PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

FRED KWONG

CISO, DELTA DENTAL PLANS ASSOCIATION

HEADQUARTERS: Chicago, IL

EMPLOYEES: 44

ANNUAL REVENUE: $23 Million

In all aspects of the security program, I am looking for synergies where a security investment makes sense not just for DDPA, but also for Delta Dental companies. I call this modular security. As I build out our security programs, I want to have every single security component available for our member companies.

- FRED KWONG

MODULAR SECURITY PROTECTS BRAND REPUTATION

Fred Kwong is 18 months into his role as Chief Information Security Officer for Delta Dental Plans Association (DDPA). He is the not-for-profit's first CISO and is tasked with managing security operations for the association, protecting the Delta Dental brand identity and driving security standards across DDPA's national network of 39 independent companies.

With independent companies functioning under the Delta Dental brand, sharing security standards and best practices is a critical part of reputation management. One of Kwong's main priorities at DDPA is to build out security programs that may be replicated and leveraged by the Delta Dental companies at low costs, and with limited resource investment.

"In all aspects of the security program, I am looking for synergies where a security investment makes sense not just for DDPA, but also for Delta Dental companies. I call this modular security. As I build out our security programs, I want to have every single security component available for our member companies. They need to be able to take advantage of our programs and implement systems without any heavy lifting in terms of technical expertise or financial burden. To do this, I am working with vendors to provide synergistic mindshare across the system."

Kwong says, "For example, we needed a vulnerability management program for the association. While we implemented this first at DDPA, we also completed a

THE CYBERSECURITY SKILLS GAP

"I have a small team at DDPA, there are only two of us dedicated to security within the association. The rest of my team is located at our MSSP. My security model is all about modular security. Our programs need to be able to support Delta Dental across the nation. That cannot be done if we rely on a large internal team, because security expertise is in high demand.

There is a real shortage of proper skill sets in security today and it is difficult to hire and retain appropriate skills. With the MSSP model, Delta Dental companies do not need to worry about hiring and retention of security staff. Our MSSP takes on that burden for us."

template for standing up vulnerability management at Delta Dental companies. We give them everything they need – a pricing model, properly vetted products and access to a MSSP."

He continues, "Some Delta Dental companies are very small with only four or five employees, others are quite large. For smaller companies, I provide more counsel and advice, whereas with the larger organizations, I partner with their internal staff."

ALIGNING RISK MANAGEMENT WITH STRATEGIC OBJECTIVES

Kwong's overall effort at DDPA is focused on ensuring his security program aligns with the association's strategic pillars.

To align the security program with these pillars, Kwong takes a quantitative approach to risk management via a business impact model. In his first 90 days at the company, he listened to the security challenges and concerns from other executives in the association and at the network of companies, and he performed an internal Gap Analysis. From there, he worked to deploy the risk management strategy.

"With the help of our CFO and General Counsel, I now have a plan to decrease risk to the organization. With this model, we can correlate risk to goals. If these are the areas where we want to decrease risk, then this is what we must prioritize. We have a three-year roadmap with a goal of reducing risk year-over-year."

As part of the business impact model Kwong and his team focus on the following six risks:

1. External threats against business partners and members
2. External threats against DDPA systems
3. Malicious actions by trusted parties
4. Social engineering against employees
5. Unintentional data loss
6. Ability to react quickly to incident response

He explains, "We correlated these six risks back to our business goals, the strategic pillars. Now, each security project we put in place has a correlation to the amount of risk we are mitigating and how that impacts the business. We define the success of the program by the decrease in severity or likelihood that an incident will occur in the future."

Kwong notes there will always be inherent risk in doing business. He says, "CISOs struggle with risk management. It might be because we do not all come naturally to risk. Many of us have compliance or technical backgrounds instead. The other problem is that the risk models available to us are not very good. Most are flawed in the ways that they account for risk, some are missing threat intelligence or they are not taking proper account of other areas."

He believes risk management is an evolving area for CISOs. "I was on a CISO panel with three other CISOs last year to talk about risk management. Each one of us had a different methodology in terms of reporting risk. My model was the most quantitative in nature, other models were spotlight models at a high level. We were able to agree that it almost does not matter what model you use, as long as the Board understands it and as long as it provides the information the Board desires to know. I think that as Boards become smarter about security they are going to want to understand risk in a more quantifiable way."