Baby Monitors & Steel Mills: The New World of Cybersecurity Risk

by Joshua Gold

No doubt, policyholders have been the regular targets of cyberthieves for the better part of a decade and will continue to be. Whether the thief is after cargo, health information or a wire transfer, thieves continue their imaginative and often effective ploys to profit. Perils such as the loss of money through ransomware, hacked payment card data, or misdirected funds through social engineering schemes remain a huge problem.

But increasingly we are seeing a new breed of cybercriminal that appears to lack a clear profit motive, and instead is focused on causing business interruption, economic mayhem, political instability and outright carnage.

TROUBLING DAMAGE AND INJURY SCENARIOS

The Stuxnet virus previously was documented to have been used as a military grade weapon of espionage in the battle over nuclear proliferation. This same virus has now appeared in attacks against the computer controls in a foreign steel mill, leading to an explosion, with resulting property damage. Some months ago, the internet itself was attacked through a distributed denial-of-service attack using, among other things, baby monitors. Other hackers have used malicious code to destroy hardware and prevent access to websites for a host of causes and motivations. Hackers have also made their way into critical infrastructure by attacking a dam in New York and a utility in Vermont. So-called "white hat" hackers have demonstrated on numerous occasions that they can infiltrate the safety features of connected vehicles.

As is by now axiomatic, risk management geared toward preventing intrusions is critical. Loss of money is no longer the sole downside to system compromises—lives and nations are now at stake. Most now take seriously the obligation to involve senior management in cybersecurity procedures and process, tap a cross-section of departments to gauge and address cyberrisk, continuously train users and update security protocols, and have action plans in place in the event of a compromise.

INSURANCE CHALLENGES

Cyber insurance products will need to address claims in which the hacker is not after just money and sensitive information. Specifically, policyholders will absolutely need insurance coverage when a cyber event ends up destroying property and taking lives. And these coverage needs will likely implicate insurance policies well beyond what we typically would refer to as a "cyber policy."

On the insurance end, things have been challenging already when it comes to cyber products. Over the last five years or so, the insurance industry has pushed more and more policyholders into specialty policies. Many of these policies, however, have not kept up with the morphing nature of the cyber peril. These insurance policies are intended to cover core cyberrisks. But where hackers look to do more than just steal money and account information, bodily injury and property damage claims will play a central role. Some cyber insurance companies will refuse to pay these claims, arguing that their policies only cover such items as privacy class actions, breach notification costs and forensic analysis of the hack. This scenario, in turn, points to CGL and property insurance policies to pick up the slack. Some do so expressly (there are some property insurance forms that offer express coverage for property damage arising from cyber-related perils). But since 2014, those CGL policies are seeing a greater imposition of ISO

RISK MANAGEMENT

Reprinted with permission from *Risk Management*.

www.rmmagazine.com

form cyber exclusions in varying scope. Even those CGL cyber exclusions that purport to be limited in scope are far from clear in what the coverage boundaries will be.

Some insurance companies are offering endorsements to policies to offer affirmative coverage, and some cyber-specific insurance products are deleting property damage and bodily injury exclusions. Meanwhile, some insurance companies are offering yet another insurance product that will fill the gap between cyber policies and property and bodily injury coverage—sometimes referred to as DIC insurance coverage. Clearly, with these competing and alternative approaches to coverage, nothing is set in stone, and the insurance industry will likely continue to offer a patchwork solution to cyber perils for the foreseeable future.

The bottom line: do not think your risk management analysis is complete just because you have been handed a policy described as "cyber insurance." It may turn out that your work is only just beginning. ■

Joshua Gold *is a shareholder in Anderson Kill's New York office and chair of Anderson Kill's Cyber Insurance Recovery Group. He regularly represents policyholders in insurance coverage matters and disputes concerning arbitration, time element insurance, electronic data and other property/casualty insurance coverage issues.*

RISK MANAGEMENT

Reprinted with permission from *Risk Management*.

www.rmmagazine.com