Managing Cybersecurity and Data Privacy Concerns During the COVID-19 Pandemic

IN SHORT

The Situation: The global spread of the novel coronavirus (COVID-19) has prompted the workforce to migrate from the office to remote-working environments and businesses to adopt new data collection, use, and disclosure practices to address the outbreak's effect on the organization.

The Issues: Responses to the pandemic are giving rise to cybersecurity and data privacy concerns.

Looking Ahead: In response to these concerns, U.S. and international authorities are taking action to encourage—and in some instances to require—organizations to monitor and respond to these evolving cybersecurity and data privacy issues.

The COVID-19 pandemic poses heightened cybersecurity and data privacy risks for businesses. With the rapid deployment of remote-working solutions, malicious actors already are attempting to exploit weaknesses due to reduced IT staffing and the use of personal devices and insecure public and home networks. Businesses also are experiencing an uptick in social engineering schemes aimed at inducing employees to open coronavirus-related messages infected with malware. Meanwhile, many businesses are facing data privacy questions regarding the collection and disclosure of personal information as they monitor the virus's impact on their organizations.

Animated by these concerns, U.S. and international authorities are taking action to guard against possible disruptions to the nation's critical infrastructure and to help businesses manage the cybersecurity and data privacy risks posed by the pandemic.

> U.S. and international authorities are warning businesses of increased cybersecurity threats from actors seeking to exploit the pandemic.

Cybersecurity

U.S. and international authorities are warning businesses of increased cybersecurity threats from actors seeking to exploit the pandemic. They also have provided guidance on mitigating cybersecurity risks and, in some instances, imposed reporting obligations on regulated entities. Examples include:

- **New York Department of Financial Services ("NYDFS")**:
  - On March 10, 2020, NYDFS released an industry letter requiring that "each regulated institution submit a response to DFS describing the institution's plan of preparedness to manage the risk of disruption to its services and operations … as soon as possible and in no event later than thirty (30) days from the date of [the] letter." Among the issues the plan

must address is "[a]n assessment of potential increased cyber-attacks and fraud."

- In a separate industry letter directed to regulated entities engaged in "Virtual Currency Business Activity," NYDFS specifically underscored "the risk to Virtual Currency businesses of increased instances of hacking, cybersecurity threats, and similar events, as bad actors attempt to take advantage of a COVID-19 outbreak, and the possible resulting need for heightened security measures, such as enhanced triggers for fraudulent trading or withdrawal behavior."

- NYDFS has extended the compliance deadline for annual statements certifying compliance with the Cybersecurity Regulation (23 NYCRR 500) from April 15, 2020, to June 1, 2020. However, this extension does not alter a company's 72-hour notification obligations of a cybersecurity event.

- **Cybersecurity and Infrastructure Security Agency ("CISA")**: On March 13, 2020, CISA issued an alert urging businesses to adopt a heightened state of cybersecurity as they transition employees to remote working options. CISA recommended alerting employees to increased coronavirus-related phishing attempts and pointed IT professionals to a July 2016 guide to telework security issued by the National Institute of Standards and Technology.

- **Federal Trade Commission ("FTC")**: On March 18, 2020, the FTC issued cybersecurity tips for remote working during the coronavirus outbreak, which urge individuals to follow their employer's security practices while home, and provides advice for securing home networks, disposing of sensitive data securely, and ensuring devices are protected with strong passwords.

- **North American Electric Reliability Corporation ("NERC")**: On March 10, 2020, NERC issued an alert, which required its registered entities to report by March 20, 2020, the status of their emergency pandemic plans. NERC also recommended that its registered entities "[a]nticipate and prepare for coronavirus-themed opportunistic social engineering attacks," to "[t]ake steps to ensure continued visibility and maintenance of cyber assets in the event of staffing disruptions … [and to] [e]nsure information and communications technology resources are appropriate to accommodate increased use of remote work arrangements consistent with business continuity plans, without compromising security."

- **Financial Industry Regulatory Authority ("FINRA")**: On March 26, 2020, FINRA issued an alert on measures that firms and their associated persons should take to address the increased vulnerability to cybersecurity attacks and to protect customer and firm data. While FINRA stated that the alert "does not create any new legal requirements or change any existing regulatory obligations," the guidance provides practical measures to mitigate cybersecurity risks, including by providing employees with secure connections through virtual-private networks ("VPNs") or multifactor authentication, and by recommending that associated persons review the firm's file storage and back-up policies, particularly when accessing files containing customer personally identifiable information on a personal device.

Data Privacy

U.S. and international authorities have issued COVID-19 specific guidance to assist organizations as they navigate novel data privacy issues.

- **Department of Education ("DOE")**: In March 2020, the DOE issued guidance on the Family Educational Rights and Privacy Act ("FERPA") in the form of "frequently asked questions." The guidance reminds officials that although FERPA generally requires consent before the disclosure of a student's personally identifiable information ("PII"), the "health or safety emergency" exception to prior consent may apply to certain COVID-19-related scenarios.

- **Department of Health and Human Services ("HHS")**: Effective March 15, 2020, HHS waived certain penalties and sanctions against covered hospitals for noncompliance with certain provisions of the HIPAA Privacy Rule, including the requirement to distribute a notice of privacy practices and the patient's right to request privacy restrictions.

- **Equal Employment Opportunity Commission ("EEOC")**: On March 19, 2020, the EEOC updated a public statement (previously issued on March 18, 2020), which clarifies that during

the COVID-19 pandemic, employers may take certain measures that impact employee privacy, provided that such actions are job-related and consistent with business necessity. For example, an employer is authorized to measure employees' body temperatures—an activity that is typically considered a medical examination.

- **International Data Protection Authorities**: A number of data protection authorities ("DPAs") in Europe, Latin America, and the APAC region have provided guidance on issues arising under applicable data privacy laws. For example, the European Data Protection Board issued a formal statement on the processing of personal data in the context of the COVID-19 outbreak, calling on data controllers and processors to ensure the protection of the personal data of data subjects while at the same time taking measures to prevent further spread of the virus.

We have compiled updated guidelines issued by DPAs.

In addition to new regulatory guidance and any additional reporting or other requirements, existing privacy laws, such as the California Consumer Privacy Act, may be relevant to new or changed practices for the collection, use, or disclosure of personal data. Companies also may receive government requests for information—including those outside the ordinary course, such as public health authorities seeking data to help track the pandemic—that give rise to novel issues under applicable privacy laws and company policies

THREE KEY TAKEAWAYS

1. Businesses should take immediate steps to mitigate heightened cybersecurity risks arising from the surge in remote work, as identified in our previous *Alert*, "Coronavirus and Remote Work Heighten Cybersecurity Risks," and confirm that their incident response and business continuity plans account for the current conditions.
2. Businesses should stay current with evolving data privacy guidance relating to the pandemic, and align with their internal and consumer-facing policies, or update such policies as necessary, to reduce risk.
3. Regulated entities should expect increasing and specific guidance from their regulatory bodies and meet any new requirements.


Lisa M. Ropple
Boston


Samir C. Jain
Washington


Jennifer C. Everett
Washington


Jörg Hladjk
Brussels


Undine von Diemar
Munich


Todd S. McClelland
Atlanta


Mauricio F. Paez
New York


Guillermo E. Larrea
Mexico City

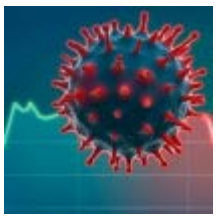
Clinton P. Oxford, an associate in the Washington Office, assisted in the preparation of this Commentary.

SHARE THIS ON LINKEDIN

FORWARD TO A COLLEAGUE

YOU MIGHT BE INTERESTED IN: Go To All Recommendations >>

Coronavirus and Remote Work Heighten Cybersecurity Risks



COVID-19 Crisis Response and Post-Recovery Planning: Financial Litigation Considerations

HHS Issues Limited Waivers of HIPAA Sanctions and Penalties for Hospitals in Response to COVID-19

Coronavirus: Critical Considerations for the Energy Industry

SUBSCRIBE SUBSCRIBE TO RSS

Jones Day is a global law firm with more than 2,500 lawyers on five continents. One Firm Worldwide®

North Point, 901 Lakeside Avenue, Cleveland, Ohio 44114-1190
www.jonesday.com