ceocfointerviews.com
© All rights reserved
Issue: April 27, 2020

Concierge Cyber® works hand in hand with your insurance

Kurtis Suhs
Founder and Managing Director

Cyber Special Ops, LLC
https://cyberspecialops.com/

Contact:
(678) 576-1106
Kurtis.Suhs@CyberSpecialOps.com
https://www.linkedin.com/in/kurtis-suhs-688a136/
https://www.linkedin.com/company/cyber-special-ops-llc

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

Concierge Cyber®
https://cyberspecialops.com/wp-content/uploads/2020/04/CSO_Concierge_Cyber_121719.pdf

Cyber Special Ops Services
https://cyberspecialops.com/services/

CEOCFO: ***Mr. Suhs, What was the vision when you founded Cyber Special Ops? What is the focus today?***
Mr. Suhs: I've spent the past 23 years working with organizations to evaluate cyber risk and helped launch the first cyber insurance product back in 1997. While the acquisition rate for cyber insurance has increased over the years, today still only 2 out of 10 small and middle market enterprises buy stand-alone cyber insurance. The first question I ask an organization that doesn't purchase cyber insurance is: when you have a cyber incident, who do you call? Even when they have cyber insurance, insureds still may not know whom to call. Therefore, I wanted to solve that problem, and, in doing so, help clients respond to a cyber incident with guaranteed same-day access and availability, whether you have cyber insurance or not.

That is where I looked to concierge medicine and the model of availability, same-day appointments, and personalized care. When I launched Cyber Special Ops, I trademarked and launched Concierge Cyber®, a new delivery model for cyber support based on concierge medicine, which has proven to result in positive outcomes for both the patient and physician. For a modest annual fee, an organization has access to a team of credentialed third-party experts, at pre-negotiated discounted rates, to minimize and respond to a cyber incident. Like concierge medicine where patients have health insurance, Concierge Cyber® works hand in hand with your insurance and our allegiance is to you and not your insurance company.

CEOCFO: ***How do you reach out to potential customers and why does your service feature make a difference for those eight out of ten who are not being proactive?***
Mr. Suhs: We work directly with clients and their insurance brokers. We have packaged and bundled services to help the C-Suite manage cyber risk. For example, our bronze package provides 12 information security policy templates, two hours with an On-Call Chief Security Officer for a pre-incident consultation, a ransomware hostage manual and access to My-

CERT™ (My Cyber Emergency Response Team). This global team is highly experienced and includes law firms, information security, identity/credit monitoring, call center and public relation companies. Whether you have cyber insurance or not, we help clients maximize a financial recovery from a cyber incident by evaluating their entire property, casualty or personal lines insurance coverage. For example, we had one client who lost an unencrypted laptop. The client had cyber insurance; however, the policy had an exclusion for loss from an unencrypted computer. We were able to identify a means of financial recovery in their property insurance.

CEOCFO: *What do companies misunderstand about security?*
Mr. Suhs: Cyber security isn't a technology issue. We view cyber risk as a peril that involves the financial health of your organization. For example, how do you train employees to protect intellectual property? Does your organization have a process to evaluate third party vendor contracts for cyber risk? Just because you outsource to a third party doesn't mean you aren't legally liable for data of your employees and customers. Do you have dual authentication for online banking, including wire transfers? We help senior management proactively evaluate cyber risk from a multifaceted basis.

CEOCFO: *Do you see increased interest, perhaps as a result of COVID, where people will pay more attention in general than they have in the past?*
Mr. Suhs: A cyber virus and COVID-19 have a lot of similarities. Many organizations think it will never happen to them. Some will get infected and go out of business. Others will prepare for the virus, get infected and sustain a slow and painful recovery. And others will have no idea they are infected and will go about their business in complete denial, infecting those around them.

"For a modest annual fee, we provide our clients with guaranteed access to personalized care and availability with a team of highly credentialled third-party service providers at pre-negotiated discounted rates to help minimize and respond to cyber risk." Kurtis Suhs

With respect to COVID-19, most organizations now understand that their insurance may not provide coverage for business interruption since the insured's property didn't sustain physical damage. In the cyber world the question has always been: when you have malware that encrypts a computer and prevents you from accessing the data, is that a property loss? The computer is still functioning, it is physically not damaged. In the cyber world there are cases that say no, and there are some cases that say yes. In recent litigation, a Federal judge ruled that State Auto Property & Casualty Insurance Co. must cover an embroidery and screen printing company's costs to replace its computer systems following a ransomware attack in 2016.

State Auto had argued that the direct physical loss requirement wasn't satisfied because the attack merely blocked National Ink's ability to access intangible electronic data files without fully disabling its computers. But Judge Gallagher was unconvinced, saying that, "in many instances, a computer will suffer 'damage' without becoming completely inoperable."

Certainly if you look at the analogy with COVID-19, your building is still there and not physically damaged but you cannot get access. It is so similar to cyber that I think within the insurance industry you are going to have some deep discussions of whether business interruption policies should provide coverage for these types of events, or should the federal government have a backstop. For example: what happens in the cyber world where some computer malware virus hits so many organizations in critical infrastructure that they cannot operate? You could be looking at a very similar event to what you are seeing with COVID-19 now.

CEOCFO: *What has changed in your approach over time?*
Mr. Suhs: I now communicate to organizations that they should operate with zero trust, an information security framework which states that organizations shouldn't trust any entity inside or outside their perimeter at any time. While you can't prevent a cyber incident, you can control the incident response by having the right team in place. Who do you call when you are sick? The answer isn't your health insurance company. You call a first responder. Cyber Special Ops is your cyber first responder who will triage the cyber event and hand the matter to an experienced law firm who then may engage an information security firm under attorney client privilege. That can make a world of difference.

CEOCFO: ***What do you look for in your team; what is important for Cyber Special Ops?***
Mr. Suhs: I look for people who are entrepreneurial, good listeners, and who can provide guidance to solve problems. Our team is consultative and collaborative and serve as a trusted resource to find the right resources to help our clients with the best solution.

CEOCFO: ***Are there continually new resources that become available?***
Mr. Suhs: I see a lot of venture capital investment placed into cyber analytics firms. These companies will scan an organization's URL and provide a security score based upon proprietary scanning and open source intelligence. I liken this model to a real estate drive-by appraisal. Yes, the house from the curbside looks well maintained and secure; however, the interior is completely empty, vandalized, and trashed. Drive-by appraisals didn't work in the mortgage industry and they won't accurately score cyber risk. To make matters worse, a good score may lead to a false sense of security. Today, the mortgage industry utilizes full appraisals whereby the appraiser actually goes into each room within the house in addition to an outside evaluation. Unless you can go into the organization, you will never glean the true risks.

For example, when Target was hacked, the bad guys stole a vendor's credentials, which were used to access Target's system. The discovery that the credentials stolen in the Target breach were from an HVAC contractor shows how much we live in a connected world and how insider threats are the hardest to detect since outside attackers look just like employees when they are on the network. How would an analytics firm look at that type of scenario? They wouldn't even know about that vendor relationship.

CEOCFO: ***What is the competitive landscape for you? Are their many companies that have recognized the concierge approach?***
Mr. Suhs: We have several broker clients. We also have direct clients ranging from small startups to one of our largest clients being a large national trucking company. Concierge Cyber® is new but the model is well proven in the healthcare industry. We are seeing a lot of interest and tremendous support on the Concierge Cyber® value proposition. We are building and growing considerably. We have offices in New York and Chicago are going to be launching in London next month. We continue to grow.

CEOCFO: ***Why London?***
Mr. Suhs: We have a seasoned cyber risk consultant that I've worked with in the past in London and see an opportunity not only for U.S. placed business at Lloyds of London, what we call the reverse flow, but also Concierge Cyber® membership for U.K. organizations. We are unique and look to expand there for that opportunity. We have added two U.K. law firms that are very well-known in the data breach arena who will join our existing My-CERT™ panel of service providers.

CEOCFO: ***What has changed day-to-day in your organization with COVID?***
Mr. Suhs: I think the most common discussion with clients and their insurance brokers is business interruption coverage related to the pandemic. I know that there are several states and federal legislation that would nullify existing exclusions and force insurers to cover business interruption from viral pandemics. Organizations are financially hurting and looking for any means to stay afloat. Sadly, cyber threats haven't diminished, and organizations of all sizes are still getting hit with cyberattacks, particularly from ransomware.

CEOCFO: ***Why take a look at Cyber Special Ops?***
Mr. Suhs: For a modest annual fee, we provide our clients with guaranteed access to personalized care and availability with a team of highly credentialled third-party service providers at pre-negotiated discounted rates to help minimize and respond to cyber risk. That is what we do. Some people use the analogy that, "It is not if, but when." I like to say, "It is not if, it is not when, it is how big."