CyberInsecurity News™
WHAT LAWYERS NEED TO KNOW

SEPTEMEBR 2019

INTERVIEW: KURTIS SUHS / CYBER SPECIAL OPS, LLC

WHO YOU GOING TO CALL?

A startup, backed by a team of professionals, aims to help companies make the right decisions after cyber incidents.

He runs a one-man shop, but he's been around the block. ***Kurtis Suhs*** (pronounced like Dr. Seuss) was an investigator with the FDIC, where he worked on fraud and professional liability claims at failed banks. He was later cyber chief underwriting officer at Ironshore Insurance (a Liberty Mutual company). And he'd been a managing general underwriter for INSUREtrust.com, the first company to release a cyber insurance product—in 1997. "I was one of the individuals that helped launch the first cyber insurance product," he says.

He took all the skills he'd acquired, and in January he founded Cyber Special Ops, LLC. For an annual membership fee, the company provides "Concierge Cyber™" services to companies that need help figuring out if they've experienced a cyber incident, and if they have, navigating their next steps with the assistance of a panel of vendors available at preset rates.

CyberInsecurity News: *Let's cut right to the chase. Can you give us an example of what you've done for your clients?*

Kurtis Suhs: My first client had a cyber incident regarding a lost laptop. They had cyber insurance coverage with an exclusion for unencrypted laptops, so the claim was denied. However, the insurer recommended a law firm on its panel to help them get through it. About a month and a half after engaging the law firm, the not-for-profit company called me and said, "We got our invoice, and we didn't expect this large a bill." I helped them get their bill reduced. But the lesson learned for them was that if they'd engaged me immediately, it would have been a $3,000 bill for 100 records lost. Whereas they paid five times that much.

CIN: *When do you get involved in a case?*
KS: Ideally, I like to get involved well before the client believes there's an incident. I've put the third-party panel together with negotiated rates for both pre- and post-loss control services. And when our client has an event, our team is able to walk them through the incident, and better manage it, saving them a bundle.

Cyber Special Ops, LLC

CIN: *What are the most common mistakes that companies make in this area?*
KS: Not knowing what to do or who to call. The first question is: Do you have cyber insurance? I recommend that we first look at all your insurance policies, because you might be able to find coverage in a crime policy, or in a professional liability or a property policy. Even if you don't have stand-alone cyber insurance, you still need to triage the event to determine whether it was an incident—meaning, was there a data breach, was there a bad guy or malware in your environment? If that's the case, then we need to contact outside counsel, and I have experienced law firms on my panel. If we engage a forensics firm, then the engagement needs to be done through the law firm to maintain attorney-client privilege. Companies may have relationships with information security experts, but if they reach out to them immediately, whatever services are rendered are potentially discoverable. And that's not good.

CIN: *What are the easiest things that companies can do to avert mistakes and start fixing their cybersecurity posture so that they're better prepared if and when an attack occurs?*
KS: It goes back to the basics of people, processes and technology. If you're looking to protect things, the first thing I would ask is, What are you trying to protect? If you have personally identifiable information—PII—how much do you have, and where does it reside? PII could be with third-party service providers. If that's the situation, then you should look at contracts and make sure that they have procedures in place to protect that data for you. Because you, as the owner of that data, are responsible for it.

And then there's people and training. Do people know what to do if there is an event? Who do they notify within the company if there is a ransom demand? And the processes are the last component. Do you have an incident response plan? Do you have a disaster recovery/ business continuity plan? And it's great to have a plan, but you need to test it.

CIN: *What are your Concierge Cyber services, and where did this name come from?*
KS: It came out of the analogy of concierge medicine. When the Affordable Care Act was enacted, I saw a lot of physician groups marketing concierge medicine, in which patients would pay an annual membership fee to have greater visit time with the doctor and guaranteed same-day appointments. So I wondered, when only two out of 10 companies buy stand-alone cyber insurance, what do the other eight companies do? Who do they call? I saw an opportunity to help these companies.

In the same vein as concierge medicine, they would have access to a specialist who could provide them with best-of-breed third-party service providers. So, whether it's the law firms, the information security professionals, the crisis management or identity-monitoring companies, for an annual membership fee my clients get access to them all. And through the various programs, whether it's bronze, silver or gold, each of the levels of customization offers more. For example, the bronze service offers a virtual chief security officer on a pre-incident basis. It also offers cyber triage for post-loss incidents, and access to the My-CERT team. The silver program adds online security awareness training, crisis management and information security policy templates. And then the gold program includes tabletop exercises.

CIN: *You mentioned My-CERT. What is that, and where did you get the name?*
KS: I got the concept from the U.S. government utilizing US-CERT [computer emergency response team]. Mine stands for *cyber* emergency response team. The team that I put together offers a one-stop shop for customers on a post-incident breach basis at pre-negotiated rates and credentialed firms that are experienced in handling data breaches and network security incidents.

CIN: *Are you providing the services that an insurance agent would, for companies that have cyber insurance?*
KS: There is some overlap. However, not all incidents trigger coverage in an insurance policy. For example, a cyber insurance policy excludes theft of intellectual property and often excludes theft of money. The greatest benefit in our services is 24/7 guaranteed access for any cyber event.

CIN: *Let's break off one piece of it. You offer a virtual chief security officer. Tell me about that service.*
KS: When I was working at the insurance company, people didn't know when an event within the organization became an incident. Your firewall log and your technology will have bells and whistles ringing, but is that actually something that's meaningful? Our security team—third-party service providers—will triage an event, ascertain whether it's an incident, and then determine the next steps—whether outside counsel needs to be engaged, or whether perhaps it's nothing at all.

CIN: *What kind of relationships do you have with your vendors, and how did you form alliances with them?*
KS: I've been working in this business for 33 years, 22 in the cyber insurance arena. So these are all firms that I've worked with over the past 20 years. We have pre-established pricing for services from these credentialed firms.

CIN: *What is the role of outside lawyers in the My-CERT plan?*
KS: Attorney-client privilege. You really want to be able to preserve privilege with any work product, whether it's the

forensics, the crisis management, any type of interactions with third-party vendors—accountants and so forth.

CIN: *How about you? If you are the first person your clients hire, how does that work?*
KS: Basically, I'm the first contact. And the cyber triage goes to an information security partner. If we determine that it's an incident—especially if it involved PII, or protected health care or credit card information—we engage outside counsel.

CIN: *Who do you work with at the companies that hire you? Are in-house lawyers usually involved?*
KS: A lot of the firms that work with us don't have in-house counsel. We most often work with senior management who have an organizational financial stake in a cyber incident. And that typically isn't the information technology team.

CIN: *Is this because you're often working with smaller firms?*
KS: Right. Generally, I work with the C-suite. And that varies by the size of the companies. I've been involved with companies where it could be the CEO or the COO or the risk management folks. At others it's been the CFO. My target is middle market companies—$2 billion in annual revenue and smaller.

CIN: *You are not a lawyer. You majored in economics and earned an MBA. Yet you clearly understand the value of working closely with lawyers. And you seem comfortable with them. Was this working relationship something that came from years of experience?*
KS: Yes. I began gaining this experience when I was an investigator with the FDIC, where I worked with professional liability attorneys in Washington, D.C. I worked on failed-bank professional liability claims. As the investigator, you're working hand in hand with FDIC counsel, looking at financial institution bonds, director and officer liability claims, accountants' malpractice claims, and broker and security malpractice claims relating to failed banks. Doing that for eight years gave me a lot of experience. And so did working on the insurance side, underwriting with the claims attorneys.

CIN: *One of the legal issues you have to deal with involves breach notification. What makes that so tricky?*
KS: I've seen clients that wanted to notify right away: "Let's notify everyone." Well, how do you do that? Do you do that by first-class postage? Do you do that by email? Can you do it on your website? You can look at the implications of doing it the wrong way. And if it's not handled properly, it can be costly. There are notification laws, which provide for alternative means to notify. Every state has alternative means to notify individuals impacted by a breach. And that's by the number of records, and the cost to notify. With the exception for health care, if the incident involves 500,000 individuals or more and the cost to notify is $250,000 or more, then you can use alternative means to notify. Which means that you can put it in the newspaper or on your website, conspicuously posted. And that cost is almost nothing. In the case of Target, their cost to notify was next to nothing, because once it hit the media, their notification requirement was met. Mississippi has the lowest threshold to trigger alternative means. It's $10,000 or more and 10,000 people or more. But health care data is different. Health care requires first-class postage. There's a lot to know. It's not so easy. And there are a few firms that have a lot of experience doing this correctly. And I've got some assembled on my panel.

CIN: *How prepared are companies to deal with the challenges of a data breach?*
KS: In the small and medium-size company market, they generally don't even know the first steps.

CIN: *And that hasn't changed, even after all the publicity about ransomware attacks every week?*
KS: No. Even some of the bigger firms are working through issues. Do you want to sue your vendors? Do you want to sue your business partners? Are you going to help hold them accountable? You're starting to see litigation over that. And then subrogation on the insurance side for recovery—if there is a recovery.

CIN: *We have heard that small companies think that all this cybersecurity stuff is about larger companies, not them.*
KS: People tend to talk about cyber as data risk. And people think, "I don't have a lot of data." But when you look at theft of money, that impacts every company's cash flow. The other aspect is the business interruption related to ransomware. If you get hit with your organization having military-grade encryption on your computers and servers, and you can't operate, that's crippling. And because the insurance companies are paying the ransoms from the stand-alone cyber policies, it's a moneymaker for the bad guys. I think you'll see the frequency and severity of ransomware increase over time.