The North Korea Gap in Your Cyber Insurance

By: Brandy Worden, Esq. CIPP/US

North Korea's Cyber Extortion Campaign

North Korea was recently identified as the powerhouse behind the WannaCry ransomware attack that swept across 150 countries and 200,000 computers. Panicked hospitals cancelled thousands of operations, ambulances were diverted, and concerns about security of individual medical information bubbled to the surface. But, it struck more than hospitals. Businesses of all types and sizes were forced to contend with the expensive aftermath of WannaCry, which included:

- Interrupted business operations;
- Paying ransom demands;
- Fear of losing their data;
- Reputational damage;
- Expensive security assessments to evaluate if personally identifiable information had been compromised; and
- At times, actually footing the bill for data breach notification to affected consumers.

Businesses should evaluate their business practices and insurance policies to find what ways they can offset the risk and kinds of costs arising out of these kinds of attacks.

The Four Steps Your Company Should Take To Protect Itself

Step One - Get Cyber Insurance: Ransomware is only one potential attack your business faces, but it can be quite costly. Traditional insurance policies often do not cover ransomware damages. Fortunately, your business can obtain coverage for ransomware attacks, and many other types of cyber-attacks, through a cyber insurance policy. As discussed further below though, to maximize coverage you must carefully review any potential cyber policy.

Step Two - Update Software: Many insurance policies predicate coverage on the insured taking reasonable steps to ensure cyber security. It was determined that WannaCry took advantage of a vulnerability in a Microsoft operating system. This particular vulnerability was identified months before the attack and Microsoft had issued a patch for it. Some carriers may take the position that this was failure to take reasonable cyber security measures and deny coverage. Ensuring your business has protocols in place to regularly update software will help prevent attacks and will also help protect your coverage.

Step Three - Demand Removal of Any Nation-State Exclusions in Your Cyber Policies: Some cyber policies expressly exclude coverage for actions by nation states. As a result, your carrier might argue there is no coverage if it is determined that a country like North Korea is behind the attack. This exclusion

may impact more than just the ransomware provision of your company's policy since North Korea has been identified to be behind a variety of attacks – not just ransomware. (Similarly, other nation states have been identified as being involved in attacks against U.S. companies, like Russia and the Yahoo breach.) Additionally, coverage under cyber policies is often broken down into multiple "modules" for various types of claims. You may need coverage for a ransomware attack under various modules. For example, the ransomware module may cover the ransom itself, while the business interruption module may cover the income your business lost as a result of the inability to access data.

Step Four - Enlist Coverage Counsel to Review Your Company's Cyber Risk Management Program: Given the scale of the ransomware attacks, and the perception of nation state involvement, this trend is unlikely to stop. Therefore, it is important for companies to take actions to effectively manage these risks now. The types of exclusions and gaps that appear in cyber coverage can be complex and difficult to identify. Enlisting the assistance of experienced coverage counsel to navigate coverage for the ever-evolving cyber security landscape can help ensure your company's resilience to these attacks.

Taking these steps can be valuable to minimize the financial and reputational costs to your business and keeping your costumers happy in the face of nation-state threat actors like North Korea.

For assistance reviewing your coverage, please contact the firm's managing partner, Jeff Dennis, Esq. based in the Newport Beach office (949.854.7000; jeff.dennis@ndlf.com) or Las Vegas office managing partner, Nathan Owens, Esq. (702.777.7500; nathan.owens@ndlf.com).

ABOUT NEWMEYER & DILLION LLP

For more than 30 years, Newmeyer & Dillion has delivered creative and outstanding legal solutions and trial results for a wide array of clients. With over 70 attorneys practicing in all aspects of business, employment, real estate, construction and insurance law, Newmeyer & Dillion delivers legal services tailored to meet each client's needs. Headquartered in Newport Beach, California, with offices in Walnut Creek, California and Las Vegas, Nevada, Newmeyer & Dillion attorneys are recognized by The Best Lawyers in America©, and Super Lawyers as top tier and some of the best lawyers in California, and have been given Martindale-Hubbell Peer Review's AV Preeminent® highest rating.

For additional information, call 949.854.7000 or visit www.ndlf.com.