Consider Cyberliability and Network Business Interruption Insurance Coverage in Light of Recent DDoS Internet Attack

At a Glance…

The October 21, 2016 DDoS attack on the internet’s domain name system infrastructure underscores the need to consider cyberliability insurance coverage as a critical component of your company’s security and privacy breach response plan, and if your company carries cyberliability insurance, to ensure that your coverage will respond to a network business interruption, security breach or privacy event against or within your company or its vendors.

The Eastern United States experienced a massive internet outage on the morning of October 21, 2016, as Americans started to arrive at work. The outage disrupted access to a number of major websites and online services throughout the United States and Europe. Although the outage initially appeared to subside, it flared up again as West Coast users logged on at the beginning of their work day. And again, just as connectivity appeared to be stabilizing, the disruption further spread late in the afternoon. The October 21 internet outage appear to have been caused by a series of distributed denial-of-service (“DDoS”) attacks directed at the domain name system (“DNS”) infrastructure maintained by Dyn Inc., which essentially works as a phonebook for navigating parts of the internet. A DDoS attack deliberately floods a targeted system with superfluous, junk traffic requests in order to overload the system and prevent it from fulfilling legitimate requests. Disrupting the DNS infrastructure left internet users and major websites unable to navigate the web or communicate with each other.
Perhaps more remarkable than the unprecedented severity of the DDoS attack on Dyn is the manner in which it was reportedly launched: hackers were able to temporarily bring down large portions of the internet by hijacking the Internet of Things (“IoT”). Dyn and its data centers received malicious requests from tens of millions of unique internet protocol (“IP”) addresses that may have been harvested by “Mirai,” malware that scans the internet for connected devices with weak login credentials, such as web cameras and thermostats and other internet connected household devices, on which weak factory default passwords have not been changed or set.

**Cyberliability insurance may be a critical part of your company’s security and privacy response plan**

There are a number of ways companies may protect themselves, their personnel, their computer networks and their customers, and their financial health, from the damage caused by a security or privacy breach, including incidents that originate outside of the organization. Insurance, including cyberliability coverage, should be considered a critical component of those protections.

Cyberliability insurance typically covers the costs of investigating, responding to and terminating an actual or suspected security or privacy breach, often including the fees, costs and expenses to retain counsel to determine notification obligations, to retain forensic investigators, to retain communications and public relations professionals, to provide notification to potential affected persons, and to provide remedial services, such as credit file monitoring. In addition, cyberliability insurance covers liability arising from an alleged failure to prevent a security or privacy breach, or the disclosure of protected confidential information, including the costs of defending against claims by affected parties.

In addition, because it covers both first-party losses and third-party liabilities, cyberliability insurance policies often have complex loss or claim-reporting requirements. Cyberliability policies may require the insurer’s prior consent to retain professionals and incur costs to respond to a security or privacy breach, even if the initial costs are within a self-insured retention or deductible. The obligation to promptly report a loss may also be triggered by the “discovery” of the loss by any person within the organization, including lower-level employees. Accordingly, it is important that companies have in place clear lines of communication between personnel in a position to potentially discover covered events or losses (such as persons in the company’s information technology or security departments) and management with knowledge of the company’s insurance coverage and its reporting requirements.
Does your company's cyberliability insurance include network business interruption coverage?

Network Business Interruption ("NBI") insurance covers certain business income losses directly caused by a company's actual and measurable interruption, suspension, failure, degradation or delay in a company's computer network caused by a security breach. Although the scope and wording of cyberliability insurance policies can vary significantly from insurer to insurer, many cyberliability insurance carriers include NBI coverage as part of their standard cyberliability policy form, or will add it to a policy by endorsement.

Does your company's cyberliability policy cover losses or claims arising from DDoS attacks?

Cyberliability insurance generally responds to security and privacy breaches caused by malicious or negligent conduct caused by outsiders or employees. It is important to ensure that the types of breaches expressly covered by your company’s policy broadly include DDoS attacks, as well as intrusions by hacking, malicious acts by “rogue” insiders, and negligent acts, such as the loss of hardware or disclosure of passwords or credentials.

Does your company's cyberliability policy cover losses or claims as a result of attacks on or disruptions to third-party computer systems?

Many companies rely on vendors to provide essential data and network services, such as cloud and application hosting, data storage and data processing. Many cyberliability insurance policies cover the liability risks your company faces in the event a security or privacy event occurs at a third-party vendor, but some do not, and the scope of coverage available under particular policies may vary.

As the cyberliability insurance market continues to mature and evolve, policyholders should be aware of the scope of available coverage, and should seek assistance when negotiating new or renewal cyberliability insurance to ensure they obtain the most comprehensive coverage available to fit their needs.