New York Law Journal
Cybersecurity
WWW.NYLJ.COM
An ALM Publication
VOLUME 257—NO. 42
MONDAY, MARCH 6, 2017

Insurance Challenges Ahead As Cyber Perils Shift

BY JOSHUA GOLD

© SHUTTERSTOCK

For years now, cyber crimes have mostly been viewed through the prism of financial harm—essentially money and identities stolen. True, some cyber crimes over the years have also been calculated to invade privacy, taunt or embarrass (e.g., sexting, trolling, cyber stalking, cyber bullying, etc.) rather than just steal money or business secrets. But even in such circumstances, rarely did it feel like life or brick and mortar property were on the line. That perception is changing with news that Stuxnet was used to cause an explosion overseas and that multiple organizations (including hospitals) have had their data and property controlled by hackers to extort ransom payments.

What if Ferris Bueller and The HAL 9000 Coupled-Up?

One of the early popular culture references to computer hacking was in the film "Ferris Bueller's Day Off." By today's standards, Ferris' hacking was relatively benign—reducing, online, his number of school absences. Perhaps then "2001: A Space Odyssey" is a more apt warning of the harm to come. In that film, the computer HAL murders one astronaut and attempts to kill a second during the ambitious mission to Jupiter. While not a hacking event, it is an ominous depiction of the severity of harm faced once humans make their everyday functionality entirely reliant upon computer systems. That future is upon us in the form of system glitches, cyber attacks, programming errors, and hacking, which pose all too real harm to humans and real property.

With the advent of smart devices and the Internet of Things, the risk to human health and real property is bound to trend higher. The automotive and airline industries

JOSHUA GOLD, *a shareholder in the New York office of Anderson Kill P.C., is chair of the firm's cyber insurance recovery group. Mr. Gold can be reached at jgold@andersonkill.com or (212) 278-1886.*

have already begun to tighten their network security after a rash of claims by "white hat" hackers indicated they could wrest control of key vehicle and aircraft functionality. Recently, a European hotel was said to be the target of cyber criminals gaining control of "smart locks" to keep people out of their rooms. While there were no reports of resulting injuries, it may just be a matter of time before a guest is injured or dies when unable to gain access to life-saving medication during an asthma attack. Similarly, it is a matter of time before medical providers targeted by ransomware are prevented from accessing direly needed medical records that contain information on serious allergies and individual health histories. Concern has also been raised as to whether medical implant devices may be hacked and manipulated to kill or injure.

Of more **immediate concern to policyholders** seeking to plug the property damage/bodily injury hole in cyber polices is the fact that since 2014, more and more CGL insurance companies have been injecting **cyber-related exclusions into the insurance they sell.**

With the rash of cyber events over the last several months involving devices as common as baby monitors hacked to inflict damage and cause interruption, the case for examining the implications for traditional insurance protection against bodily injuries and property damage is upon us.

Trying to Make Sense Of One's Protection

The commercial insurance industry's response to computer-related exposures has evolved rapidly. Today, dozens of different insurance companies actively market and sell primary-level insurance products dedicated to cyber perils. Industries and organizations across the board (including law firms) are buying cyber-specific insurance policies. Some purchase hundreds of millions of dollars in limits but most purchase coverage way under that amount. However, many of these cyber policies impose exclusions for bodily injury and property damage claims. Given the implications of smart devices and the Internet of Things, this makes the prospect of cyber insurance companies contesting injury and damage claims an enormous concern.

Traditional business insurance policies, such as property insurance and so-called CGL (or commercial general liability) insurance become increasingly important should a cyber claim result in death, injury or destruction of real property. Since the early years of the millennium, policyholders have sometimes had success securing insurance coverage under their first-party property insurance policies for cyber-related events. Comparatively early, a number of courts ruled that damage to electronic data is property damage.

In *NMS Services v. The Hartford*, 62 Fed. App'x 511, 514 (4th Cir. 2003), the U.S. Court of Appeals for the Fourth Circuit ruled against the insurance company's arguments against paying a claim and held that the intentional "erasure of vital computer files and databases necessary for the operation" of its systems by a former employee was "damage to its property, specifically, damage to the computers it owned." In a case that garnered a lot of attention at the time, *American Guarantee & Liability Insurance Company v. Ingram Micro,* 2000 U.S. Dist. LEXIS 7299 (D. Ariz. April 18, 2000), a federal trial court held that "physical damage" includes loss of use of programming instructions and custom configurations that, among other things, left the computer mainframe inoperable when the data center experienced a power outage. In *Southeast Mental Health Center v. Pacific Ins.*, 439 F. Supp. 2d 831, 837 (W.D. Tenn. 2006), another federal trial court held that "the corruption of the pharmacy computer constitutes 'direct physical loss of or damage to property'" entitling the policyholder to business income coverage under its property insurance policy. Similar to the rulings above, the court in *Landmark American Ins. v. Gulf Coast Analytical Laboratories,* 2012 U.S. Dist. LEXIS 45184 (M.D. La. March 26, 2012), found that electronic data is susceptible to "'direct, physical loss or damage.'"

These cases indicate that insurance companies have often taken a hard line on covering computer-related claims over the last 15 years or so. Some have observed that Y2K was the event that spooked the insurance industry given the scale of disruption and carnage imagined

at the time. But insurance disputes involving computer related claims happened even before the advent of the Y2K scare. Looking back to the 1980s and 1990s, policyholders and their insurance companies were wrangling over insurance coverage for electronic information. Some of the earliest fights over property damage insurance coverage involving electronic information focused on whether computerized information was "tangible property" under commercial general liability insurance. For example, in *Centennial Insurance v. Applied Health Care Systems*, 710 F.2d 1288 (7th Cir. 1983), the insurance company refused to cover a claim where it was alleged that a faulty controller caused loss of computer data. There, the policyholder was able to obtain defense coverage for the underlying claim against it.

In *Magnetic Data v. St. Paul Fire & Marine Insurance*, 442 N.W.2d 153 (Minn. 1989), however, the policyholder was unable to prove coverage for the erasure of data due to an exclusion for property under the control of the policyholder. In *Retail Systems v. CNA Insurance Cos.*, 469 N.W.2d 735 (Minn. App. 1991), the court found the phrase "tangible property" ambiguous in the context of electronically captured information on computer tapes.

ISO Exclusions in CGL Insurance: Life Made Harder

Of more immediate concern to policyholders seeking to plug the property damage/bodily injury hole in cyber polices is the fact that since 2014, more and more CGL insurance companies have been injecting cyber-related exclusions into the insurance they sell. Some exclusions are intended only to apply to so-called advertising and personal injury coverage claims (e.g., copyright suits, invasion of privacy suits, defamation claims, etc.). But others purport to go beyond those perils and attempt to exclude property damage claims and possibly even bodily injury claims. Again, this is bad news for many policyholders facing Internet of Things and smart device risks, even where they purchase additional coverage specifically for cyber claims.

The bottom line is that if the cyber policy has a bodily injury and property damage exclusion, then it is essential to have one's first-party property policy and third-party CGL coverage untainted by cyber exclusions that apply to such claims. Otherwise, the policyholder will likely be left in a complex coverage fight with its insurance companies over the scope of both insuring clauses and exclusions.

Regarding property risks, we are even beginning to see cyber-related exclusionary language make its way into marine cargo insurance policies, and sub-limits for cyber claims make their way into first-party all-risk property insurance. Policyholders and their brokers should be very careful with the fine print and address these issues upfront during underwriting meetings and renewals.

While the coverage landscape is definitely challenging for policyholders, it is not all doom and gloom. Some cyber insurance companies will agree to remove the bodily injury and property damage exclusions from their policies (but make sure this is done throughout the entire program if buying multiple layers of insurance coverage). Also, some property insurance policies are expressly placing cyber risk under the blanket limits of the policy and making such coverage primary for the policyholder, even when it purchases cyber insurance. Other options are developing as well, where some insurance companies are filling potential coverage gaps in insurance programs with "difference in conditions" insurance products.

Conclusion

The landscape of insurance coverage for technology risk alters as fast as the risk itself—that is, constantly and dramatically. Today's conventional wisdom can become obsolete in a heartbeat. Sound risk management will continue to require close monitoring of the situation, smart decision making and adaptability. Very soon, unfortunately, computers will kill or be used to kill, as Arthur C. Clarke predicted a half-century ago.