July 2, 2021

New York State Department of Financial Services Issues New Guidance on Preventing Ransomware Attacks

Agency Recommends Preventative Measures Amid Growing Regulatory Focus on the Ransomware Threat

SUMMARY

On June 30, 2021, the New York State Department of Financial Services ("DFS") released new guidance (the "Guidance") for regulated entities to "significantly reduce the risk of a ransomware attack."[1] In the Guidance, DFS describes lessons learned from its investigation of each of the 74 ransomware attacks reported to DFS by regulated entities between January 2020 and March 2021. DFS recommends that all DFS-regulated entities implement, whenever possible, nine specific measures to prevent ransomware attacks. DFS stresses the urgency with which companies need to improve their cybersecurity defenses, describing ransomware as a "crisis" which "threatens every financial services company and their customers," and which could cause the next great financial crisis.[2]

BACKGROUND

Ransomware is a form of malicious software, or "malware," that generally encrypts, and blocks access to, a victim's computer systems or data, rendering it effectively useless. After encrypting the systems or data, the attacker demands a ransom payment in exchange for the decryption key. In a scenario that's become increasingly common, the attacker may also steal the victim's data prior to deploying the ransomware and then threaten to sell or publish the data if the ransom is not paid—so-called "double extortion." In May 2021, Secretary of Homeland Security Alejandro Mayorkas warned that the number of ransomware attacks increased by over 300% in 2020, with victims paying over $350 million in ransom last year.[3] This follows a 37% increase in ransomware attacks between 2018 and 2019.[4]

According to DFS, this rapid increase in ransomware attacks has been "fueled by the ever-growing payments made by ransomware victims."[5] As hackers collect ever-higher ransom payments, these payments fund "more frequent and more sophisticated ransomware attacks."[6] Average ransom payments increased 171% from 2019 to 2020.[7]

This increase in the frequency of attacks and the size of ransom demands also has implications for insurance coverage and insurance providers, as the increased costs stemming from attacks affect premiums and the scope of coverage. DFS observes that these rising costs are "pressuring insurers to be more rigorous in assessing the cybersecurity of their customers and pricing insurance according to that risk."[8]

DFS FINDINGS AND RECOMMENDATIONS

In the Guidance, DFS emphasizes in stark terms the ransomware "crisis" facing "every financial services company and their customers."[9] According to DFS, the next great financial crisis could stem from a major ransomware attack that cripples financial services companies and leads to a loss of confidence in the financial system as a whole.[10] DFS notes that a ransomware attack of that scale may take place through the exploitation of a vulnerability or compromise in software used by many companies, as recently occurred in separate incidents involving SolarWinds software and Microsoft Exchange, or through a single ransomware attack that disables critical infrastructure, such as a cloud services provider or a regional power grid, similar to the recent attack on Colonial Pipeline.

According to DFS, 74 DFS-regulated companies reported suffering ransomware attacks between January 2020 and March 2021.[11] Certain of these attacks resulted in days-long shutdowns, and 17 of the companies paid a ransom in response to an attack.[12] DFS notes that both DFS and the Federal Bureau of Investigation advise against paying ransoms to cybercriminals, and that paying a ransom does not ensure the safety of data. DFS cites industry reporting that "80% of victim organizations who paid a ransom experienced subsequent attacks," sometimes reportedly by the same actor and sometimes reportedly by different actors.[13]

The Guidance clarifies certain reporting requirements pursuant to § 500.17(a) of DFS's Cybersecurity Requirements for Financial Services Companies (the "Cybersecurity Regulation").[14] Specifically, the Guidance provides that "any successful deployment of ransomware on [a regulated company's] internal network" should be reported to DFS "as promptly as possible and within 72 hours at the latest."[15] The Guidance further states that "any intrusion where hackers gain access to privileged accounts" should be reported under § 500.17(a), and that DFS "is considering clarifying its reporting requirements by expressly requiring these types of incidents to be reported."[16]

The Guidance also provides that DFS intends to impose additional requirements on regulated entities under its Cybersecurity Regulation. Specifically, DFS is currently "evaluating what additional controls should be added to its Cybersecurity Regulation," and "welcomes engagement with industry and experts on [these] revisions."[17]

A. THE "SIMILAR PATTERN" OF ACTIVITY LEADING TO A RANSOMWARE ATTACK

As set forth in the Guidance, based on information collected by DFS on each of the 74 ransomware attacks reported to DFS between January 2020 and March 2021, and extensive consultation between DFS and experts, DFS found that each of the 74 ransomware attacks followed a similar pattern.[18]

- *First*, hackers gain entry to a victim's network using one of three techniques: (1) phishing; (2) exploiting unpatched vulnerabilities; or (3) exploiting poorly secured Remote Desktop Protocols ("RDPs").[19]

- *Second*, having accessed a victim's network, hackers "escalate privileges by obtaining access to administrator (or privileged user and privileged service) accounts."[20] The hackers accomplish this privilege escalation by "stealing encrypted ('hashed') passwords and then employing password cracking tools on their own computers to decipher stolen passwords."[21]

- *Finally*, the hackers will use their privileged access to "deploy ransomware, circumvent security controls, and target backups."[22]

B. DFS'S RECOMMENDATIONS

DFS sets forth nine proposed measures for preventing ransomware, described below. Certain of the proposed measures reflect current requirements under the Cybersecurity Regulation, and others expand on existing guidance and regulations. Some of these proposed measures, including implementing vulnerability management programs and incident response plans, were also mentioned in DFS's report on the SolarWinds attack.[23] DFS recommends that the following measures be "implemented by companies wherever possible."[24]

1. ***Email Filtering and Anti-Phishing Training***. DFS recommends that training includes "recurrent phishing training, including how to spot, avoid, and report phishing attempts."[25] DFS recommends filtering e-mail to block spam and malicious links and attachments, and periodically testing employees' phishing avoidance.

2. ***Vulnerability/Patch Management***. "Companies should have a documented program to identify, assess, track, and remediate vulnerabilities on all enterprise assets within their infrastructure."[26] It should include "periodic penetration testing" and timely patch application and updates.[27] The

Cybersecurity Regulation requires annual penetration testing and biannual vulnerability assessments.[28]

3. ***Multi-Factor Authentication ("MFA")***. According to DFS, MFA can prevent hackers from gaining network access and escalating privileges once inside. The Cybersecurity Regulation requires MFA for remote network access and "all externally exposed enterprise and third-party applications."[29]

4. ***Disable RDP Access***. DFS recommends that regulated entities disable RDP access from the internet wherever possible. If deemed necessary, RDP access should be limited to approved, or "whitelisted," originating sources and require MFA and strong passwords.[30]

5. ***Password Management***. Companies should ensure that "strong, unique" passwords are used.[31] DFS recommends passwords of at least 16 characters, turning off password caching—where a browser or device "remembers" login credentials, and password access management solutions for larger organizations. Such a password management solution may require employees to request and check out passwords with expiry dates to gain network access.

6. ***Privileged Access Management***. Section 500.7 of the Cybersecurity Regulation requires that regulated entities limit access privileges to nonpublic information and periodically review such access privileges. In the Guidance, DFS recommends that regulated entities implement the principle of least privileged access, which provides that each user or service account should be given the minimum level of access necessary to perform the required job.[32] Administrators should thus have a second, non-privileged account for tasks that do not require those elevated privileges, *e.g.*, logging into a work station or drafting an e-mail. Companies should maintain and periodically audit an inventory of all privileged accounts.

7. ***Monitoring and Response***. DFS recommends that regulated entities implement an Endpoint Detection and Response ("EDR") solution, which monitors for anomalous activity. According to DFS, an advanced EDR can quarantine infected systems, thus potentially stopping ransomware from executing before it can encrypt the endpoint.[33] DFS further recommends that companies with larger and/or more complex networks adopt "lateral movement detection" and a Security Information and Event Management ("SIEM") solution which "centralizes logging and security event alerting."[34]

8. ***Tested and Segregated Backups***. To prepare for a ransomware attack or other cybersecurity incident, DFS states that regulated companies should maintain segregated backups which may be recovered in the event of an attack.[35] Such backups should be segregated from a company's network and stored offline to prevent cybercriminals from deleting or encrypting the backups. DFS further recommends regularly testing backups to ensure they are usable.

9. ***Incident Response Plan***. Finally, while the Cybersecurity Regulation already requires that a regulated entity "establish a written incident response plan" for addressing a cybersecurity incident,[36] the Guidance recommends that an incident response plan explicitly cover ransomware attacks and be regularly tested—including by senior leadership.

IMPLICATIONS

DFS's Guidance is consistent with a heightened focus on ransomware attacks across the U.S. government as these attacks have increased in frequency, and particularly in the wake of the recent attack on Colonial Pipeline, which disrupted fuel supplies along the East Coast. In May, President Biden issued an Executive Order on Improving the Nation's Cybersecurity, which requires sweeping cybersecurity enhancements across the federal government, including measures specifically designed to bolster ransomware defenses.[37] The Executive Order specifically calls on the private sector to "adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace."[38]

DFS's new Guidance makes clear that DFS may soon revise the Cybersecurity Regulation consistent with the recommendations it sets forth in the Guidance. Regardless of whether the Cybersecurity Regulation is revised, however, and taken together with analogous recommendations in the Executive Order, the Guidance will establish baseline expectations for ransomware preparedness. In the event that a DFS-regulated entity suffers a ransomware attack, DFS can be expected to use the Guidance as a touchstone in analyzing whether the company was adequately prepared.

DFS-regulated entities should assess and update, as needed, their cybersecurity defenses in light of DFS's recommended ransomware prevention measures. Some measures may be easier to deploy than others, and some may require the assistance of outside experts to effectively implement.

* * *

ENDNOTES

1 New York State Department of Financial Services, Ransomware Guidance ("Guidance") (June 30, 2021), *available at* https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202106302.

2 *See id.*

3 James Rundle & David Uberti, *How Can Companies Cope With Ransomware*, WALL STREET JOURNAL (May 9, 2021, 10:35 AM EDT), *available at* https://www.wsj.com/articles/how-can-companies-cope-with-ransomware-11620570907.

4 *See* U.S. Department of Treasury, Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (Oct. 1, 2020), *available at* https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

5 *See* Guidance.

6 *See id.*

7 *See id.*; Highlights from the 2021 Unit 42 Ransomware Threat Report, Unit 42, Palo Alto Networks (Mar. 17, 2021), *available at* https://unit42.paloaltonetworks.com/ransomware-threat-report-highlights/.

8 *See* Guidance.

9 *Id.*

10 *Id.*

11 *Id.*

12 *Id.*

13 *See id.*; *see also Ransomware: The True Cost to Business*, CYBEREASON at 4 (June 16, 2021), *available at* https://www.cybereason.com/ebook-ransomware-the-true-cost-to-business.

14 *See* Guidance; 23 NYCRR § 500.17(a).

15 *Id.*

16 *Id.*

17 *Id.*

18 *Id.*

19 *Id.* An RDP allows a user to remotely access or control a desktop computer on an organization's network.

20 *Id.*

21 *Id.*

22 *Id.*

23 *New York State Department of Financial Services Releases Report on SolarWinds Cyber Espionage Attack* (Apr. 29, 2021), *available at* https://www.sullcrom.com/sc-publication-ny-dfs-releases-report-solarwinds-cyber-attack.

24 *See* Guidance.

25 Cybersecurity awareness training is required under 32 NYCRR § 500.14(b). *See also* Guidance.

26 *Id.* (citing 23 NYCRR § 500.3(g)).

ENDNOTES (CONTINUED)

27 *Id.* (citing 23 NYCRR § 500.5(b)).

28 23 NYCRR §§ 500.5(a) & (b).

29 Guidance (citing 23 NYCRR §§ 500.12, 500.3(d) & (g)).

30 *Id.* (citing 23 NYCRR § 500.3(g)).

31 *Id.* (citing 23 NYCRR § 500.3(d)).

32 *Id.* (citing 23 NYCRR §§ 500.3(d), 500.7).

33 *Id.*; *see also id.* (DFS-regulated entities must maintain system-monitoring processes to identify intruders and respond to alerts of suspicious activity) (citing 23 NYCRR § 500.3(h)).

34 *Id.*

35 *Id.* (citing 23 NYCRR §§ 500.3(e), (f) & (n)).

36 23 NYCRR § 500.16(a).

37 Exec. Order No. 14,028; *see also President Issues Executive Order on Improving the Nation's Cybersecurity* (May 14, 2021), *available at* https://www.sullcrom.com/sc-publication-president-issues-executive-order-improving-nations-cybersecurity.

38 Exec. Order No. 14,028 at § 1.

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 other 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.