Insurance BUSINESS AMERICA

Department of Homeland Security reveals top sector at risk for cyber attacks

by Caitlin Bronson | Aug 14, 2015

The increasing importance of cyber risk insurance has been well-documented, but new information suggests one industry is more at risk of cyberattacks than any other. According to data from the Department of Homeland Security (DHS), more than 50% of investigated cyber incidents from October 2012 to May 2013 occurred within the energy sector.

Specifically at risk are power and utilities companies, which provide heat and electricity to homes and businesses across the US.

To help bolster client safety, producers advising energy companies on cyber security need to do more than provide industry-appropriate coverage, advised global broker Marsh, which compiled a report on the DHS statistics.

Energy company clients will need advice on proper employee training, system penetration testing and periodic treat assessment reviews. Producers should also work with clients to develop an effective plan of action if attacks do occur.

“Definitely have a response plan. It will limit a lot of confusion and costs,” said Jake Kouns, chief information security officer at Risk Based Security. Kouns recommended having a forensics team on alert to investigate the attack, as well as a system for notifying “the affected state agencies.”

That latter piece of advice is something many companies in the energy industry don’t follow. Marsh noted that in all of 2012, just 198 cyberattacks were reported to the government.

Christine Marciano, president of Cyber Data-Risk Managers and specialist in cyber security, says the attacks on the energy sector represent a growing trend in cyber attackers’ motivations—instead of stealing information for financial gain, attackers are now seeking to cause as much havoc as possible.

Insurance BUSINESS AMERICA

“[Attackers] have political agendas with a political motivation,” Marciano said. “Their attacks can impact political structure through the corruption and destruction of our critical infrastructure systems…targeting and potentially harming civilians, causing havoc and property damage and generating fear.”

If they are successful, the results could be disastrous both for the company and their customers.

“A power grid interruption as a result of a cyberattack has the potential to cost utilities and other infrastructure facilities millions of dollars in lost revenue, regulatory fines, and additional expenses to restore operations and to improve cyber securities defenses, not to mention reputational damage,” said Matt McCabe, a senior advisory specialist with Marsh’s Network Security and Privacy Practice.