Debevoise
& Plimpton

The Debrief

# Debevoise Coronavirus Checklists—Cybersecurity

**March 10, 2020**

As companies dust off their Business Continuity Plans to prepare for possible disruptions and remote working due to COVID-19, here are 10 cybersecurity considerations to add to the list of preparations:

- Phishing—Look out for coronavirus phishing scams. We have already seen fake CDC updates, IT alerts and software notices that attempt to obtain user credentials or install malware, so consider implementing coronavirus-specific phishing training or testing. It is also a good idea to redistribute any company policies that cover the use of personal computers, smartphones, tablets and WiFi networks for work and emphasize that (a) those policies still apply to those working from home, and (b) security protocols will not be relaxed absent a clear change in policy.

- More Phishing—Do not send legitimate emails to employees that look like phishing emails, so official COVID-19 updates to employees should have a consistent format and not include links or attachments, which will help employees properly identify phishing emails.

- Remote Capacity—Consider testing the company's remote capacity by having many employees try to login remotely simultaneously, and consider adding or expanding use of secure, web-based video conferencing options.

- Real Time Vulnerability Updates—It will be important to keep on top of new vulnerabilities and scams by subscribing to various threat-sharing groups, including the CISA Alert service, FBI cyber alerts, IT-ISAC and industry threat-sharing groups.

- Help for the Help Desk—Anticipate the additional burden on the IT help desk and make sure those employees have the policies, training and tools they need to handle the increased number of requests for technical assistance from people working from home, including the ability to verify the identity of employees using measures like phone number authentication, challenge questions and two-factor authentication.

- Anticipate Remote Work Problems—Employees who experience difficulties using their home computers (for example, printing) will be tempted to use less secure means to accomplish work tasks, such as emailing confidential documents to their personal email accounts so that they can be easily printed at home. Companies should try to anticipate and solve for these problems ahead of time.

- Essential Employees—Determine how many people, if any, will be needed on-site to protect the network, including patching systems and conducting information security reviews of any new systems that need to be added in haste throughout this period, as well as those needed to conduct investigations and remediation if a cyber event were to occur. Consider backup personnel in case some of those people become unavailable.

- Vendors—Coordinate with the company's key third-party data vendors to make sure that their cybersecurity contingency plans are adequate.

- Update Contact Information—Ensure that contact information is up to date for key employees, especially mobile numbers.

- Protect Medical Information—If employees become ill, there will be good reasons to want to share that information, but it is also important to maintain the confidentiality of employees' medical data as required by law, including the medical status and identities of diagnosed employees or family members of employees.

* * *

Please do not hesitate to contact us with any questions.

**Luke Dembosky**
Partner, Washington, D.C.
+1 202 383 8020
ldembosky@debevoise.com

**Jeremy Feigelson**
Partner, New York
+1 212 909 6230
jfeigelson@debevoise.com

**Avi Gesser**
Partner, New York
+1 212 909 6577
agesser@debevoise.com

**Jim Pastore**
Partner, New York
+212 909 6793
jjpastore@debevoise.com

**Lisa Zornberg**
Partner, New York
+212 909 6945
lzornberg@debevoise.com

**Tricia Bozyk Sherno**
Counsel, New York
+1 212 909 6717
tbsherno@debevoise.com

**Hilary Davidson**
Associate, London
+44 20 7786 5476
hdavidson@debevoise.com

**Christopher S. Ford**
Associate, New York
+ 1 212 909 6881
csford@debevoise.com