February 12, 2021

New York Department of Financial Services Issues Cyber Insurance Risk Framework

The DFS Issues Guidance to Insurers on Best Practices to Manage Their Cyber Insurance Risk

SUMMARY

On February 4, 2021, the New York State Department of Financial Services (the "DFS") issued Insurance Circular Letter No. 2 (2021), which includes a "Cyber Insurance Risk Framework" (collectively, the "Framework"), to outline what the DFS describes as best practices for managing cyber insurance risk. Among other things, the Framework urges all property and casualty insurers licensed in New York to establish a cyber risk insurance strategy directed and approved at the insurers' highest levels and identifies principles to consider when developing an effective and sustainable program in response to the ever-heightening risks posed by cyber events.

BACKGROUND

As the DFS notes in issuing the Framework, cyber insurance is playing an increasingly important role in managing and mitigating cyber risk as the frequency and severity of cybercrime increase. According to the DFS, the U.S. cyber insurance market is estimated to increase six-fold by 2025 over the 2019 market, from $3.15 billion to over $20 billion.[1]

In issuing the Framework, the DFS notes that while cyberattacks take many forms, in its view, ransomware[2] in particular has been the "biggest driver" in the increasing damage done by cybercrime. For example, the 2017 "NotPetya" global ransomware attack that spread from Ukraine to some of the largest businesses worldwide led to $3 billion in insurance claims, of which $2.7 billion were made under property or casualty policies that were silent about cyber events.[3] In addition, according to a survey conducted by the DFS,

from early 2018 to late 2019, the number of insurance claims arising from ransomware increased by 180%, and the average cost of those claims rose by 150%.[4]

As part of the Framework, the DFS recommends that insurance companies not make ransom payments in response to ransomware attacks because ransom payments "fuel the vicious cycle of ransomware, as cybercriminals use them to fund ever more frequent and sophisticated ransomware attacks." The DFS refers to October 2020 guidance from the U.S. Department of Treasury's Office of Foreign Asset Control ("OFAC") warning that intermediaries (including insurers) of ransom payments can be liable for ransom payments made to sanctioned entities. The DFS further notes that the Federal Bureau of Investigation counsels against paying ransom, in part because paying a ransom does not guarantee that an organization will regain access to its data or that the data will not be released publicly.

THE FRAMEWORK

With a stated goal of "foster[ing] the growth of a robust cyber insurance market that maintains the financial stability of insurers and protects insureds," the Framework outlines "best practices for managing cyber insurance risk" and is the result of "extensive consultation with industry, cybersecurity experts, and other stakeholders." The DFS advises that "all authorized property/casualty insurers [licensed in New York] that write cyber insurance should employ" seven particular practices to sustainably and effectively manage their risks, in a manner proportionate the insurer's cyber insurance risk.[5] These practices include:

1. **Establish a Formal Cyber Insurance Risk Strategy.** The Framework counsels insurers to have a formal strategy, directed and approved by senior management and the board of directors, for measuring and assessing cyber insurance risk. Establishing such a strategy and ensuring that it is appropriately resourced and prioritized can be effective in conveying the seriousness of the risk through a tone from the top. The strategy should incorporate all of the six key practices identified below, and progress against the strategy goals should be reported to senior management and the board of directors on a regular basis.

2. **Manage and Eliminate Exposure to Silent Cyber Insurance Risk.** The Framework identifies "silent" or "non-affirmative" cyber insurance risk as the risk that an insurer must cover loss from a cyber incident under a policy that does not explicitly mention cyber risks. The Framework indicates that silent risk can be found in various combined coverage or stand-alone policies, including errors and omissions, burglary and theft, general liability and product liability insurance. Silent cyber-related risks covered in a policy may not be effectively assessed or priced, and expose insurers to unexpected losses. To manage this exposure, the DFS encourages insurers to make clear in policies that could be subject to cyber-related claims whether the relevant policy provides or excludes coverage for cyber-related losses, and should seek to take steps to mitigate existing silent risk by, for example, purchasing reinsurance.

3. **Evaluate Systemic Risk.** Cyber risks pose unique systemic risks not seen in other insured areas. Insureds are relying on an increasing number of third party vendors and providing those vendors access to many of their networks. Insurers should evaluate insureds' use of third parties to better understand and to model the systemic risk that a catastrophic attack could present simultaneous losses to many of their insureds.

   The DFS identifies several examples of cyber events that could present systemic risk, such as an attack by self-propagating malware or a supply chain attack that infects many institutions at

the same time. The DFS also identifies cyber events against major cloud services providers as a potential source of systemic risk.

In addition, the DFS advises that insurers should conduct "internal cybersecurity stress tests based on unlikely but realistic catastrophic cyber events." These tests are designed to assess possible loss in adverse scenarios and should include modeling exposure across industries, by type and size of the insured, and by the type of insurance offered. The cyber insurance risk strategy should account for possible losses identified in these stress tests.

4. **Rigorously Measure Insured Risk.** The DFS suggests a "data-driven" plan for assessing the cyber risk of each insured and potential insured that involves analyzing their "corporate governance and controls, vulnerability management, access controls, encryption, endpoint monitoring, boundary defenses, incident response planning and third-party security policies." This could involve surveys, interviews and third party sources such as external cyber risk evaluations. The Framework recommends that this information should be compared with past claims data to identify specific gaps in cybersecurity controls. The DFS notes in this respect that in its view cyber risk correlates with the caliber of the insured's cybersecurity program, and that insurers that do not effectively measure the cyber-related risks of their insureds "risk insuring organizations that use cyber insurance as a substitute for improving cybersecurity, and pass the cost of cyber incidents on to the insurer" and that, "[w]ithout an effective ability to measure risk, cyber insurance can therefore have the perverse effect of increasing cyber risk."

5. **Educate Insureds and Insurance Producers.** Insurers that offer cyber insurance are well placed and incentivized to educate their insureds about cybersecurity and reducing the risk of cyber incidents. The Framework commends certain insurers that "already offer their insureds guidance, discounted access to cybersecurity services, and . . . cybersecurity assessments and recommendations for improvement." The DFS also encourages insurers to educate insurance agents and brokers to convey to potential insureds the need for, benefits of, and limitations to cyber insurance.

6. **Obtain Cybersecurity Expertise.** Critical to the development and implementation of an effective cybersecurity strategy, insurers should have the expertise required to properly understand and evaluate cyber risk. Insurers should recruit employees with cybersecurity experience, supplemented as need be with consultants or vendors.

7. **Require Notice to Law Enforcement.** The Framework encourages insurers to require that victims of cybercrime notify law enforcement of cyber events.[6]

DISCUSSION

The Framework demonstrates the DFS's continued focus on the cybersecurity threats facing the entities which it supervises, and the DFS's particular focus on systemic cyber risk and ransomware as issues of concern for the insurance sector. The DFS's recommendation that insurers require insureds to make law enforcement notification is also a novel approach to increasing law enforcement awareness of cybercrime matters that could have effects throughout and beyond the insurance industry.

Systemic Risk. The release of the Framework comes less than two months after the public reporting of the cyberattack at SolarWinds, one of the most significant cyberattacks in history. In December 2020, public reporting indicated that certain software manufactured by SolarWinds, a U.S. company, and widely used throughout U.S. public and private sector networks, had been infected with malware that could be particularly harmful and difficult to detect. This "supply chain" cyberattack, which infiltrated third party

networks through SolarWinds software, affected as many as 18,000 public and private sector entities, including widely reported compromises at various U.S. federal agencies and technology companies. The DFS subsequently reported that the "adversary responsible for the compromise is sophisticated, well-resourced, and persistent," and public reporting has widely identified the adversary as Russia.[7]

The issuance of the Framework underscores the DFS's concern that widespread compromises such as that involving SolarWinds present a systemic risk to the entities that the DFS regulates and the financial system more broadly. With the cyber insurance market growing rapidly but still relatively new, it may be difficult to detect—and thus for insurers to adequately anticipate, price, and prepare for—systemic cyber risks that may impact many insureds concurrently. These concerns are exacerbated by the ever-evolving nature of the cyber threat, including the relatively recent rise of widespread ransomware attacks, and the inherent interconnectedness of institutions' networks that make it possible for compromises quickly to affect many entities at once. The DFS's concern about the challenge and importance of understanding an institution's cyber risk is shown most clearly in the Framework's emphasis on the "silent risks" of cyber incidents to insurers, the need for insurers to adopt a cyber risk strategy at the highest levels of the company, and the need for insurers to have access to sufficient cybersecurity expertise in making risk assessments.

Ransomware. Like U.S. law enforcement and other agencies, the Framework recommends that companies not pay ransom when subject to a ransomware attack, but the Framework does not purport to prohibit insurers *per se* from paying or covering ransom payments. In doing so, the Framework reveals a particular challenge for companies and their insurers. On the one hand, companies may seek insurance that covers ransom payments as part of their overall cyber risk management. On the other hand, when companies pay a ransom (and, by extension, when insurers make it easier for companies to decide to pay a ransom by providing coverage for the payment), they may inadvertently "fuel the vicious cycle of ransomware."

Law Enforcement Notification. The Framework's recommendation that insurers require insureds to provide notification to law enforcement is novel. Like the requirements imposed by its first-in-kind cybersecurity regulation,[8] the DFS's recommendation in this regard could have effects throughout and beyond the insurance industry, not limited to companies regulated by the DFS, to the extent it becomes a model for other regulators. The recommendation is likely to be welcomed by law enforcement officials who have long encouraged victims of ransomware and other cyberattacks to come forward even if they are not legally required to do so, and aligns with recent guidance by OFAC that encourages companies that are victims of ransomware attacks to engage with law enforcement.[9]

* * *

ENDNOTES

1 NYDFS, Insurance Circular Letter No. 2 (2021): Cyber Insurance Risk Framework (February 4, 2021), *available at* https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02.

2 Ransomware is a form of malicious software designed to block access to, and often encrypt, computer systems or data unless the victim makes a requested ransom payment in exchange for providing a method to decrypt it. The attacker may also copy the victim's data in the course of the attack and threaten to sell or publish the data if the ransom is not paid.

3 NYDFS, Insurance Circular Letter No. 2 (2021): Cyber Insurance Risk Framework (February 4, 2021), *available at* https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02. Silent risk may exist in a variety of policies, including those that provide business interruption, errors and omissions, burglary and theft, general liability, product liability, or kidnap and ransom coverage. *Id.*; *see also* Reuters, Companies use kidnap insurance to guard against ransomware attacks (May 19, 2017) *available at* https://www.reuters.com/article/us-cyber-attack-insurance/companies-use-kidnap-insurance-to-guard-against-ransomware-attacks-idUSKCN18F1LU.

4 NYDFS, Insurance Circular Letter No. 2 (2021): Cyber Insurance Risk Framework (February 4, 2021), *available at* https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02. Industry reports confirm this extreme rise in cyber insurance claims. In November 2020, one insurer reported a 950% increase in cyber insurance claims over the last three years. Allianz Global Corporate & Specialty, Managing the Impact of Increasing Interconnectivity: Trends in Cyber Risk (October 2020), *available at* https://www.agcs.allianz.com/news-and-insights/news/cyber-risk-trends-2020.html. Another insurer reported that the manufacturing sector saw a 156% increase in cyber incidents during the first quarter of 2020 over the final quarter of 2019. Beazley Group, The enduring threat of ransomware (June 9, 2020), *available at* https://www.beazley.com/news/2020/beazley_breach_insights_june_2020.html.

5 DFS also notes that "property/casualty insurers that do not write cyber insurance should still evaluate their exposure to 'silent risk' and take appropriate steps to reduce that exposure." NYDFS, Insurance Circular Letter No. 2 (2021): Cyber Insurance Risk Framework (February 4, 2021), *available at* https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02.

6 *Id*.

7 NYDFS, Supply Chain Compromise Alert (December 18, 2020), *available at* https://www.dfs.ny.gov/industry_guidance/industry_letters.

8 23 NYCRR Part 500. See our memoranda to clients "New York Department of Financial Services Issues Proposed Cybersecurity Regulations," dated September 19, 2016, and "DFS Issues Updated Proposed Cybersecurity Regulations," dated January 3, 2017.

9 For additional information regarding ransomware attacks and the October 2020 guidance issued by the Department of Treasury, see our memorandum "Treasury Department Issues Advisories on Ransomware Attacks," dated October 2, 2020.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.