Insurance Circular Letter No. 2 (2021)

February 4, 2021

TO: All Authorized Property/Casualty Insurers

RE: Cyber Insurance Risk Framework

REGULATORY REFERENCE: 23 NYCRR 500

Introduction

As cybercrime becomes more common and costly, cyber risk continues to increase for all organizations. The COVID-19 pandemic has shifted more of our work and lives online, and this shift has introduced new vulnerabilities that cybercriminals are aggressively exploiting.[1] From the rise of ransomware to the recently revealed SolarWinds-based cyber-espionage campaign, it is clear that cybersecurity is now critically important to almost every aspect of modern life – from consumer protection to national security. This is why DFS has led by promulgating the nation's first cybersecurity regulation for financial services in 2017 and creating its Cybersecurity Division in 2019.

Cyber insurance plays a key role in managing and reducing cyber risk. This is a relatively new area of insurance for most insurers, but one that has grown rapidly. In 2019 the U.S. cyber insurance market was $3.15 billion.[2] It is estimated that by 2025, it will be over $20 billion.[3] And these numbers understate insurance coverage of cyber risk, as many insurance claims arising from cyber incidents are submitted under non-cyber insurance policies. As the insurance regulator for New York, our goal is to facilitate the continued growth of a sustainable and sound cyber insurance market.

A robust cyber insurance market that effectively prices cyber risk will also improve cybersecurity. By identifying and pricing risk created by gaps in cybersecurity, cyber insurance can create a financial incentive to fill those gaps to reduce premiums.[4] By driving improved cybersecurity and cyber risk management, cyber insurance can also benefit consumers who entrust their sensitive data to these organizations.

To foster the growth of a robust cyber insurance market that maintains the financial stability of insurers and protects insureds, we have created a Cyber Insurance Risk Framework that outlines best practices for managing cyber insurance risk (the "Framework"). The Framework is based on our extensive consultation with industry, cybersecurity experts, and other stakeholders. The Framework applies to all authorized property/casualty insurers that write cyber insurance. However, 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.

The Risks for Insurers

As cyber risk has increased, so too has risk in underwriting cyber insurance. The damage done by many types of cybercrime – such as business email compromises – continues to rise. But the biggest driver is an increase in the frequency and cost of ransomware attacks. A 2020 survey by DFS revealed that from early 2018 to late 2019, the number of insurance claims arising from ransomware increased by 180%, and the average cost of a ransomware claim rose by 150%. Moreover, the number of ransomware attacks reported to DFS almost doubled in 2020 from the previous year.[5] Costs continued to rise in 2020 as ransomware attacks increased in frequency and scale.[6] The global cost of ransomware was approximately $20 billion in 2020.[7] The cyber insurance industry has reported that escalating costs are creating pressure to increase rates and tighten underwriting standards for cyber insurance.

DFS recommends against making ransom payments. Ransom payments fuel the vicious cycle of ransomware, as cybercriminals use them to fund ever more frequent and sophisticated ransomware attacks. An October 2020 guidance by the Office of Foreign Assets Control ("OFAC") stressed the national security risk posed by ransom payments, and stated that intermediaries – including insurers – can be liable for ransom payments made to sanctioned entities.[8] Given the problem of identifying the attacker at the time of a ransomware incident, insurers and their policyholders risk violating OFAC sanctions when paying a ransom. Similarly, the FBI warns against paying a ransom because it fails to guarantee that an organization will regain access to all of its data or that its data won't be released publicly, and also because paying a ransom

emboldens criminals to target other organizations. In 2020, data extortion became a common feature of ransomware attacks, but experts have noted that in many cases even when victims paid, their data was subsequently leaked.[9]

Many insurers still have work to do to develop a rigorous and data driven approach to cyber risk, and experts have expressed concerns that insurers are not yet able to accurately measure cyber risk.[10] The decision to offer and price cyber insurance for specific organizations should be based on a careful assessment of that organization's risk. Cyber risk is driven in large part by the caliber of an organization's cybersecurity program, and so can vary considerably from one organization to the next. Insurers that don't effectively measure the risk of their insureds also risk insuring organizations that use cyber insurance as a substitute for improving cybersecurity, and pass the cost of cyber incidents on to the insurer. Without an effective ability to measure risk, cyber insurance can therefore have the perverse effect of increasing cyber risk – risk that will be borne by the insurer.

Managing this growing cyber risk is an urgent challenge for insurers. In addition to overall rising costs, insurers must account for the systemic risk that occurs when a widespread cyber incident damages many insureds at the same time, potentially swamping insurers with massive losses. This systemic risk is illustrated by the massive supply chain compromise in SolarWinds' Orion enterprise network management software.[11] Orion was widely used by critical infrastructure entities, private sector organizations, service providers, and government agencies. As a result of the compromise, thousands of organizations had malware backdoors installed in their networks. We have been assessing the impact of this compromise and appreciate the engagement of industry in this process.[12] Although this cyber campaign appears to have been focused on espionage and not destructive attacks, given the number of impacted organizations the total remediation costs are likely to be substantial.

Moreover, insurers often incur losses from cyber incidents in insurance policies that do not explicitly grant or exclude cyber coverage – so-called "non-affirmative" or "silent" risk. Because silent risk can reside in many different types of policies, even insurers that write little or no cyber insurance need to measure and manage silent risk in their

non-cyber insurance policies. While the industry has taken steps to address silent risk in recent years, it remains a significant problem for many insurers. According to a global survey in the second quarter of 2020, 65% of underwriters were concerned about cyber coverage exposure in property/casualty policies that do not explicitly cover cyber risks.[13]

These challenges – systemic risk and silent risk – are exemplified by the 2017 NotPetya incident, where malware unleashed by the Russian government caused damage across the globe. The incident led to $3 billion in insurance claims, of which $2.7 billion were made under property/casualty policies that were silent about cyber risks.[14]

The Framework is a result of our ongoing dialogue with the insurance industry and experts on cyber insurance. Over the past year, we have had dozens of meetings with insurers, insurance producers, cyber experts, and insurance regulators across the U.S. and Europe. In July 2020, we hosted a cyber insurance roundtable with representatives from five global insurance groups. Also in 2020, we collected survey data from 49 insurers on cyber insurance and ransomware. We continue to welcome input from industry and other interested parties on challenges facing the cyber insurance market.

Conclusion

Insurers play a critical role in mitigating and reducing the risks of cybercrime. We commend the progress many insurers have made in managing their cyber insurance risk to date and look forward to continuing to work with the industry to address challenges in the cyber insurance market.

Please direct any questions regarding this Circular Letter to CyberInsurance@dfs.ny.gov.

Sincerely,

Linda A. Lacewell

Superintendent

Cyber Insurance Risk Framework

All authorized property/casualty insurers that write cyber insurance should employ the practices identified below to sustainably and effectively manage their cyber insurance risk.[15] Based on our engagement with industry and experts, certain best practices have emerged.

Each insurer's cyber insurance risk will vary based many factors, including the insurer's size, resources, geographic distribution, market share, and industries insured. Each insurer should take an approach that is proportionate to its risk.

1. Establish a Formal Cyber Insurance Risk Strategy

   Insurers that offer cyber insurance should have a formal strategy for measuring cyber insurance risk that is directed and approved by senior management and the board of directors, or the governing body if there is no board.[16] The strategy should include clear qualitative and quantitative goals for risk, and progress against those goals should be reported to senior management and the board, or the governing body if there is no board, on a regular basis. The strategy should incorporate the six key practices identified below.

2. Manage and Eliminate Exposure to Silent Cyber Insurance Risk

   Insurers that offer cyber insurance should determine whether they are exposed to silent or non-affirmative cyber insurance risk, which is risk that an insurer must cover loss from a cyber incident[17] under a policy that does not explicitly mention cyber. Even property/casualty insurers that do not explicitly offer cyber insurance should evaluate their exposure to silent risk and take appropriate steps to reduce their exposure. Silent risk can be found in a variety of combined coverage policies and stand-alone non-cyber policies, including errors and omissions, burglary and theft, general liability and product liability insurance.[18] Cyber risk likely has not been quantified or priced into these policies, which exposes insurers to unexpected losses.

   Ultimately, insurers should eliminate silent risk by making clear in any policy that could be subject to a cyber claim whether that policy provides or excludes coverage for cyber-related losses. Elimination of this risk will take some time, given the many existing

policies that can contain silent cyber risk. Insurers should therefore also take steps to mitigate existing silent risk, such as by purchasing reinsurance.

3. Evaluate Systemic Risk

   As part of their cyber insurance risk strategy, insurers that offer cyber insurance should regularly evaluate systemic risk and plan for potential losses. Systemic risk has grown in part because institutions increasingly rely on third party vendors and those vendors are highly concentrated in key areas like cloud services and managed services providers. Insurers should understand the critical third parties used by their insureds and model the effect of a catastrophic cyber event on such critical third parties that may cause simultaneous losses to many of their insureds. Examples of such events could include a self-propagating malware, such as NotPetya, or a supply chain attack, [19] such as the SolarWinds trojan, that infects many institutions at the same time, or a cyber event that disables a major cloud services provider. A catastrophic cyber event could inflict tremendous losses on insurers that may jeopardize their financial solvency.[20]

   Insurers also should conduct internal cybersecurity stress tests based on unlikely but realistic catastrophic cyber events. Accurate stress testing requires accounting for both silent and affirmative risk. Moreover, because exposure to catastrophic cyber events varies across business industries and by type and size of the insured, insurers should track the impact of stress test scenarios across the different kinds of insurance policies they offer as well as across the different industries of their insureds. The cyber insurance risk strategy should account for possible losses identified in stress tests.

4. Rigorously Measure Insured Risk

   Insurers that offer cyber insurance should have a data-driven, comprehensive plan for assessing the cyber risk of each insured and potential insured. This commonly starts with gathering information regarding the institution's cybersecurity program through surveys and interviews on topics including corporate governance and controls, vulnerability management, access controls, encryption, endpoint monitoring, boundary defenses, incident response planning and third-party security policies. The information should be detailed enough for the insurer to make a rigorous assessment of potential

gaps and vulnerabilities in the insured's cybersecurity. Third-party sources, such as external cyber risk evaluations, are also a valuable source of information. This information should be compared with analysis of past claims data to identify the risk associated with specific gaps in cybersecurity controls.

5. Educate Insureds and Insurance Producers

   Insurers that offer cyber insurance have an important role to play in educating their insureds about cybersecurity and reducing the risk of cyber incidents. Insurers should strive to offer more comprehensive information about the value of cybersecurity measures and facilitate the adoption of those measures. Insurers should also incentivize the adoption of better cybersecurity measures by pricing policies based on the effectiveness of each insured's cybersecurity program.

   Several leading insurers already offer their insureds guidance, discounted access to cybersecurity services, and even cybersecurity assessments and recommendations for improvement.[21] We commend these initiatives, and insurers should continue to expand the type, scope and reach of such offerings.

   Insurers should also encourage and assist with the education of insurance producers who should have a better understanding of potential cyber exposures, types and scope of cyber coverage offered, and monetary limits in cyber insurance policies.[22] Ensuring that the need for, benefits of, and limitations to cyber insurance are well understood and conveyed to insureds and potential insureds will facilitate the growth of a robust cyber insurance market.

6. Obtain Cybersecurity Expertise

   Insurers that offer cyber insurance need appropriate expertise to properly understand and evaluate cyber risk. Insurers should recruit employees with cybersecurity experience and skills and commit to their training and development, supplemented as necessary with consultants or vendors.

7. Require Notice to Law Enforcement

   Cyber insurance policies should include a requirement that victims notify law enforcement. Some insurers that offer cyber insurance already engage in this best

practice.[23] Notice to law enforcement may be beneficial both to the victim-insured and the public.[24] Law enforcement often has valuable information that may not be available to private sources and can help victims of a cyber incident. Law enforcement can help recover data and funds that were lost. For instance, when funds are stolen through a business email compromise, law enforcement can sometimes block or reverse wire transfers if alerted of the incident promptly. Notice to law enforcement also can enhance a victim's reputation when its response to a cyber incident is evaluated by its shareholders, regulators, and the public. Finally, information received by law enforcement can be used to prosecute the attackers, warn others of existing cybersecurity threats, and deter future cybercrime.

[1] *See* NYDFS, Guidance to Department of Financial Services ("DFS") Regulated Entities Regarding Cybersecurity Awareness During COVID-19 Pandemic, April 13, 2020; U.S. Treasury Dep't Financial Crimes Enforcement Network (FinCEN) Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic, FIN-2020-A005, July 30, 2020.

[2] *See* NAIC, Report on the Cyber Insurance and Identity Theft Coverage Supplement (December 4, 2020). Note that this includes both standalone cyber insurance coverage as well as endorsements to non-cyber insurance policies.

[3] *See* Munich Re, Cyber Insurance: Risks and Trends (April 14, 2020).

[4] *See* Cyberspace Solarium Commission, March 2020 Report at 79.

[5] *See* 23 NYCRR 500.17.

[6] FinCEN Advisory on Ransomware and Use of the Financial System to Facilitate Ransom Payments, FIN-2020-A006, October 1, 2020 at 4 (citing FBI Internet Crime Complaint Center reports from 2018 and 2019 for the proposition that the "severity and sophistication of ransomware attacks continue to rise" and noting that the average dollar

amount in financial institution SARs on ransomware is $783,000 thus far in 2020, an increase of $280,000 from 2019).

[7] *See* Purple Sec, 2020 Ransomware Data, Statistics, and Trends (2020).

[8] *See* OFAC, Advisory on Potential Sanctions Risk for Facilitating Ransomware Payments at 1, October 1, 2020.

[9] *See* Coveware, Ransomware Demands continue to rise as Data Exfiltration becomes common, and Maze subdues, Nov. 4, 2020.

[10] *See* Cyberspace Solarium Commission, March 2020 Report at 80.

[11] *See* NYDFS Industry Letter -- Supply Chain Compromise Alert, December 18, 2020. *See also* Cybersecurity & Infrastructure Security Agency (CISA) Alert (AA20-352A) Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations; CISA Emergency Directive 21-01 Mitigate SolarWinds Orion Code Compromise.

[12] *See* NYDFS Industry Letter -- Supply Chain Compromise Alert, December 18, 2020.

[13] Partner Re, Cyber Insurance The Markets View Report at 2, September 17, 2020. *See also* Bank of England Prudential Regulation Authority, Letter to Chief Executives of Specialist General Insurance Firms Regulated by PRA, at 1, 2019 ("[f]irms almost all agreed that a number of traditional lines of business have considerable exposure to non-affirmative cyber risk").

[14] *See* Jon Bateman, War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions, Carnegie Endowment for International Peace, at 8-9 (October 2020).

[15] All DFS-regulated insurers also must address their own cybersecurity and comply with the cybersecurity regulations set forth in 23 NYCRR 500.

[16] *See* Bank of England Prudential Regulation Authority, Cyber Insurance Underwriting Risk, 2017 at 6-7 (recommending that cyber risk strategy be reviewed by the Board).

[17] A “cyber incident” occurs when an unauthorized user gains access to, disrupts or misuses an organization’s information system or gains access to or misuses information stored on that system which is of value to the organization, including, but not limited to, patient records, nonpublic information, intellectual property, and customer information. An “information system” is a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

[18] *See* Bank of England Prudential Regulation Authority, Letter to Chief Executives of Specialist General Insurance Firms Regulated by PRA, at 1-2, 2019.

[19] *See* Cyberspace Solarium Commission, March 2020 Report at 8 (describing the global chaos caused by the NotPetya attack in 2017 when Russian cyber operators launched a malware attack targeted at Ukrainian institutions that quickly spread to, and disabled, critical systems worldwide).

[20] *See* NAIC, Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement, September 12, 2019 (“[a] systemic event continues to be the top threat to cyber insurers’ solvency”), citing AM Best Market Segment Report, June 17, 2019.

[21] *See, e.g.*, American International Group (AIG), CyberMatics (providing insureds tools to manage their cybersecurity risk).

[22] *See* Cyberspace Solarium Commission, March 2020 Report at 80 (recommending training and certification for those in the insurance industry, emphasizing that in order for “underwriters to effectively evaluate and analyze risk in a given industry, they must understand it”).

[23] Based on DFS’s survey, 36% of insurers required their cyber insurance insureds to notify law enforcement of a cyber incident.

[24] For ransomwares incidents, OFAC will consider contacting law enforcement as a mitigating factor in case sanctions laws are violated. OFAC, Advisory on Potential Sanctions Risk for Facilitating Ransomware Payments, October 1, 2020 at 4.