COVID-19: Cybersecurity and Data Privacy Implications

UPDATED APRIL 17, 2020

What Are We Seeing and Hearing?

- **The COVID-19 pandemic is significantly increasing cybersecurity and data privacy challenges**

- **Cybersecurity**
  - Organizations face increased risk of cyberattacks ranging from ransomware attacks targeting the health care sector and other essential sectors, to phishing emails seeking to exploit new network vulnerabilities in companies adjusting to operational disruptions and workplace modifications
  - External crises often bring opportunistic attacks on business networks; the current climate is particularly challenging because organizations must try to mitigate such attacks while also adapting their IT systems to support remote workforces

- **Data privacy**
  - Organizations increasing the volume of data they collect, use and disclose—or changing the type of such data (*e.g.*, by collecting employee medical and travel data)—face increased challenges in complying with federal and state (and foreign) privacy laws
  - Businesses operating in California face additional challenges given regulatory uncertainty relating to the privacy provisions of the California Consumer Privacy Act (CCPA), as well as recent developments in private enforcement of the new law

- **While regulators have relaxed certain cybersecurity and data privacy rules, civil and criminal enforcement is an increasing priority**
  - HHS waived or relaxed enforcement of certain HIPAA provisions against hospitals and other health care providers
  - NYDFS extended deadline for certain cybersecurity-related compliance filings but otherwise is continuing to require compliance with existing regulations by covered financial institutions and insurance companies
  - SEC is examining the timeliness and accuracy of disclosures related to cyber risks and incidents
  - California AG rejected requests from business groups to delay CCPA enforcement; enforcement scheduled to begin July 1
  - DOJ is prioritizing investigations and prosecutions of COVID-19-related cybercrimes

Statements from Key Regulators

- **US Department of Justice**
  - March 16 Statement (Attorney General)[1]
    - Directed US Attorneys to prioritize investigation and prosecution of cyber frauds related to COVID-19, citing reports of malware attacks and phishing emails sent by scammers posing as the WHO and CDC

- **California Attorney General**
  - March 19 Statement (Office of the Attorney General)[2]
    - Confirmed the AG is "committed to enforcing the [CCPA] upon finalizing the rules or July 1, whichever comes first"
    - Encouraged businesses "to be particularly mindful of data security in this time of emergency"

- **US Department of Health and Human Services**
  - Bulletins (Office for Civil Rights)
    - February - advised covered entities that the protections of the HIPAA Privacy Rule, which establish national standards to protect medical records and other personal health information (PHI), "are not set aside during an emergency"[3]
    - March - waived sanctions and penalties for covered hospitals that do not comply with certain Privacy Rule provisions [4]
  - Notices of Enforcement Discretion (Office for Civil Rights)
    - March 17 - announced that HHS will exercise enforcement discretion for HIPAA violations against hospitals and other health care providers arising from "good faith" uses of telehealth (audio and video communication technologies)[5]
    - April 2- announced that HHS will not penalize "good faith" uses or disclosures of PHI by health care providers or their business associates for public health or health oversight purposes[6]
    - April 9 - announced that HHS will not impose penalties for HIPAA violations against covered entities or business associates in connection with "good faith" participation in the operation of COVID-19 testing sites[7]

Statements from Key Regulators

- **US Securities and Exchange Commission**
  - March 25 Disclosure Guidance (Division of Corporation Finance)[8]
    - Provided guidance regarding COVID-19-related disclosures and other securities law obligations
    - In discussion of evolving business risks, cited the SEC's past statement "highlight[ing] that although no existing disclosure requirement specifically refers to cybersecurity risks and cyber incidents, a number of requirements may impose an obligation on companies to disclose such risks and incidents"

- **New York State Department of Financial Services**
  - March 10 Guidance Letter (Executive Deputy Superintendent—Banking)[9]
    - Required regulated financial institutions to submit within 30 days (April 9) a "plan of preparedness to manage risk of disruption to . . . services and operations," including "[a]n assessment of potential increased cyber-attacks and fraud"
  - March 12 Relief Order (Superintendent of Financial Services)[10]
    - Advised regulated entities that they "remain subject to . . . full supervision and oversight" and "shall maintain appropriate safeguards and controls, including . . . those related to data protection and cybersecurity"
    - Ordered 45-day extension for annual cybersecurity compliance certifications; certifications now due June 1
      - Extension does not apply to required notice of a "cybersecurity event" under 23 NYCRR 500.17(a)

- **Federal Trade Commission**
  - April 9 Guidance (Division of Consumer & Business Education)[11]
    - Provided guidance on FTC's Business Blog for education technology companies supporting remote learning for schools during the pandemic to make clear that the Children's Online Privacy Protection Act (COPPA) permits schools to consent on behalf of parents of children under 13 to the collection of personal data for educational purposes

Cybersecurity: Elevated Risk of Ransomware Attacks

- **Hospitals and other organizations in the health care sector face elevated risk of ransomware attacks because of their perceived willingness to pay**
  - Other sectors viewed as essential to the COVID-19 response may also face elevated risk of such attacks

- **COVID-19-related ransomware attacks have already been publicly reported in the US and overseas**
  - On March 12-13, a major COVID-19 testing hospital in the Czech Republic was reportedly hit with a ransomware attack that shut down its computers and forced relocation of patients
  - On March 14, a hacker group reportedly conducted a ransomware attack against a UK medical research company that was scheduled to test a potential vaccine for COVID-19; the hackers stole and released sensitive medical and personal information of over 2,300 former patients after the company refused to pay the ransom
  - On March 22, Spanish police reported that several hospitals had received emails purporting to offer information on COVID-19 that contained PDF attachments that, if opened, activated ransomware commonly associated with computer crime groups in Eastern Europe
  - On April 1, a California biotechnology company reportedly working on COVID-19-related research disclosed in an SEC filing that it had experienced an attempted ransomware attack and data breach; it noted that it had "isolated the source of the attack and restored normal operations with no material day-to-day impact to the Company or the Company's ability to access its data", and that it was working with outside experts and law enforcement to investigate the attack

Cybersecurity: Elevated Risk of Unauthorized Access

- **Organizations face elevated risk that malicious actors will exploit operational vulnerabilities created by the shift to telework to bypass security measures and gain unauthorized access to systems and information, potentially leading to data breach and data loss**
  - Key vulnerabilities include
    - Inadequate physical security and/or access controls for IT assets, such as multi-factor authentication for accessing networks and email
    - Forwarding of company information to personal email accounts
    - Storage of company information on unprotected personal computers or other personal devices
    - Failure of warnings about potentially malicious links and attachments to appear on mobile devices and personal computers
    - Failure of financial or accounting controls to protect against email scams designed to convince finance department personnel employees to wire funds to accounts controlled by scammers posing as company executives or vendors

- **On March 13, the US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) issued an alert on "Enterprise VPN Security" urging companies moving to remote environments in response to COVID-19 to "adopt a heightened state of cybersecurity"[12]**
  - On April 8, CISA followed up by issuing a joint advisory with the UK government's National Cyber Security Centre, "COVID-19 Exploited by Malicious Bad Actors," that provides a summary of the types of threats detected to date, noting that "the surge in teleworking has increased the use of potentially vulnerable services," including VPNs, that "amplify[]" these threats, and offers mitigation advice for both organizations and individuals[13]

Data Privacy: CCPA Enforcement Update

- **CCPA implementing regulations are not yet final**
  - Regulations still under review include key privacy provisions, including the right-to-know and opt-out provisions, as well as provisions governing the obligation of companies to respond to requests to know and requests to delete within 45 days

- **California AG remains committed to keeping the July 1 enforcement date in place**
  - Several businesses and national trade associations had urged the AG to delay public enforcement to 2021, citing difficulties in developing CCPA-compliant policies in light of workforce disruptions from COVID-19 and continuing regulatory uncertainty
    - The AG's Office responded that it plans to begin enforcement "upon finalizing the rules or July 1, whichever comes first"

- **Even as public enforcement has not yet begun, recently filed putative class actions suggest courts will soon be asked to decide whether the CCPA's private enforcement provision extends to privacy claims outside of the data breach context**
  - In late March and early April, several CCPA actions were filed against social media and technology companies, including the maker of video conferencing software that has become widely used during the COVID-19 pandemic
    - Notably, these actions do not allege data breaches or claims under the CCPA's provision expressly creating a private right of action for consumers harmed by data breaches; rather, they appear to argue that an *implied* private right of action exists permitting consumers to sue to enforce the law's data privacy provisions even in the absence of a breach

- **Companies operating in California should not wait for CCPA regulations to be finalized to update their policies and procedures on data privacy in light of the impact of COVID-19**
  - Companies experiencing an increase in the volume of data they collect, use and/or disclose—or changes in the type of such data—should pay particular attention to ensuring their policies and procedures related to data privacy (as well as cybersecurity) are CCPA-compliant

Risk Mitigation Considerations

- **Organizations should review and strengthen their existing cybersecurity risk controls to address network and human vulnerabilities created or exacerbated by COVID-19**
  - Identify existing controls, including as to third parties, such as
    - Automated flags/checkboxes highlighting whether an email address is external
    - Warnings when users click on external links or open attachments from an external source
    - Accounting controls that mitigate risk of unauthorized wire transfers arising from business email compromise schemes, including maker-checker, call-back and other controls
    - Requiring employees to use VPN with multi-factor authentication to access networks
    - Prohibitions on accessing company files via personal email accounts
  - Assess—and continue frequently to re-assess—how existing controls function in remote and mobile environments
    - If day-to-day cyber-risk controls do not function well in a remote-work context, consider whether and how they should be modified based on practical necessity and degree of risk
    - Document the nature and expected duration of any changes or exceptions made
  - Continually reinforce the importance of cybersecurity risk controls and policies
    - Conduct targeted, supplemental cybersecurity trainings to reinforce existing policies and procedures and educate employees about key differences in the work-at-home environment
    - Warn employees that malicious third parties may attempt to pose as senior company management—what the SEC has described as “Emails from False Executives”—and try to convince them to sidestep technical controls in connection with COVID-19-related issues
      - Consider running periodic phishing tests and publishing the results (anonymously)
    - Emphasize that employees may face repercussions for failing to adhere to defined security protocols

- **Confirm that incident response plans are effective in a remote environment and breach notifications can be made on the timelines prescribed by all relevant federal, state and foreign authorities**

Disclosure Considerations

- **Public companies should consider whether disclosure of cybersecurity risks or incidents specific to COVID-19 is required under federal securities laws**
  - SEC has previously highlighted that, although no existing disclosure requirement specifically refers to cybersecurity risks and incidents, a number of requirements may impose an obligation on companies to disclose such risks and incidents
  - SEC has recently advised public issuers that they may need to update the risk factor and MD&A sections of periodic reports in response to the COVID-19 pandemic
    - Cravath has posted on its website a separate publication, *COVID-19: Initial Insights and Expectations for Government Enforcement*, with more information on how companies should consider approaching questions related to the effect of the COVID-19 pandemic on SEC disclosures generally
    - Earlier this year, Cravath also published a client memorandum entitled U.S. Securities and Exchange Commission Issues Report on Cybersecurity and Resiliency Practices, with more information on how companies can manage and mitigate cybersecurity risks related to market systems, disclosure of material risks and incidents, customer data protection and compliance[14]

References

[1] ***Memorandum for All U.S. Attorneys***, Office of the U.S. Attorney General, U.S. Department of Justice, March 16, 2020, ***available*** here

[2] Marty Swant, ***Citing COVID-19, Trade Groups Ask California's Attorney General To Delay Data Privacy Enforcement***, FORBES, March 19, 2020, ***available*** here

[3] ***Bulletin: HIPAA Privacy and Novel Coronavirus***, Office for Civil Rights, U.S. Department of Health and Human Services, February 2020, ***available*** here

[4] ***Bulletin: Limited Waiver of HIPAA Sanctions and Penalties During a Nationwide Public Health Emergency***, Office for Civil Rights, U.S. Department of Health and Human Services, March 2020, ***available*** here

[5] ***Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency***, Office for Civil Rights, U.S. Department of Health and Human Services, March 17, 2020, ***available*** here

[6] ***Notification of Enforcement Discretion under HIPAA to Allow Uses and Disclosures of Protected Health Information by Business Associates for Public Health and Health Oversight Activities in Response to COVID-19***, Office for Civil Rights, U.S. Department of Health and Human Services, April 2, 2020, ***available*** here

[7] ***Notification of Enforcement Discretion under HIPAA to Allow Operation and Disclosures of Testing Sites by Business Associates for Public Health and Health Oversight Activities in Response to COVID-19***, Office for Civil Rights, U.S. Department of Health and Human Services, April 9, 2020, ***available*** here

[8] ***CF Disclosure Guidance: Topic No. 9***, U.S. Securities and Exchange Commission, March 25, 2020, ***available*** here

[9] ***Guidance to New York State Regulated Institutions and Request for Assurance of Operational Preparedness Relating to the Outbreak of the Novel Coronavirus***, New York State Department of Financial Services, March 10, 2020, ***available*** here

[10] ***Order Granting Temporary Relief to COVID-19 Affected Regulated Entities and Persons***, New York State Department of Financial Services, March 12, 2020, ***available*** here

[11] ***Guidance to EdTech Companies facilitating remote learning during COVID-19***, Federal Trade Commission, April 9, 2020, ***available*** here

[12] ***Alert on Enterprise VPN Security,*** U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, March 13, 2020, ***available*** here

[13] ***Alert on COVID-19 Exploited by Malicious Cyber Actors***, U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, and United Kingdom's National Cyber Security Centre, April 8, 2020, ***available*** here

[14] ***Client Alert: U.S. Securities and Exchange Commission Issues Report on Cybersecurity and Resiliency Practices***, Cravath, Swaine & Moore LLP, January 29, 2020, ***available*** here

CRAVATH

Worldwide Plaza
825 Eighth Avenue
New York, NY 10019-7475
+1-212-474-1000 Phone
+1-212-474-3700 Fax

CityPoint
One Ropemaker Street
London EC2Y 9HR England
+44-20-7453-1000 Phone
+44-20-7860-1150 Fax