Cyber Risk and Incident Response
Where it all began…and the journey forward

Kurtis Suhs
Founder and C.E.O., Cyber Special Ops, LLC

Mr. Suhs serves as Founder and Chief Executive Officer for Cyber Special Ops, LLC, a company that provides its clients with Concierge Cyber®. ***Modeled after roadside assistance, Concierge Cyber is a subscription membership model that guarantees members emergency response to a cyberattack or data breach through a team of highly respected third-party service providers, on a pay-as-you-go basis, at pre-negotiated and substantially discounted rates.*** *Kurt has over 35 years of experience in the insurance and financial services sectors and helped launch the first cyber insurance product in 1997, with INSUREtrust.com.*

Prior to founding Cyber Special Ops, Kurt served as SVP and Cyber Chief Underwriting Officer for 9 years at Ironshore Insurance, a Liberty Mutual Insurance Company, where he was responsible for innovating cyber insurance products and risk management solutions across all lines of coverage on a global basis. Earlier in his career Kurt was an Investigator with the FDIC where he investigated financial institution fraud and professional liability claims for failed banks.

Of all the technologies that changed our lives, perhaps the most profound of the last 50 years has been the Internet. But it wasn't the ability to hyperlink documents that made the most impact. Instead, it was the platform that presented all that information to users, the browser. In 1995, the world's first pure Internet bank, Security First Network Bank, was launched in Atlanta, Georgia. Obviously, bank regulators had several concerns, including the ability to safely deliver online banking services and the threat of financial institution fraud arising from this new technology. Below is a screenshot of Security First Network Bank's website which was really innovative at the time:

The insurance broker for Security First Network Bank, who was also based in Atlanta, was asked to find insurance to protect the online only bank from internet threats. The insurance agent sought out coverage, but no coverage existed for web perils. That is when and where the insurance agent had a vision for hacker insurance. So in 1997, this agent created Network Risk Management Services, LLC (later known as INSUREtrust.com), as a Managing General Agency (MGA) that launched the world's first cyber insurance policy at the height of the dot com era.

INSUREtrust's model was based on Highly Protected Risk (HPR) where property insurers designed property insurance and engineering-based risk management solutions by employing state-of-the-art sprinkler systems. In a similar vein, INSUREtrust hired information security professionals to conduct an external vulnerability assessment against a cyber insurance applicant's computer network. As a condition of binding coverage, the applicant had to immediately remediate any discovered high vulnerabilities and address and fix any medium vulnerabilities within 30 days of the policy's effective date. The cyber applicant also had to complete a 12-page insurance application that addressed their risk management controls around people, processes and technology.

By 2015, the marketplace continued to expand with over fifty standalone cyber insurers who were continually offering ever broadening terms and conditions at accelerating premium reductions. Not only were external vulnerability assessments no longer required, but the cyber insurance applications shrank down to 2-3 pages. This soft market was remarkably close in offering an All-Risks policy - an insurance policy that automatically covers any risk that the contract doesn't explicitly omit. For example, coverage was readily expanded to include 1) bricking, which is when malware doesn't physically damage tangible property, but the hardware is essentially useless, 2) business email compromise, where the attacker sends a spoof email or hacks into the insured's network to redirect a money transfer to the threat actor and 3) system failure where an insured mistakenly takes their network offline resulting in business interruption loss.

Around 2017, private equity firms began heavily investing in cyber insurance MGAs, who took on traditional insurers with online and streamlined applications, quoting, binding and policy issuance. These cyber-MGAs also touted their innovative underwriting prowess by offering external vulnerability scanning at the time of application and during the policy period.

In 2020, the cyber insurance market showed signs of hardening as the frequency and severity of claims increased from ransomware attacks and the theft of money arising from business email compromise. To complicate matters, organizations had greater interconnectivity of devices, business partners and third-party providers with respect to both information technology (IT) and operational technology (OT).

By 2021, the cyber insurance market was in an unprecedented hard market cycle. The 2021 Ransomware Report by Sophos stated that over a third of the 5,400 surveyed were hit by ransomware. Additionally, the average ransom paid by mid-sized organizations was $170,404 while the average bill for rectifying a ransomware attack, considering downtime, people time, device cost, network cost, lost opportunity and ransom paid was $1.85 million.

Today, cyber insurers have restricted their appetite for certain industry classes, reduced overall policy limits, sub-limited coverage for ransomware and theft of money, added co-insurance provisions, added additional exclusions and increased premium anywhere from 25 – 400% over the prior year. Furthermore, the majority of cyber insurers now require multi-factor authentication (MFA) enterprise wide, regardless of user privilege for all applicants and insureds. This generally is non-negotiable and a minimum requirement for a cyber insurance applicant. Many cyber insurers may also inquire on an applicant's use of 1) endpoint protection monitoring and response tools, 2) a 24/7 security operations center (SOC), 3) regular security awareness and phishing training, 4) a strategy on backups of data and are the backups stored offsite and air gapped from the Internet, and 5) a privileged access management tool to protect user credentials.

Given all these new and onerous cyber insurance requirements, what is your plan if your organization either doesn't qualify to meet minimum information security insurance requirements or for other reasons decide to forgo the purchase of cyber insurance? Who do you call on a 24/7 basis if you have a cyberattack or theft of money? Even if you have an outsourced information security or information technology relationship, how will you preserve the forensics work product? And how does an organization's directors and officers address their added responsibilities that include 1) duty of care, 2) duty of loyalty and 3) duty of obedience.

Concierge Cyber® was designed to provide a plan and equip your organization with the best resources you need to respond to a cyber incident. Concierge Cyber membership will ensure your organization is covered 24/7 with a dedicated team of credentialled, nationally recognized, third-party firms with the added benefit of a cost savings between 35-50% off their normal rates. To sign up for Concierge Cyber membership, go to https://cyberspecialops.com/ or contact us at Info@CyberSpecialOps.com.