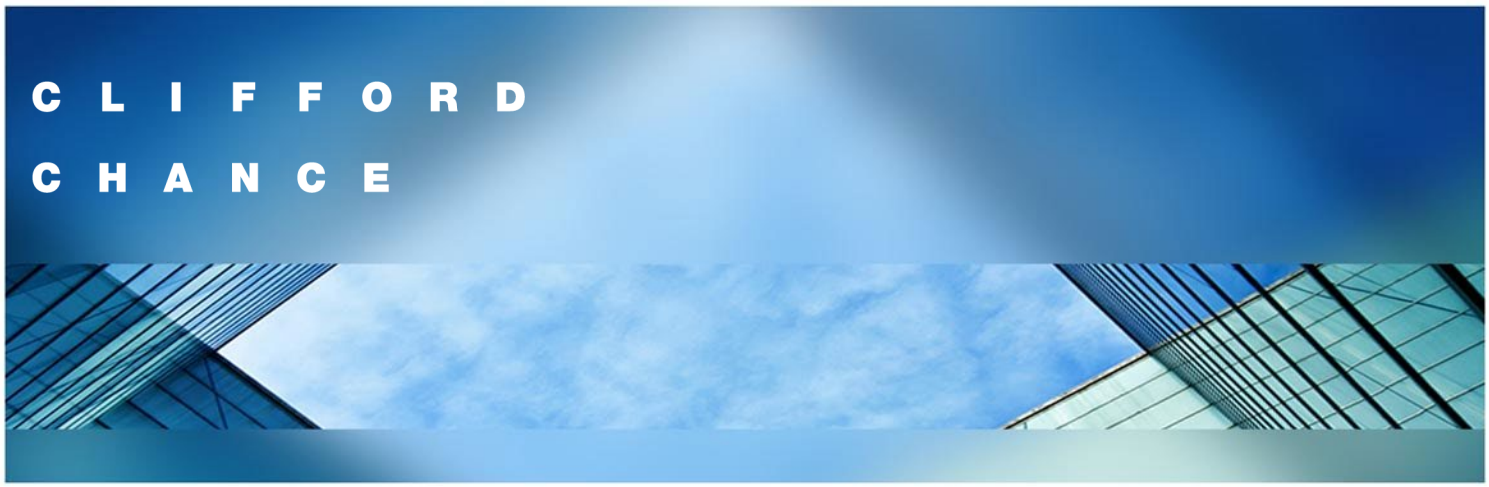

NEW YORK DEPARTMENT OF FINANCIAL SERVICES ISSUES RANSOMWARE GUIDANCE IN WAKE OF INCREASED ATTACKS

Key issues

- The New York Department of Financial Services has issued guidance to regulated entities to prevent ransomware attacks.
- The guidance contains nine controls that the Department "expects" regulated entities to implement.
- Companies should review their cybersecurity program to ensure they are protected against attacks.

On June 30, 2021, the New York Department of Financial Services ("DFS") issued Ransomware Guidance to help companies prevent and respond to attacks. While the alert is styled as "guidance," it is hard to imagine many situations, even applying a risk-based analysis, where DFS would not "expect" supervised entities to implement the controls listed, which repeatedly cross-reference the Department's Cybersecurity Regulation. As ransomware attacks continue to increase in frequency and sophistication, supervised entities should review their cybersecurity controls against DFS's guidance to ensure that they have adequate protections in place.

NYDFS CYBERSECURITY REGULATION

The NYDFS Cybersecurity Regulation went into effect on March 1, 2019 and, among other requirements, instructs covered entities to report cybersecurity events to the Superintendent within 72 hours. The regulation defines a "cybersecurity event" broadly to include any attempt (whether successful or not) to gain access to or disrupt a covered entity's information systems.

The Ransomware Guidance is intended to supplement these reporting requirements by clarifying that successful ransomware attacks as well as any instance where unauthorized users gain access to privileged accounts (e.g. administrative accounts) are subject to the DFS reporting requirements.[1]

AN INCREASING THREAT

According to the DFS guidance, in the past 15 months supervised entities have reported 74 ransomware attacks to DFS. These attacks have ranged in severity, but all proceed in a similar fashion: hackers gain access to a company's network through phishing, by exploiting unpatched vulnerabilities, or through unsecured

[1] Clifford Chance has published a series of briefings discussing the NYDFS Cybersecurity Regulations. For more information, see here.

Remote Desktop Protocols (RDPs), and then acquire administrative access to commence ransomware attacks.

Surprisingly, DFS reported that only 17 companies paid a ransom. This proportion—less than 25%—is significantly lower than global surveys would suggest, with many reporting that more companies acquiesce to ransomware demands than do not, despite government authorities uniformly advising companies not to do so. The guidance appears to try to discourage companies from paying a ransom, noting that payments do not guarantee recovery of data or prevent leaks—and they may embolden attackers. DFS also cited recent guidance from the Office of Foreign Assets Control (OFAC) that ransomware payments may violate sanctions laws.[2]

DFS also noted that companies have reported a "growing number" of attacks against critical vendors. In February, the Department issued a Cyber Insurance Risk Framework to help insurers effectively price and manage their cyber risk, citing the steady rise in ransomware attacks as one of the primary drivers of increasing risk and uncertainty in the industry.[3] In that Framework, DFS expressed particular concern over the systemic risk attacks on widely-used vendors and software can create. The DFS reiterated this concern here, name-checking SolarWinds and the recently-uncovered Microsoft Exchange vulnerability in the opening paragraph of its letter.

THE GUIDANCE: PREVENTION AND PREPARATION

The guidance lists nine controls that DFS says will help companies prevent and prepare for a ransomware attack:

1. **Email Filtering and Anti-Phishing Training**. Companies should implement anti-phishing training and conduct periodic tests to determine whether remedial training is necessary. Filters should also be put in place to block spam and harmful email.
2. **Vulnerability and Patch Management**. Companies should conduct periodic penetration testing and have a program to identify, assess, track, and remediate vulnerabilities. This includes patch management, which should be automated where possible.
3. **Multi-Factor Authentication**. Companies should require multi-factor authentication for all remote access and third-party applications, as well as logins to privileged accounts.
4. **Disable Remote Desktop Protocol (RDP) Access**. Companies should disable RDP unless strictly necessary—and then access should be restricted and secured.
5. **Password Management**. Companies should have password policies in place with specific requirements for privileged accounts (16 characters or longer, password vaulting privileged access management, forbidding caching and commonly-used passwords).

---

2 For more on the risks to consider when deciding whether to pay, see our analysis on Law360 here.
3 For more on the Cyber Insurance Risk Framework, see our briefing here.

6. **Privileged Access Management**. Companies should restrict privileged accounts, assigning the minimum level of access necessary for job functions. All company users should have non-privileged accounts for tasks that do not require privileged access. Privileged account access should be audited periodically.
7. **Monitoring and Response**. Companies should have a way to monitor their systems and networks for suspicious activity, commensurate with the size and complexity of their network. This should include at a minimum Endpoint Detection and Response (EDR). It may also include lateral movement detection and a Security Information and Event Management (SIEM) solution.
8. **Tested and Segregated Backups**. Companies should have a set of regularly tested backups segregated from their networks and offline.
9. **Incident Response Plan**. Companies should ensure incident response plans include ransomware response and are regularly tested by senior leadership (up to and including the CEO).

Notably, each control is specifically mapped to at least one provision of the Department's Cybersecurity Regulation, reinforcing the guidance's admonition that DFS "expects" regulated companies to implement these controls wherever possible.

CONCLUSION

This guidance is yet another indication that DFS has made cybersecurity one of its key priorities. Senior DFS officials have recently stated that cybersecurity matters comprise 20% of the Department's enforcement caseload, a surprisingly high percentage given the Department's broad enforcement mandate. In the past year, the Department has issued several fines of over a million dollars for failures to comply with the Cybersecurity Regulation, making it one of the most active US regulators in the realm of cybersecurity.[4] Especially after this guidance, it would not be surprising to see DFS make an example out of a company that has failed to implement these controls and then suffers a ransomware attack. Companies must make effective cybersecurity controls a priority—not just to protect against attacks, but to avoid costly enforcement actions.

Effective ransomware response begins before an attack. Clifford Chance has published a Ransomware Playbook to help companies prevent and respond to attacks.

[4] For more on DFS cybersecurity enforcement actions, see our briefings here, here, and here.

CONTACTS

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

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@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

www.cliffordchance.com

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

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.