak participates in an Enterprise Risk meeting along with the CEO, COO, CFO and General Counsel. He provides valuable updates on progress within their risk program, and continues to align himself with key executives. They also discuss plans for growth and how security plays a role in vital initiatives.

Building out his program to ensure it keeps pace with growth goals set by the organization's leadership is imperative to Ramsaywak. He comments, "As the organization grows, we're growing with it. The company has grown by at least 40 percent since I've gotten here. KIND has a very aggressive goal by the year 2021 and I have already built out what my organization will look like for this year and then next year and the following year in order to enable the business to achieve its goals."