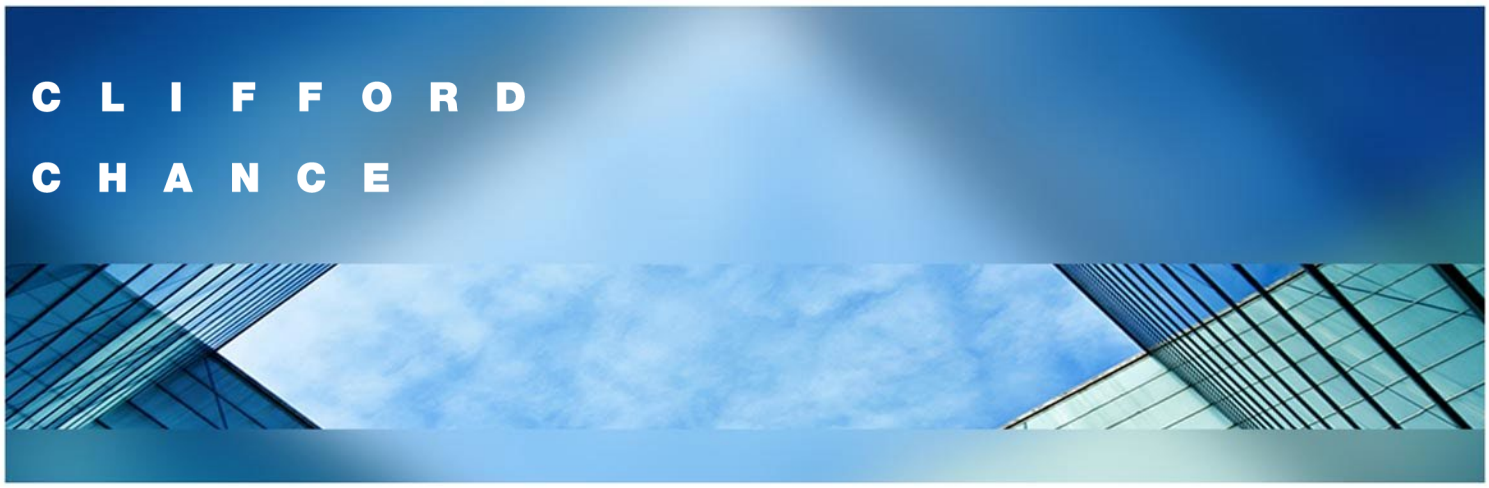

NEW YORK DEPARTMENT OF FINANCIAL SERVICES ISSUES CYBER INSURANCE RISK FRAMEWORK

On February 4, 2021, the New York Department of Financial Services ("DFS") issued its Cyber Insurance Risk Framework ("Framework") to help insurers effectively price and manage cyber insurance risk. In a Circular Letter introducing the Framework, DFS cautioned insurers that failure to accurately price cyber risk can lead to compounded losses that threaten their stability and viability. DFS also expressed concern that insurers may create improper incentives for their clients, who may see paying for cybersecurity insurance as a substitute for an effective cybersecurity infrastructure. The Framework reflects the DFS's continued focus on cybersecurity.[1]

Key issues

- NYDFS has issued guidance to help insurers manage cyber insurance risk.
- Insurers who price cyber risk inaccurately can face significant losses.
- Improper cyber risk pricing can also increase insureds' cyber risk by disincentivizing necessary investments in cybersecurity protection.
- Insurers who do not offer cyber insurance must still manage "silent" cyber risk.

RISING COSTS OF RANSOMWARE

DFS identified the rise in frequency and costs of ransomware attacks as the biggest driver in the continued increase in cyber risk and cyber-related liability in recent years. According to a DFS survey, from 2018 to 2019 the number of ransomware attacks increased by 180% and the average cost of a ransomware claim rose by 150%. In 2020, the number of ransomware attacks reported to DFS almost doubled as the global cost of ransomware reached USD 20 billion. As a result, the cyber insurance industry faces significant pressure to manage rising costs by raising rates and tightening standards for underwriting cyber insurance.

While discussing the rise in ransomware attacks, DFS explicitly recommended against making ransom payments, cautioning that insurers may be liable for sanctions from the Office of Foreign Assets Control ("OFAC") if they make ransom payments, which often go to sanctioned entities. As discussed in recent OFAC guidance,[2] OFAC sanctions are strict liability offenses, meaning that intent and knowledge are irrelevant to liability–and not even considered mitigating factors. As DFS points out, the risk of sanctions is especially not worth taking since companies

1 https://talkingtech.cliffordchance.com/en/data-cyber/cyber/dfs-proposes-cybersecurity-regulations-.html.
2 https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

that pay ransom still may not recover their data and could face subsequent data leaks.

THE SOLARWINDS HACK

DFS mentioned the recent SolarWinds hack several times throughout the letter, suggesting that the department is concerned about the type of systemic risk such an incident can cause for insurers. SolarWinds is a U.S. information technology firm that sells "Orion," an enterprise network management software used by thousands of public and private sector customers. In Winter 2020, SolarWinds revealed that hackers had embedded code into a routine software update for Orion that allowed them to access customer information technology systems, install more malware, and subsequently monitor the breached organizations. The hack affected thousands of Orion users and SolarWinds (and insurers) are still assessing the consequences of the hack.

As DFS points out, this type of cyber-attack, which affects a widely used part of the software supply chain, can lead to many claims by insureds at the same time, resulting in potentially massive losses that could threaten an insurer's financial solvency.

CYBER INSURANCE RISK FRAMEWORK

To guard against significant losses arising from improperly priced risk, DFS instructs insurers to develop a "rigorous and data driven approach" to cyber risk pricing, driven by a case-by-case assessment of a customer's level of risk. In particular, DFS cautions that insurers should avoid the risk that clients will view cyber insurance as an adequate replacement for an effective cybersecurity infrastructure. This would create a vicious cycle that would open both parties up to steadily escalating levels of cyber risk.

The Framework comprises seven best practices for insurers to properly evaluate their cyber insurance risk. In creating this framework, DFS spoke with insurers, cyber insurance experts, and insurance regulators from the U.S. and Europe. They also conducted a roundtable with representatives from the insurance industry and collected survey data from 49 insurers.

The best practices:

1. **Establish a Formal Cyber Insurance Risk Strategy**. This strategy should be directed and approved by senior leadership and informed by the other six best practices.
2. **Manage and Eliminate Exposure to Silent Cyber Insurance Risk**. Insurers–even those that do not offer cyber insurance—are subject to "silent risk," which is insurance that does not explicitly grant or exclude cyber coverage. The Framework recommends that all insurers aim to eliminate silent risk by explicitly stating whether that policy covers cyber-related losses. For existing policies, insurers can also mitigate their risk by purchasing reinsurance.
3. **Evaluate Systemic Risk**. Systemic risk has become an issue because institutions increasingly rely on third party vendors, particularly cloud services and managed services providers. As a result, an attack on a

third-party vendor may trigger further attacks on parties that use that vendor (like the SolarWinds hack). Insurers should run cybersecurity stress tests on their clients to get a more accurate reading of systemic risk. The results of the stress tests should inform insurer cyber insurance risk strategies moving forward.

4. **Rigorously Measure Insured Risk**. Insurers should learn about the client's cybersecurity program through surveys and interviews on topics including corporate governance and controls, vulnerability management, access controls, encryption, endpoint monitoring, boundary defences, incident response planning and third-party security policies, as well as third-party sources. The information gathered should be analysed with past claims data to identify the risk associated with specific gaps in cybersecurity controls and allow the insurer to make a comprehensive risk assessment of potential gaps and vulnerabilities in the client's cyber program.
5. **Educate Insureds and Insurance Producers**. Insurers may help their clients and other insurance producers understand and appreciate the risks posed by cyberthreats and the types of cyber coverage available by advising on the importance of effective cybersecurity, aiding in their implementation, and incentivizing better cybersecurity programs. By educating other insurers as well insureds, insurers contribute to the growth of a robust cyber insurance market.
6. **Obtain Cybersecurity Expertise**. In line with completing a comprehensive risk analysis before offering cyber insurance, DFS recommends that insurers hire employees with cybersecurity experience and skills, supplemented as necessary with consultants or vendors. Insurers should ensure these individuals receive continued training and development.
7. **Require Notice to Law Enforcement**. Insurers should include a clause in their cyber insurance policies that requires victims to inform law enforcement. Law enforcement may have information and resources to help recover data and funds that were lost due to a cyber-attack. Law enforcement can also prosecute cybercriminals, issue warnings to other vulnerable entities, and deter future attacks, benefiting the market as a whole.

In describing the Framework, DFS noted that the risk analysis should be informed by several factors, including the insurer's size, resources, geographic distribution, market share, and industries insured.

CONCLUSION

With pandemic-related shifts to an online work environment and recent high-profile cybersecurity incidents like the SolarWinds hack making headlines, the demand for cyber insurance is higher than it has ever been, with estimates that by 2025 the market will reach USD 20 billion. Insurers must ensure that they assess this risk to protect themselves from incurring unnecessary losses and avoid disincentivizing their customers from also investing in key cybersecurity infrastructure. The Framework will hopefully help insurers continue to play the key role they do in helping companies manage their cyber risk.

CONTACTS

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon@cliffordchance.com

Celeste Koeleveld
Partner

T +1 212 878 3051
E celeste.koeleveld@cliffordchance.com

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver@cliffordchance.com

Benjamin Berringer
Associate

T +1 212 878 3372
E benjamin.berringer@cliffordchance.com

Brian Yin
Associate

T +1 212 878 4980
E brian.yin@cliffordchance.com

Christine Chen
Associate

T +1 202 912 5081
E christine.chen@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA