CYBERSECURITY INSURANCE AND THE NEED FOR A STANDALONE CYBER PRODUCT

By: Daniel A. Cotter, Esq.

In the last several months of 2017, many computers around the world were attacked by the Wannacry and Petya[1] ransomware programs. Ransomware attacks have increased in the last year[2] and insureds need to consider exposure to damages such as reputational risk, business interruption, and other losses. These recent ransomware attacks should also focus the attention of both insureds and insurers to review both the coverages or exclusions under traditional insurance policies as well as consider the need for a standalone insurance product to address cybersecurity risks.

Recent ransomware attacks should focus attention on need for a stand-alone insurance product to address cybersecurity risks… traditional policies specifically exclude cybersecurity coverage…

Coverages Implicated by Cybersecurity

Cybersecurity attacks implicate a number of potential insurance coverages and exposures, including these common categories: Third-party information security and privacy coverage; Privacy notification; crisis management and public relations; Business interruption; Cyber extortion threats; Data recovery; regulatory defense and penalties; Website and off-line media liability; PCI fines, penalties and assessments; Forensic services to help determine the extent of the breach and the steps needed to comply with applicable breach notice laws; and Credit Monitoring.

Without a standalone cybersecurity insurance policy, it can be a difficult process to determine whether a traditional insurance policy provides coverage for a cybersecurity attack and if so, to what extent that policy provides coverage. Some traditional policies have specifically excluded cybersecurity from coverage. A standalone cyberinsurance policy may be the best way to address this issue.

Ransomware Attack

A ransomware attack is one in which the hacker prevents the attacked computer(s) from operating, usually by encrypting the victim's data and demanding a payment, usually in bitcoin – the "ransom" – to decrypt the data.

A Standalone Product

The current market for cybersecurity insurance is estimated at $2.5 to $3.5 billion in annual premiums, with that number expected to triple by 2020.[3] Insureds in the United States represent the vast majority of cybersecurity coverage purchasers in the world.[4] One challenge in determining a more precise estimate of the size of the cybersecurity insurance market is that many insurers include some form of cybersecurity coverage in their traditional property and casualty ("P&C") products, and it is difficult to allocate the amount of premium attributable to that cybersecurity coverage.

A standalone insurance product is one that is designed to provide insurance protection for a "specific risk or cost"[5] and affords an insured coverage for a particular concern. The concept of standalone coverage has been around for some time, but it developed quickly during the late 1990s when many in the insurance industry were addressing a way to cover risks for Y2K that were excluded under traditional P&C policies.[6]

The market for cybersecurity insurance is estimated at $2.5-$3.5 billion in annual premium… tripling by 2020….with the vast majority of purchasers in the US.

A standalone cyberscurity insurance product potentially can address ransomware attacks. In some standalone cybersecurity insurance policies, "extortion coverage" is included and is intended to cover ransom attacks and the resulting work required to prevent future attacks.

Conclusion

The continued growth of standalone cybersecurity insurance products offers a number of potential

Continued on page 18

During the Q & A that followed, it was clear that there was disagreement among the panel members on the meaning and benefits that would be derived if the Covered Agreement were approved as it was presented to Congress.

From the divergence of opinion, it seemed clear that there are ambiguities in the Covered Agreement that leave the terms open to numerous interpretations. For the initial intent of the Agreement to be effective, this author believes that "tweaking" is required to ensure that the U.S. not only be deemed "equivalent" upon the execution of the Agreement, but also that U.S. insurers and policyholders will be protected. Clearly, that did not happen and it remains to be seen what the Trump administration Policy Statement will provide regarding the implementation of the terms of the Covered Agreement.

The author believes that "tweaking" is required for the Covered Agreement, to ensure that the US is not only deemed "equivalent", but that US insurers and policyholders will be protected.

Prior to the U.S. consent to sign the Covered Agreement, on May 30, 2017, the EU received authorization to sign the Covered Agreement and the EU countries have 24 months from execution to revise their laws so that U.S. insurers and reinsurers can operate in the EU without having to establish a branch office or a local subsidiary.

CYBERSECURITY INSURANCE...

Continued from page 9

benefits to insurers and insureds alike, including better understood needs for the insurance and increased clarity regarding what is covered. Insureds need to review their policies for cybersecurity coverage and consider purchasing a standalone to better address the ransomware attacks that have become more prevalent, if the Wannacry and Petya attacks are any indication of what is likely to come.

Dan Cotter is a partner at Butler Rubin Saltarelli & Boyd LLP, where he chairs the Insurance Regulatory and Transactions practice and is a member of the Cybersecurity and Privacy practice. He obtained his CIPP/US in 2016.

1 The Petya ransomware attack hit a number of organizations around the world, including the law firm DLA Piper.

2 The Department of Justice estimates that the number of ransomware attacks has increased in the last year to 4,000 per day. Most are smaller and not of the magnitude of Wannacry or Petya.

3 Heller, Mark, "Cybersecurity Insurance Market to Triple by 2020," CFO.com, http://ww2.cfo.com/risk-management/2015/09/cyber-insurance-market-triple-2020/.

4 *See* Souter, Gavin, "Global ransomware attack hits cybersecurity insurers, but losses limited," Business Insurance, available at http://www.businessinsurance.com/article/20170515/NEWS06/912313427/Global-ransomware-WannaCry-attack-hits-cyber-insurers-losses-limited ("the United States is by far the biggest market for cybersecurity insurance").

5 Hartman, Dennis, "What is Standalone Insurance?," Sapling, available at https://www.sapling.com/8597896/standalone-insurance.

6 *See, e.g.*, "Cybersecurity insurance continues to evolve," available at http://www.agcs.allianz.com/insights/expert-risk-articles/cyber-insurance-continues-to-evolve/ ("Standalone cybersecurity insurance can trace its roots to 'Y2K' and the infamous 'Millennium bug'. Concerns that programming issues associated with the Year 2000 date change would cause widespread computer system failure prompted many companies to first assess the potential for cybersecurity risk to their businesses.")

AROUND THE STATES:...

Continued from page 10

sclerosis, Crohn's disease, mitochondrial disease, Parkinson's disease and sickle cell disease.

Vetoed: ***Expansion of Insurers' Permissible Payment Means*****:** Georgia Governor Nathan Deal vetoed HB 174 which would have amended Georgia Insurance Code Section 33-24-43 to expand the means by which insurers may pay insurance policy benefits or covered losses to include wire transfers, cashier's checks, bank checks and drafts, electronic funds transfers and other forms of electronic payments, general use gift cards without any expiration date, dormancy or non-use fee and any other payment method that the Georgia Insurance Commissioner may approve.

Brian T. Casey, Esq., is the Co-Chair of the Regulatory & Transactions Insurance Practice Group, Locke Lord LLP (Atlanta), bcasey@lockelord.com, (404) 870-4638. He is also a member of the ABA TIPS Insurance Regulation Committee.