Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
Office of the Comptroller of the Currency
Conference of State Bank Supervisors

March 16, 2020

To: CEOs, CIOs, and CISOs

Subject: Managing Cybersecurity Risks Related to Coronavirus Disease 2019 (COVID-19)

As U.S. financial institutions manage the impacts of COVID-19, the agencies are relaying information from the Department of Homeland Security (DHS) and the Federal Financial Institutions Supervisory Council (FFIEC) that may help you protect your organization and customers.

- On March 13, 2020, the Cybersecurity and Critical Infrastructure Agency (CISA) of DHS issued Awareness Alert AA20-073A[i], "Enterprise VPN Security," to advise organizations of cybersecurity considerations and mitigations for enterprise virtual private network (VPN) solutions enabling teleworking employees to connect to an organization's information technology (IT) network. As organizations implement telework, CISA encourages them to adopt a heightened state of cybersecurity.
- On March 6, 2020, CISA issued a Cyber Alert[ii], "Defending Against COVID-19 Cyber Scams," reminding individuals to remain vigilant for scams related to COVID-19. Cyber actors have been sending emails with malicious attachments or links to fraudulent websites attempting to trick recipients into revealing sensitive information or donating to fraudulent charities or causes. Organizations are encouraged to caution staff and customers in handling any email with a COVID-19-related subject line, attachment, or hyperlink, and be wary of social media pleas, texts, or calls related to COVID-19. Such cautions are particularly important as banks have urged customers to shift to use of banking through the internet and mobile banking to avoid contact through in-person banking.
- On March 6, 2020, CISA issued a CISA Insights document[iii], "Risk Management for Novel Coronavirus (COVID-19)," outlining physical, supply chain, and cybersecurity issues that may arise from the spread of COVID-19. As organizations explore various alternate workplace options in response to COVID-19, CISA recommends examining the security of information technology systems by taking the following steps:
    - Secure systems that enable remote access.
        - Ensure Virtual Private Network and other remote access systems are fully patched.
        - Enhance system monitoring to receive early detection and alerts on abnormal activity.
        - Implement multi-factor authentication.
    - Ensure all machines have properly configured firewalls, as well as anti-malware and intrusion prevention software installed.oTest remote access solutions capacity, and increase capacity, as necessary.
    - Ensure continuity of operations plans or business continuity plans are current.
    - Increase awareness of information technology support mechanisms for employees who work remotely.

- Update incident response plans to consider workforce changes in a distributed environment.

The document also provides recommendations for infrastructure protection and managing supply chain risks.

On March 6, 2020, the FFIEC issued a press release[iv], "FFIEC Highlights Pandemic Preparedness Guidance," updating guidance identifying actions that financial institutions should take to minimize the potential adverse effects of a pandemic. Supervised institutions should periodically review related risk management plans, including continuity plans, to ensure their ability to continue to deliver products and services in a wide range of scenarios and with minimal disruption. The guidance is implemented by the agencies as follows:

- Board of Governors of the Federal Reserve System issued SR 20-3 / CA 20-2[v] (March 10, 2020): Interagency Statement on Pandemic Planning
- Federal Deposit Insurance Corporation issued FIL-14-2020[vi] (March 6, 2020): Interagency Statement on Pandemic Planning
- Office of the Comptroller of the Currency issued OCC Bulletin 2020-13[vii] (March 6, 2020): Pandemic Planning: Updated FFIEC Guidance

Financial institutions are encouraged to notify law enforcement and their primary federal and state regulator(s) of any cyber activity targeting the institution or its customers. More information about financial institution cybersecurity is available from the FFIEC at https://www.ffiec.gov/cybersecurity.htm.

---

[i] https://www.us-cert.gov/ncas/alerts/aa20-073a
[ii] https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams
[iii] https://www.cisa.gov/sites/default/files/publications/20_0306_cisa_insights_risk_management_for_novel_coronavirus.pdf
[iv] https://www.ffiec.gov/press/pr030620.htm
[v] https://spweb.frb.gov/sites/BSRWeb/SR/Policy/Pages/SRLtrs/SR2003.aspx
[vii] https://www.fdic.gov/news/news/financial/2020/fil20014.html
[vii] https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-13.html

Thank you,

Emergency Communications System