Published on *The National Law Review* https://natlawreview.com

COVID-19 Update: Cybersecurity and Data Privacy Best Practices Remain Critical During the Coronavirus Pandemic

Article By:

Joseph V. Moreno

Keith M. Gerver

Hyungjoo Han

Stephen Weiss

With much of the nation's workforce transitioning to telework for the foreseeable future, hackers and scammers are lurking to take advantage of technical vulnerabilities and anxious targets. As companies amass—and create new repositories of—personal and health information for employees and customers as a result of the coronavirus (COVID-19) pandemic, adherence to cyber and data privacy best practices remains critically important. Companies, firms, employees, and consumers are increasingly relying on home networks, virtual workspaces, videoconferencing, and other forms of remote work practices, further opening the door to cyber concerns.

Over the past few weeks, various federal and state agencies and industry groups have issued guidance and published information on these threats and recommendations. This information is a helpful reminder of best practices that companies should follow to solidify their cyber controls.

I. Cybersecurity Concerns Relating to Teleworking

- The Cybersecurity and Infrastructure Security Agency (CISA) published an alert to employers stating that telework options require an enterprise virtual private network (VPN) solution to connect employees to an organization's information technology network. The alert contains a number of recommendations for organizations to review when considering alternate workplace options for employees. (Mar 13, 2020)

- The Financial Industry Regulatory Authority (FINRA) published an information notice encouraging firms and their associated persons to take appropriate measures to address increased cyber vulnerabilities and protect customer and firm data on company and home networks as well as mobile devices. The notice provides measures that firms and associated persons can take to reduce cyber risks related to the COVID-19 outbreak. (Mar 26, 2020)

II. Continuity of Operations Plans

- New York's Department of Financial Services (DFS) issued guidance to regulated institutions in the virtual currency space. DFS urges businesses to implement a preparedness plan to manage the risk of disruption to services and operations in light of the COVID-19 outbreak. At a minimum, plans should include an assessment of potential increased risk of cyber-attacks and fraud. Responses detailing such plans are required within 30 days of the notice. (Mar 10, 2020)

III. Data Privacy Issues

- Entities that are regulated under the Health Insurance Portability and Accountability Act (HIPAA) should review two pieces of guidance from the U.S. Department of Health and Human Services: (1) a bulletin (Feb 2020) addressing application of the HIPAA Privacy Rule in the context of the COVID-19 outbreak, and (2) a notice (Mar 23, 2020) regarding enforcement of HIPAA rules against health care providers in connection with the good faith provision of telehealth during the COVID-19 nationwide public health emergency.

- California's Attorney General rejected industry requests to postpone the effective date of the state's new data privacy law, the California Consumer Privacy Act (CCPA), which is currently set for July 1, 2020. Unless this changes, covered businesses that collect certain health related information from California residents, employees, or customers should plan to comply with the CCPA's various requirements regarding the collection and use of personal information. Covered businesses subject to the CCPA should specifically consider the law's implications if they intend to share their employees' or consumers' personal information as it relates to the COVID-19 pandemic with health authorities.

IV. Critical Infrastructure

- CISA issued an advisory memorandum (Mar 28, 2020) for state, local, and tribal authorities and their industry partners to assist in the identification of essential workers in seventeen critical infrastructure sectors in light of the COVID-19 pandemic.

V. Anti-Fraud Precautions

- CISA published a warning to individuals to remain vigilant for scams related to COVID-19. These include emails with malicious attachments or links to fraudulent websites to trick victims into revealing sensitive information or donating to fraudulent charities. (Mar 6, 2020)

- The Federal Bureau of Investigation (FBI) issued a public service announcement warning that it has seen a rise in COVID-19-related fraud schemes from scammers trying to steal money or personal information. The public should remain vigilant about fake emails claiming to be from the Centers for Disease Control and Prevention (CDC), phishing emails asking the recipient to verify their personal information to receive a federal economic stimulus check, and offers to sell counterfeit treatment or equipment to prevent, treat, diagnose, or cure

COVID-19. (Mar 20, 2020)

- The Federal Trade Commission (FTC) is hosting a page dedicated to helping consumers avoid coronavirus scams, including how to handle robocalls, online offers for vaccinations and home test kits, and how to identify fraudulent emails about government stimulus checks and public health information.

- The Department of Justice (DOJ) has created a page outlining its efforts to detect, investigate, and prosecute wrongdoing related to fraud schemes and COVID-19. Individual United States Attorney's Offices have also launched efforts to protect residents, such as the Virginia Coronavirus Fraud Task Force.

- The Consumer Financial Protection Bureau (CFPB) published an informational guidance for consumers regarding the rise of COVID-19 related fraud schemes. In addition to scams related to vaccines, test kits, cures and treatments, there has been an increase in the number of fake coronavirus-related charity scams, "person in need" scams from purported friends and relatives asking for money, and scams targeting Social Security benefits. Individuals who believe they are a victim of a scam or attempted fraud involving COVID-19 can report it to the National Center for Disaster Fraud Hotline at 866-720-5721 or via email to disaster@leo.gov. Individuals who believe they are the victim of an internet scam or cyber-crime should report it to the FBI's Internet Crime Complaint Center at 804-261-1044 or ic3.gov.

VI. Looking Ahead

As state and federal governments respond to the cybersecurity challenges posed by the COVID-19 pandemic over the coming weeks and months, businesses should stay abreast of additional guidance and information provided by government agencies and regulators. At the same time, companies must take steps to maintain a healthy (remote) security environment: placing a premium on continuing regular internal communications, keeping a close eye on potential system vulnerabilities, and practicing good digital hygiene.

National Law Review, Volumess X, Number 94