NYS Department of Financial Services Issues "Cyber Insurance Risk Framework"

On February 4, New York State's Department of Financial Services (DFS) issued a seven-part "Cyber Insurance Risk Framework" urging insurance companies, following the recent surge in ransomware, to develop a "rigorous" and "data driven approach" to insuring cybersecurity risks. Ransomware attacks reported to the DFS almost doubled in 2020 from the previous year, the regulator added, with costs continuing to rise as ransomware attacks increased in frequency and scale. In addition, the number of insurance claims arising from ransomware attacks nearly tripled between early 2018 and late 2019, according to a DFS survey. Managing a growing cyber risk continues to be a challenge for insurers, and according to the DFS, one that requires coverage offerings and pricing based on a careful assessment of an organization's risk level, which is largely driven by the caliber of the organization's cybersecurity program.

Importantly, DFS recommends against paying ransom. DFS recognizes that there are risks associated with making payment to threat actors as these attacks are becoming more sophisticated and variants more difficult to determine. Therefore, insurers may risk violating Office of Foreign Assets Control ("OFAC") sanctions. DFS further warns that experts have noted that even when payment has been made, the data was subsequently leaked.

DFS focuses on the correlation of risks between insurers and insureds as instances of cybercrime rise and become more damaging. From there, DFS urges insurance companies to develop formal strategies, directed and approved by senior management and the board of directors, for measuring cyber insurance risk. Ultimately, the Framework reinforces the criticality of insurers as it relates to mitigating—and ultimately reducing—the risks and impact of cyber incidents.

Although DFS admits that the practices employed by cyber insurers may fluctuate necessarily due to variations in size, market share, geographical location, and industries insured, DFS maintains that the following best practices ought to be implemented by all insurers,:

1. Establish a Formal Cyber Insurance Risk Strategy
2. Manage and eliminate exposure to silent cyber insurance risk
3. Evaluate systemic risk
4. Rigorously measure insured risk
5. Educate insureds and insurance producers

Carolyn Purwin Ryan
Mullen Coughlin

Carolyn Purwin Ryan is a Partner at Mullen Coughlin and serves as a Data Breach Coach for organizations who have been the victim of a real, or attempted, cybersecurity attack. Her practice includes leading investigations into cyber attacks, providing guidance on governmental or other third-party investigations and assisting in data restoration and mitigating future attacks. Carolyn also counsels clients on the development of risk assessment policies, vendor agreement analysis and implementation of data privacy practices. She can be reached at cpurwinryan@mullen.law

Maria Monastra
Mullen Coughlin

Maria Monastra is an Associate with Mullen Coughlin, focusing on providing counsel to clients who experienced a data privacy compromise or cybersecurity breach and are faced with responding to the incident. When an incident occurs, Ms. Monastra assists clients in determining the nature and scope of the incident

Cont'd...

6. Obtain cybersecurity expertise
7. Require notification to law enforcement

We should anticipate continued growth and changes to the industry at large as well as our everyday practice. Insurers are poised to begin adapting to the complex underwriting requirements unique to cyber, and as they do, our duty to counsel clients about the cruciality of system awareness and security will become even more important.

In all cases, clients should be advised to be aware of their systems and where sensitive information may be stored within them. Clients ought to similarly be encouraged to know their corporate governance and controls, limit access to sensitive information (when possible) and implement encryption, endpoint monitoring, boundary defenses, incident response planning, and third-party security policies. As acknowledged by DFS, clients should be attentive to the systemic risk presented by reliance on vendors and other third parties who manage data on behalf of numerous companies within a particular industry or supply chain, such as cloud and managed service providers. By extension, clients should understand the immediate and extended benefits of conducting risk assessments and "stress testing" internally on a regular basis.

In a similar vein, clients should review their cyber insurance policies to ensure an understanding of what they include and, perhaps more importantly, what they do not. As part of their review, clients should evaluate other coverages, including those contemplated by their errors and omissions, burglary and theft, general liability, and product liability insurance policies.

Further still, clients should be encouraged to educate employees and, in the event of an incident, to work with cybersecurity experts in the industry.

Finally, clients should be advised of the benefits of law enforcement reporting, as those benefits are in some cases far-reaching for both victim organizations and the public. Such reporting may also directly impact the ways in which insurance claims are considered.

As DFS aims to primarily educate insurers and promote formal strategies for risk management in the cyber industry, it is our obligation to provide parallel guidance to our clients and assistance to the carriers by whom they are often referred.

Monastra Bio...

and identifying potentially impacted populations, advising each client as to the applicability of state, federal and foreign privacy laws. In every event, Maria works diligently with the client to ensure proper compliance with data breach notification requirements, proper disclosure to impacted populations and preservation of institutional goodwill. She can be reached at mmonastra@mullen.law

Importantly, DFS recommends against paying ransom.