April 21, 2020 | 2:20 pm

Information on Novel Coronavirus

NY State remains on PAUSE through May 15. All non-essential workers are directed to work from home, and everyone is required to wear a face covering and maintain a 6-foot distance from others in public.

GET THE FACTS >

Department of Financial Services

April 13, 2020

Re: Guidance to Department of Financial Services ("DFS") Regulated Entities Regarding Cybersecurity Awareness During COVID-19 Pandemic

To: All New York State Regulated Entities

As we face an unprecedented threat from the novel coronavirus known as "COVID-19," every organization's highest priority must be health and safety. The extraordinary steps necessary to combat the COVID-19 pandemic have also created new challenges as regulated entities work to continue operating and providing critical services. Among these new risks is a significant increase in cybercrime, as criminals seek to exploit the situation.[1]

The Department of Financial Services ("DFS") has identified several areas of heightened cybersecurity risk as a result of this crisis. As called for by DFS's cybersecurity regulation, 23 NYCRR Part 500, regulated entities should assess the risks described below and address them appropriately.[2]

We also remind all regulated entities that, under 23 NYCRR Section 500.17(a), covered Cybersecurity Events must be reported to DFS as promptly as possible and within 72 hours at the latest. Prompt reporting will enable DFS to respond quickly to new threats as DFS works to protect consumers and the financial services industry in these difficult times.

Heightened Risks

I. Remote Working

g forced by COVID-19 has created new security
ı these new vulnerabilities.[3] These heightened risks to regulated entities' networks and Nonpublic Information[4] include:

- Secure Connections. Companies should make remote access as secure as possible under the circumstances. This includes the use of Multi-Factor Authentication and secure VPN connections that will encrypt all data in transit. See 23 NYCRR §§ 500.12 & 500.15.
- Company-Issued Devices. As new devices such as computers and phones are acquired or repurposed for remote working, regulated entities should ensure that they are properly secured. This includes locking down the devices so applications cannot be added or deleted by the user, and installing appropriate security software, such as Endpoint Detection & Response and Mobile Device Management.
- Bring Your Own Device (BYOD) Expansion. Regulated entities that have expanded their BYOD policies to enable mass remote working should be aware of the security risks and consider mitigating steps. Some personal devices are not properly secured or are already compromised. If an expanded BYOD policy is necessary, compensating controls should therefore be considered.
- Remote Working Communications. Remote working has increased reliance on video and audio-conferencing applications, but these tools are increasingly targeted by cybercriminals. Regulated entities should configure these tools to limit unauthorized access, and make sure that employees are given guidance on how to use them securely.
- Data Loss Prevention. Employees may be using unauthorized personal accounts and applications, such as email accounts, to remain productive while remote working. Regulated entities should remind employees not to send Nonpublic Information to personal email accounts and devices. Anticipating and solving productivity problems will reduce the temptation to use such devices.

II. Increased Phishing and Fraud

There has been a significant increase in online fraud and phishing attempts related to COVID-19. For example, the FBI has reported that criminals are using fake emails that pretend to be from the Centers for Disease Control and Prevention ("CDC"), ask for charitable contributions, or offer COVID-19 relief such as government checks.[5]

employees to be alert for phishing and fraud emails, at the earliest practical opportunity. Now that face-to-face work is curtailed, authentication protocols may need to be updated – especially for key actions, like security exceptions and wire transfers.

III. Third-Party Risk

The challenges created by the COVID-19 pandemic have also affected third-party vendors, and regulated entities should re-evaluate the risks to critical vendors. See 23 NYCRR § 500.11. Regulated entities should coordinate with critical vendors to determine how they are adequately addressing the new risks.

Conclusion

The COVID-19 pandemic has disrupted normal operations in the financial services industry and beyond, and cyber criminals are exploiting the crisis. Despite the extraordinary challenges, regulated entities should remain vigilant. By following good cybersecurity practices, entities can identify, mitigate, and manage the risks.

---

[1] See DHS Cybersecurity and Infrastructure Security Agency ("CISA"), COVID-19 Exploited by Malicious Cyber Actors (April 8, 2020).

[2] Heightened cyber risk should also be addressed in the COVID-19 operational preparedness plans called for by DFS guidance issued on March 10, 2020. See Guidance to New York State Regulated Institutions and Request for Assurance of Operational Preparedness Relating to the Outbreak of the Novel Coronavirus.

[3] See FBI, Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments (April 1, 2020); U.S. Secret Service, Secret Service Issues COVID-19 (Coronavirus) Phishing Alert (March 9, 2020).

[4] 23 NYCRR § 500.01(g).

[5] See FBI, FBI Sees Rise In Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic (March 20, 2020).