BCLP. Client Intelligent

Insights

NYDFS: CYBER INSURERS SHOULD NOT PAY RANSOM AND SHOULD ADOPT "BEST PRACTICES"

Feb 10, 2021

SUMMARY

On February 4, 2021, the New York Department of Financial Services (NYDFS) issued Circular Letter No. 2, "*Cyber Insurance Risk Framework*" to all property-casualty insurers authorized to transact insurance in New York. Concerned with escalating cyber insurance claims, the NYDFS has identified seven "Best Practices" that insurers should adopt in order to better manage cybersecurity risk. These "best practices" are outlined in its Circular Letter as a "Cyber Insurance Risk Framework" (Framework).

The Circular Letter includes a somewhat controversial recommendation against insurers covering ransom payments. It also recommends that an insurer's senior management and directors be formally involved in managing cyber risk. So while the recommendations in the Circular Letter and Framework do not currently have the "force of law", insurance industry participants should understand how their interests could be affected by adoption of the Framework.

Background

The Framework is the result of an intensive, year-long effort by the NYDFS to better understand cyber risk and its financial effect on insurers, including those issuing cyber insurance coverage. The NYDFS has been consulting with cyber security experts, insurance entities and regulators and has collected and analyzed detailed cyber insurance data from several insurers in 2020. While NYDFS views Cyber Insurance as an essential coverage, it is concerned about ever-increasing cyber attacks and resulting insurance claims, and their financial impact on insurers writing Cyber Insurance coverage.

Ransomware and Ransom Payments

NYDFS is particularly concerned with ransomware attacks, as they have caused massive losses and claims brought simultaneously by multiple insureds, each suffering damages from the same cyber incident, such as the SolarWinds' Orion software attack disclosed in December 2020 and the

June 2017 NotPetya cyberattack. The NYDFS notes that ransomware attacks practically doubled in the past year, with costs skyrocketing to approximately $20 Billion.

In the Circular Letter's preface, the NYFS describes ransom payments as potentially encouraging future ransomware incidents and states that it "***recommends against paying ransoms***."

Although this recommendation isn't actually included in the list of 7 Best Practices (an important omission), it will generate the most attention in the insurance industry. The NYDFS and most other insurance regulators are familiar with the arguments for and against allowing ransom reimbursement (for example - paying ransom may encourage future attacks and demands; but allowing ransom reimbursement can be less costly than paying losses incurred recovering lost data.)

Thus far, state legislators and regulators have not expressly prohibited ransomware payments and most recognize the potential complications in doing so:

- Cyber Insurance (and reinsurance) premiums may become cost-prohibitive. There are already concerns about adequate availability of reinsurance for cyber risk.
- A blanket prohibition on ransom payments could dissuade companies from purchasing Cyber Insurance. For many insureds, the prospect of having to recover lost data through back-up systems is overwhelming. Some insureds may not view Cyber Insurance as useful if they know in advance that reimbursement of a small ransom payment (and quick data recovery) is not even an option.
- Healthcare, hospital, law enforcement and other services will expect to have systems restored ASAP regardless of how that is accomplished.
- Beyond an insured's business interruption losses, prolonged data recovery could significantly impact the insured's clients and the general public.

While the Framework is not (at the moment) binding precedent, the NYDFS warns insurers that they could be breaking federal law by making ransom payments. The NYDFS describes insurers as an "intermediary" that could be held liable under rules established by OFAC to the extent a payment recipient (an attacker) is included on OFAC's Specially Designated Nationals and Blocked Person's (SDN) List or if a payment is made to a jurisdiction covered by an embargo.

In addition to ransom payment reimbursement, the NYDFS is also concerned with:

- Insurance industry exposure to cyberattack losses under more general insurance policies, i.e., ones that do not *expressly* cover cyber risk. The NYDFS refers to this as "non-affirmative" or "silent" cyber risk.

- The need to adequately price cyber risk, both to ensure claims can be paid and to incentivize insureds to fill gaps in their cyber security program (to lower their premiums.)
- "Systemic risk" to insurers when cyber incidents affect multiple industries covered under Cyber Insurance policies.

Framework Summary

Overall, the Framework encourages Cyber Insurance carriers to better manage, price and account for cyber risk. In summary, the Framework recommends that insurers:

- Establish a formal strategy for measuring and managing Cyber Insurance risk. The strategy should be directed and approved by Senior Management & Boards of Directors (or other governing body) and incorporate each key practice listed in the Framework.
- Manage and eliminate exposure to "silent" Cyber Insurance Risk by:
  - Evaluating potential exposure, particularly under combined coverage policies and certain stand-alone coverages such as errors & omissions, burglary/theft, and product liability policies;
  - Making clear in a non-cyber insurance whether the policy provides or excludes coverage for cyber-related losses; and
  - Purchasing reinsurance.
- Evaluate systemic risk, particularly through third-party vendors with high concentration in cloud services, and plan for catastrophic events such as self-propagating malware (such as NotPetya), supply chain attacks (SolarWinds trojan) or events that disable a major cloud services provider. Evaluations should include cybersecurity stress testing.
- Rigorously measure insured risk through data-driven, comprehensive assessments of each insured's (and potential insured's) cyber risk, including gathering detailed information related to an institution's cybersecurity program and corporate governance and controls, as well as vulnerability management, access controls, encryption, endpoint monitoring, boundary defenses, incident response planning and third-party security policies.
- Educate insureds and insurance producers about how to reduce cyber risk exposure and provide financial incentives for insureds to improve their cybersecurity.
- Obtain cybersecurity expertise, recruiting employees with relevant experience and commit to training and development.

- Include a requirement in Cyber Insurance policies that victims notify law enforcement, which can help insureds recover lost data and funds, as well as prosecute attackers and warn others.

RELATED PRACTICE AREAS

- Insurance
- Data Privacy & Security

MEET THE TEAM

Amy de La Lama

Boulder

amy.delalama@bclplaw.com
+1 303 417 8535
