BRINGING A

Concierge Approach

TO CYBER RISK MANAGEMENT

If it works for the body, why not business?

By Dave Willis, CPIA

"If it works so well in medicine, why couldn't it work for cyber risk management?" That's a question Kurt Suhs asked himself a few years back as he was helping to manage his mother's healthcare. "The physician group my mom had been seeing for some time shifted its approach to delivering care to its patients," he explains. "The group went from being a traditional practice to become one of a growing number of providers to adopt a new delivery model called concierge medicine."

Sometimes referred to as retainer medicine, concierge medicine is simply a relationship between a patient and a primary care doctor—or in his mom's case, a group of doctors—where the patient pays an annual fee or retainer. In return, the practice agrees to provide enhanced care, and often commits to limit its patient load so it can ensure adequate time and availability for each patient. Some agreements cover basic primary care office-based services; others offer extra benefits in the agreed-upon price. The approach has proved to result in positive outcomes for both patients and physicians.

Suhs's experience with concierge medicine formed his vision for a new delivery model for cyber risk management, which today exists as Concierge Cyber®. Here's how it works: "In return for a set annual membership fee, my firm provides businesses and individuals guaranteed quick and easy access to cyber risk resources," explains Suhs, founder and managing director of Cyber Special Ops, LLC, which offers the product. "These include same-day appointments and phone or email access on evenings and weekends, information security policy templates, and pre- and post-breach services, as needed, at pre-negotiated rates.

"We work with a respected and highly credentialed group of legal, information security, credit and identity restoration, and public relations specialists from firms located around the globe to deliver advanced cyber risk management services," he adds. "The specialists operate under the umbrella of My-CERT™ which stands for My-Cyber Emergency Response Team; they provide what we describe as 'expertise, experience and agility to effectively respond to a cyber incident under the protection of attorney-client privilege.'"

Cyber has been part of Suhs's life for more than two decades. "In 1997, I helped launch the first cyber insurance product," he recalls. "Much has changed in the ensuing 20-some years. But some things haven't. For instance, while many larger organizations today have stand-alone cyber insurance, unfortunately, statistics show, only two out of 10 organizations with less than $1 billion in annual revenue buy cyber insurance."

That's a problem. Actually, it's a big problem for these smaller firms, which are largely ill-equipped to deal with the fallout of a cyber event. "Firms of all sizes—not just the big guys—are seeing increased frequency and severity from things like ransomware, business email compromise, and more," Suhs says. "Not only do business owners face the financial challenges associated with response, often they have no clue where to start.

"Don't believe me?" he adds. "Ask any business owner whom they would first contact in the event of a cyber incident. Be prepared for a deer-in-the-headlights look. Then ask about their cyber incident response plan. Expect the same stare."

Early successes

"Since we launched the offering at the start of last year, we've had some pretty positive outcomes," Suhs says. "For example, one of our first clients had a cyber incident regarding a lost laptop. They had cyber insurance coverage, but the policy had an exclusion for unencrypted laptops, so the claim was denied. The insurer recommended that the client work with a law firm on its panel to help them get through it.

"About a month and a half after engaging the law firm, the client's broker called me," Suhs explains. "Turns out the client got the bill from the law firm and experienced sticker shock. I was able to help get the bill reduced. I also pointed out that, had they reached out to me up front, we could have delivered the same service the law firm did at a mere fraction of the cost."

With another client, they got a call from an insurance broker late in on Wednesday afternoon—but it wasn't just any Wednesday; it was the day before Thanksgiving. The broker's client had experienced a ransomware attack. "The bad guy wanted $100,000 in bitcoin and, if not paid by Friday, the price would go up to $200,000," Suhs recalls. "Of course, the broker was frantic because everyone at the cyber insurer was gone for the Thanksgiving holiday and would not be back in the office until Monday morning."

Cyber Special Ops immediately contacted the My-CERT attorney and information security provider who was on that insurer's panel and called the broker's client with a game plan. "The broker called me that following Monday and said that he received a call from the insurance claims attorney who had to first read the policy to ascertain coverage," Suhs says. "The broker asked if that was common practice. Unfortunately, some cyber incidents are like a building on fire, and the insured must take immediate action to minimize a loss.

"In yet another cyber incident, an insurance broker contacted us regarding a client who had wired $50,000 overseas from what we learned later was a business email compromise (BEC) attack," Suhs says. Unfortunately, the client had waited several days before notifying the broker of the loss and never recovered the funds.

"We advised the broker that we would immediately contact the FBI's Internet Crime Complaint Center (IC3) to report the wire fraud on behalf of our Concierge Cyber client," he adds. "The IC3 has a team that helps affected BEC victims recover funds by streamlining communications to financial institutions. Recovery rates can be surprisingly high if fraud is reported quickly."

First steps

The most common mistake organizations make is one Suhs referenced earlier: not knowing what to do or whom to call if a cyber event takes place. "The first question we ask," Suhs says, "is 'Do you have cyber insurance?' It's important to look at all of an organization's insurance policies, because sometimes coverage is hidden—like in a crime policy or in a professional liability or even a property insurance policy.

"Even in the absence of stand-alone cyber insurance, we can triage with agents or brokers and their customers to determine whether it was an incident—meaning, was there a data breach, was there a bad guy or malware in the organization's environment? If so, then we need to contact outside counsel—perhaps one of the experienced law firms on our panel."

Sometimes they'll engage a forensics firm. "If that's the case, the engagement needs to be done through the law firm to maintain attorney-client privilege," Suhs explains.

"Not only do business owners face the financial challenges associated with (cyber event) response, often they have no clue where to start."

—Kurt Suhs
Founder and Managing Director
Cyber Special Ops, LLC

"Companies may have relationships with information security experts, so it's natural that they'll reach out to them immediately. However, whatever services are rendered are potentially discoverable. And that's not good."

The cyber risk management arena is constantly changing. "Our goal is to make it easier for agents and brokers and their clients to access cyber risk management resources they need, precisely when they need them," Suhs notes. "Agents and brokers appreciate the added services we make available to their commercial and high-net-worth clients—not to mention the extra and renewable revenue for the agency or brokerage. And clients take comfort in the fact that there's a plan in place if and when an event occurs." ■

For more information:

Cyber Special Ops, LLC
www.cyberspecialops.com

Reprinted from the March 2020 issue of **Rough Notes** Magazine