akerman

Practice Update

# The New NYDFS Cyber Insurance Risk Framework – Required Reading for Insurers and Insureds

February 24, 2021

By Elizabeth F. Hodge and Christy S. Hawkins

The New York Department of Financial Services ("NYDFS") recently released its Cyber Insurance Risk Framework (the "Framework"), which provides best practices for managing cyber insurance risk. The stated goal of the Framework is to grow "a robust cyber insurance market that maintains the financial stability of insurers and protects insureds." While the Framework is directed to cyber risk insurers, organizations looking to purchase cyber insurance should also review the Framework to understand how the market is developing and what to be aware of when they next shop for cyber coverage.

In its guidance, NYDFS notes that there are several developments presenting urgent challenges to cyber risk insurers:

- Cyber insurance is a relatively new area of insurance, but is projected to grow from $3.15 billion in 2019 to over $20 billion by 2025.
- There has been a marked increase in cybercrime, especially ransomware attacks. According to NYDFS statistics, the number of insurance claims from ransomware increased by 180% from early 2018 to late 2019, with the average cost of such a claim increasing 150%. That trend continues as

## Related People

Christy S. Hawkins
Elizabeth F. Hodge

## Related Work

Data Privacy and Security
Healthcare
Litigation

the number of ransomware attacks reported to NYDFS in 2020 almost doubled from 2019.

- Many insurers offering cyber insurance are struggling to accurately identify and price the risk, potentially jeopardizing their financial stability and the stability of the cyber risk market generally.
- The unique systemic risk posed by widespread cyber incidents where many insureds can be affected and suffer losses due to the same event.
- The increasing exposure from "silent risk" for cyber events under policies that were not specifically drafted to cover or exclude cyber incidents and were not priced to cover such events, e.g., general liability policies, errors and omissions coverage.

To help insurers better understand and manage their cyber risk, NYDFS recommends that all insurers writing cyber insurance use the following seven practices in the Framework, which were developed with industry input, to "sustainably and effectively" manage their cyber insurance risk:

**1. Establish a formal cyber insurance risk strategy.** Cyber insurers should have a formal strategy for measuring cyber insurance risk that includes clear qualitative and quantitative goals for risk and reporting the progress in meeting those goals to the board or other oversight group. The strategy should be approved by the insurer's board or other governing body. The risk strategy should incorporate the six key practices below.

**2. Manage and eliminate exposure to silent cyber insurance risk.** "Silent" or "non-affirmative" risk is the risk that an insurer must cover a loss from a cyber incident under a policy, such as a traditional property or liability policy, that doesn't specifically mention cyber. Insurers that offer cyber insurance, and those who do not, should assess whether they have exposure for silent cyber risk. Then, insurers should begin the process of revising policies that

could be subject to a cyber claim to clarify whether the policy covers or excludes cyber-related losses. Because it can take time to update all policies that may unintentionally cover cyber events, insurers are urged to mitigate existing silent risk, including by purchasing reinsurance.

Organizations looking to purchase cyber insurance should be aware that they may no longer be able to rely on other policies they may have, such as errors and omissions, burglary and theft, and general liability, to cover cyber incidents and will have to depend on cyber insurance only for losses from such incidents.

**3. Evaluate systemic risk.** As noted above, systemic risk has increased in part because many organizations increasingly rely on third party vendors such as cloud service providers and managed services providers. Thus, a critical cyber event that originates at a vendor can quickly spread to customers using the vendor's services, potentially resulting in significant losses for the insurers of those customers. Recent examples of such events include the NotPetya malware attacks and the SolarWinds incident. Therefore, just as property and casualty insurers model and prepare for catastrophic events affecting a large number of property and casualty insureds (e.g., hurricanes), cyber insurers need to regularly evaluate systemic risk and plan for potential catastrophic losses arising from a critical cyber event.

**4. Rigorously measure insured risk.** NYDFS states that the quality of an organization's cybersecurity program is a significant determinant of cyber risk resulting in widely varying risk profiles among insureds. As a result, insurers should adopt a data-driven, comprehensive plan for evaluating the risk of each potential insured. The information gathered from insureds should be detailed enough so the insurer can make "a rigorous assessment" of potential gaps and vulnerabilities in the insured's cybersecurity program. In practice, this assessment

may need to go beyond the current evaluation criteria to examine the details of protections in place, as well as the culture of an insured to protect privacy in the organization.

Purchasers of cyber insurance have likely already experienced increasingly robust cyber security assessments from their insurers and should expect that trend to continue as insurers try to better understand the risk posed by each insured and price coverage accordingly. Purchasers should also be aware that false or incomplete information provided during the assessment process may be considered a material misrepresentation that could result in claim denials. Accordingly, it may be prudent to evaluate what information an insurer is requesting for its assessment well in advance of renewal deadlines so that the purchaser can mitigate deficiencies that may result in increased premiums or refusal to offer coverage.

**5. Educate insureds and insurance producers.** Cyber insurers are encouraged to offer more comprehensive information to their insureds about the value of good cybersecurity measures and facilitate implementation of those measures. Insurers can incentivize adoption of cybersecurity measures by pricing policies to reward those insureds who have implemented effective cyber measures. NYDFS encourages insurers to expand on existing efforts to offer insureds guidance, cybersecurity assessments and recommendations for improving an organization's cyber posture.

Would-be insureds should understand that cyber insurers will expect their policyholders to be partners in protecting the organization from cyber risk and reward those insureds who invest in robust cybersecurity measures by offering coverage at a lower premium.

**6. Obtain cybersecurity expertise.** Cyber insurers are encouraged to hire employees with cybersecurity experience and provide continuing

training so they can develop a knowledgeable workforce that can properly evaluate cyber risk. When necessary, insurers should supplement their employee workforce with vendors and consultants.

Relatedly, would-be insureds will benefit from documentation of the cybersecurity experience and training in the organization to demonstrate to insurers that they have similarly prioritized cybersecurity expertise and training.

**7. Require notice to law enforcement.** NYDFS recommends that cyber policies require insureds to report cyber incidents to law enforcement as law enforcement can have information that can help victims of a cyber incident, including recovering data and/or lost funds. Reporting incidents to authorities may also better position the organization with shareholders, regulators, and the public. It should be noted that NYDFS recommends against paying ransoms as this provides cyber criminals with resources to commit additional crimes and there is no guarantee that the criminals will return data and/or provide decryptions keys. This position is common among governmental and law enforcement agencies, and to that end, OFAC issued an advisory on October 1, 2020 regarding the sanctions risks of facilitating ransomware payments.

## Takeaways

Many cyber risk insurers have likely started to implement the NYDFS Framework, but the expected growth in cybercrime, including ransomware attacks, may require insurers to speed up their efforts to ensure that they are appropriately assessing and pricing cyber risk so they can remain in the market for years to come. At the same time, potential cyber insurance purchasers that understand how the insurance market will develop and invest the necessary resources to improve their cybersecurity programs should, over time, reap the benefit of being able to obtain coverage at lower premiums. Those organizations that don’t build up

their data security program could find themselves paying more to protect against cyber incidents, or not being able to obtain coverage at all.

---

This information is intended to inform firm clients and friends about legal developments, including recent decisions of various courts and administrative bodies. Nothing in this Practice Update should be construed as legal advice or a legal opinion, and readers should not act upon the information contained in this Practice Update without seeking the advice of legal counsel. Prior results do not guarantee a similar outcome.