ANDERSON KILL
POLICYHOLDER

October 25, 2016

ALERT

Internet Down?

Insurance May Cover Your Losses after a Denial of Service Attack

By Stephen D. Palley and Daniel J. Healy

A significant amount of U.S. internet service was interrupted late last week by a distributed denial of service, or DDoS, attack on a major domain name server company. A domain name server is like a telephone switchboard — it translates domain names like "www.google.com" into the numeric address needed to route client-side browser requests to the right server. If the "switchboard" is down, traffic can't be routed, and a request to access particular webpages may fail. According to news reports, the recent attack used unsecured internet of things (IoT) devices — that is, internet-connected machines, appliances and objects, ranging from routers to refrigerators and thermostats — to flood the domain name servers with traffic, preventing legitimate users from accessing many major websites.

For many businesses, internet access is as critical as electricity and other basic utilities. Without reliable access to internet functionality, significant financial losses can result. One recent study suggests that a DDoS attack can result, on average, in losses of $40,000 an hour or more.[1] In addition to lost revenue from service interruption, policyholders may also face third-party claims from customers and others for a variety of reasons.

Insurance coverage may play a role in mitigating such losses and likely will depend on the type and extent of claims at issue. First, the affected business should review what insurance coverage it has in place. Most businesses have liability coverage to protect against claims by third parties and it may apply in this context. Key provisions to look for include cyber extensions, exclusions or definitions.

Depending on the length and extent of service interruption, some form of business interruption coverage could be available for some policyholders. This sort of "first party" insurance coverage may be contained within a broad range of policies, from more generic property- and business-owner package policies, to cyber-specific policy forms. Some policy forms may cover purely economic loss, without requiring underlying property damage. This can be the case under a variety of cyber insurance policy forms, including network liability coverages that specifically cover DDoS attacks. Under those policies, coverage will be triggered if the outage is caused by a specified peril, which may include disruption

ANDERSON KILL
1251 Avenue of the Americas
New York, NY 10020
(212) 278-1000 Fax: (212) 278-1733

ANDERSON KILL
1600 Market Street, Suite 2500
Philadelphia, PA 19103
(267) 216-2700 Fax: (215) 568-4573

ANDERSON KILL
1055 Washington Boulevard, Suite 510
Stamford, CT 06901
(203) 388-7950 Fax: (203) 388-0750

ANDERSON KILL
1717 Pennsylvania Avenue, Suite 200
Washington, DC 20006
(202) 416-6500 Fax: (202) 416-6555

ANDERSON KILL
One Gateway Center, Suite 1510
Newark, NJ 07102
(973) 642-5858 Fax: (973) 621-6361

www.andersonkill.com

who's who

Stephen D. Palley is a trial lawyer based in the Washington D.C. office of Anderson Kill. A Fellow of the American College of Coverage and Extracontractual Counsel, Mr. Palley represents policyholders seeking insurance coverage, with a particular focus on emerging technology, software development and the construction industry. Mr. Palley has worked closely with clients in the design and development of a variety of software platforms, and draws on this hands-on experience to advise clients about product development, design and risk transfer and mitigation.

spalley@andersonkill.com
(202) 416-6552

Daniel J. Healy is a partner in Anderson Kill's Washington, D.C., office and deputy co-chair of the firm's Cyber Insurance Recovery practice group. Mr. Healy represents policyholders seeking insurance coverage. As a former trial attorney at the Justice Department, he has extensive experience in courts across the country.

dhealy@andersonkill.com
(202) 416-6547

to service provided by one of the insured's "service providers." For more conventional all-risk or named peril property policies, coverage may still be available, but can require development of facts that show that an outage led to some amount of covered property damage. In both cases, careful attention must be paid to policy language and specific facts at issue in a particular claim.

One issue to anticipate in a business interruption claim is the source of the disruption. The recent attack is different from more conventional DDoS attacks, in that it was directed at the DNS provider, as opposed to individual businesses. In contrast to a targeted DDoS attack focused on a particular business, downtime from a DNS provider attack may be analogous to an attack on a power plant or power transmission facility, as opposed to an attack on any individual company's access to the power grid. How this impacts coverage will depend on policy language, which remains widely variable between insurance companies. While the scope and extent of coverage will depend on specific policy language, lost revenue from this sort of service interruption could potentially fall within a company's "contingent business interruption" coverage. Other issues may also arise here, including appropriate documentation of losses, as well as time-element deductibles specifying minimum, or sub-limits specifying maximum, periods of covered loss.

While risk managers and general counsel may be focused initially on first-party losses, third-party insurance may also be available. For example, product manufacturers facing liability claims alleging that faulty or insecure software or hardware played a role in the attack may look to cyber policies, as well as protection afforded by traditional CGL, D&O and E&O policies, depending on the claims at issue. While non-cyber policies often contain exclusions that insurance companies might argue apply to DDoS-related claims, policy language is still evolving and not completely uniform.

As technology continues to march forward, insurance policies will provide some measure of protection for policyholder losses and claims by third parties. Careful review of policy language, whether pre-loss when insurance is being secured, or post-loss, will help maximize the amount of coverage that is available.

1 "Incapsula Survey: What DDoS Attacks Really Cost Businesses," available at https://lp.incapsula.com/rs/incapsulainc/images/eBook%20-%20DDoS%20Impact%20Survey.pdf (last visited 10/24/2016).