The IoT: Interconnectivity and Risk

*By **Carrie Campi, Esq.** Vice President, North American Claims Group and **Richard Mather**, Vice President, North American Claims Group*

Your new smart refrigerator knows when you need milk and eggs, but did you know it could be used in a cyberattack without you even knowing it? All of our fancy "smart" devices including phones, fitness tracking devices, thermostats, cars, etc. are connected to the internet in some capacity. These devices are collectively being referred to as the internet of things or IoT. They have varying levels of security built into them. There have been numerous articles and propositions that the devices may be taken over to possibly open the door of your refrigerator in the middle of the night or take over the navigation of your vehicle. Although these threats may be credible in theory, there have not been many instances of this occurring to date.

There have been instances, however, where security loopholes in connected devices have been utilized to wage what is known as a Distributed Denial of Service attack, otherwise known as a DDOS attack. The attackers gain access to the devices through default passwords (have you changed your router password?), devices which don't have updated security patches, and devices manufactured by companies without a strong security program. Without the owner's or user's knowledge, attackers use devices throughout the country or even the world to send constant communication traffic to a network of the target, essentially locking them up. The motive behind these attacks varies from the sport of someone trying to see if they can do it, a competitor attempting to shut down the competition, or even an attacker attempting to create civil unrest. The attack takes down websites and may stop the target from being able to conduct business for a period of time until they are able to stop the attack. There was a particularly massive attack on October 21, 2016 against Dyn, a domain name service, that impacted large online service providers such as Twitter, Paypal, Comcast and Verizon to name a few, but there are smaller attacks happening on a regular basis.

Other risks are posed by the combination of the IoT and automation of industrial control systems. Even standalone computer controlled industrial control systems have risks. When those systems are connected to the internet, the potential for compromise can be much greater. While public discussion tends to focus on high profile attacks such as the Stuxnet attack on Iran's nuclear facilities, the 2014 German steel mill attack, and various attacks on the oil and gas industry, all IoT connected companies likely have some risk.

Entities with an online presence obviously have a threat of being a target, but even if you are not a traditional online provider, your company may be at risk if one of your service or product providers is the target of an attack. The attack may materially compromise a non-target company's ability to continue conducting business.

CONTINUED >

> Without the owner's or user's knowledge, attackers use devices throughout the country or even the world to send constant communication traffic to a network of the target, essentially locking them up.

Whether there is liability for technology devices a company makes that lacks security controls, a compromise of data when hackers access payment card data through IoT devices, or if the company's business or its vendor's business is shut down due to a cyberattack, a dedicated Cyber insurance policy can respond. As a target company, it is crucial that you have business interruption coverage for cyber disruptions. Another evolving cyber coverage is contingent business interruption, which provides coverage for a non-target entity when their business is impacted by the attack on one of their service and or product providers.

The risk to companies that make devices that are part of the IoT is not even dependent upon actual breaches. Plaintiff's side law firms are working on theories of pre-breach liability, enabling them to sue based on the mere vulnerability to a breach. This greatly expands the universe of potential defendants. At least one plaintiff's firm has a laboratory analyze products for vulnerabilities. Targeted companies are given an opportunity to settle by agreeing to "fix" the vulnerabilities, thereby avoiding the adverse publicity that comes with litigation.

For more information contact carrie.campi@awac.com or rich.mather@awac.com about Allied World's Claims Services.

ABOUT THE AUTHORS

Carrie Campi, Esq.
Vice President, North American Claims Group

Carrie Campi manages the E&O claims team who are responsible for handling claims for Allied World's lawyers errors and omissions (E&O), insurance agents and brokers E&O, technology, privacy, architects and engineers and miscellaneous professional lines. Carrie Campi also is responsible for the Litigation Management team at Allied World whose goal is to ensure that Allied World insureds are provided with an efficient defense. Recently, the group has had to focus on identifying efficient and effective means of dealing with the ever increasing amounts of data that is involved in litigation.

Carrie has over 17 years of professional lines claims experience. Prior to her insurance career, Carrie was a Special Agent with the FBI. Carrie earned her B.S. in business administration at the University of Kansas and her J.D. at Rutgers University School of Law – Camden. She is a member of the Connecticut and Maryland Bars.

Richard W. Mather, Esq.
Vice President, North American Claims Group

Rich is responsible for claims under Allied World's technology errors and omissions ("E&O"), privacy and network security E&O, lawyers E&O, insurance agents and brokers E&O, insurance company E&O, media, and miscellaneous professional E&O lines.

Prior to joining Allied World, Rich spent sixteen years litigating cases in the state and federal courts in Connecticut.

He received his B.A. from the University of Connecticut, his M.A. from Trinity College, and his J.D. from the University of Connecticut School of Law.

ALLIED WORLD | CLAIMS SERVICES