JENNER&BLOCK

## Data Privacy and Cybersecurity

# Cybersecurity Concerns with Regard to Work-from-Home Policies


By: David P. Saunders and David Bitkower

The COVID-19 outbreak is causing many companies to consider work-from-home programs for many of their employees. Any arrangement where employees are permitted to work from home poses a unique set of cybersecurity risks and challenges, but those risks are heightened when a majority of the work force are away from offices that are controlled. Ensuring that appropriate technical and administrative safeguards are in place prior to launching wide-scale work-from-home programs is critical to ensuring the safety of your network and data. Below are considerations that businesses should take into account when implementing work from home programs:

### Devices

- Provide all remote user employees with company devices, do not permit Bring Your Own Device (BYOD) for access.
    - Ensure that you have a reliable inventory of who receives what devices.
- If you have to use BYOD, consider having employees sign a proper use policy/renew their agreement to proper use.
    - Consider whether you can add AirWatch or equivalent to personal devices that will be used to access your internal network.
- Ensure continuity of phone message recording and logging for call centers.
    - Have a system that users will have to call or log in to as opposed to using their own devices/phones.

### Network Access

- Access your internal network through VPN.
    - Recommend two factor or multi-factor authentication as well as strong password policy enforcement.
- If VPN is unavailable, encrypted web access is next best option.
    - Again, recommend two factor or multi-factor authentication as well as strong password policy enforcement.
- Consider having a popup upon either VPN or web login that reminds users that the information they are accessing is confidential, belongs to your company, and should not be used for any purpose other than related to their job.
- Ensure that method of connection has strong access controls.
    - Employees should only have access to information based on their needs/position and not open access to data irrelevant to their job functions.

**Confidentiality**

- Ensure that remote users are subject to strong confidentiality agreements.
    - Consider having them renew the agreement before remote usage if one is already in place.
- Retrain/recertify training on cybersecurity before permitting remote access.
    - Consider also sending out a short FAQ or reminder notice to employees as to best practices (e.g., logging out, be aware of shoulder surfing, how to identify phishing, etc…).

**Monitoring**

- Prepare IT to increase monitoring and testing of network.
    - Prepare for increased capacity/monitoring so as to be able to quickly identify and diagnose anomalous user activity.
    - Increase scrutiny of unusual login activity.
    - Consider regular scan of data flows for any leakage.
    - Make sure IT prepared for ransomware/SPAM/Phishing attacks, which there is likely to be an increased risk of given multiple, remote users.
    - Ensure that audit trail for all actions on VPN/web platform is maintained including, but not limited to:
        - Logins
        - Failed login attempts
        - Impossible IP address logins
        - User activity while active
        - Upload/download activity

## Contact Us

**David P. Saunders, Partner, Data Privacy and Cybersecurity**

Chicago | Phone: +1 312 923-8388 | dsaunders@jenner.com

David P. Saunders (CIPP/US) is a member of the firm's Data Privacy and Cybersecurity Practice and Complex Commercial Litigation Practice. Using his training as a litigator, David assists clients as they navigate their risks in the data privacy and cybersecurity arenas. Through this unique lens, David offers both proactive and reactive privacy and cybersecurity counseling to clients.

David counsels Fortune 100 companies and small businesses alike on an array of privacy matters. David works closely with clients to first understand their business and how they use data so that he can better advise them on the myriad of issues that may arise in today's digital world. He has experience conducting risk assessments, developing privacy programs, drafting privacy policies, performing due diligence for corporate transactions, negotiating vendor agreements and working with clients through data incident response. David regularly counsels clients on their HIPAA, HITECH, GLBA, CCPA and state law privacy obligations. Using his litigation experience, David has litigated and negotiated resolution of matters related to data privacy and cybersecurity issues. He has also helped clients navigate potential and actual regulatory investigations.

**David Bitkower, Partner, Data Privacy and Cybersecurity**

Washington, DC | Phone: +1 202 639-6048 | dbitkower@jenner.com

Mr. Bitkower is a member of the firm's Investigations, Compliance and Defense Practice and the firm's Data Privacy and Cybersecurity Practice. He joined the firm after more than a decade as a federal prosecutor. He has led prominent white collar cases, leading clients to turn to him for their most significant and complex matters. Mr. Bitkower's combination of deep experience with high-profile criminal investigations, ability to negotiate the optimal outcome, and familiarity with international environments offers clients the legal sophistication required to help solve their problems. As the former chief of the National Security and Cybercrime Section of the EDNY, Mr. Bitkower has significant experience advising on and understanding issues related to cybercrime, cybersecurity, electronic surveillance and FinTech.

Mr. Bitkower is a former principal deputy assistant attorney general for the Criminal Division of the US Department of Justice (DOJ), the second-highest ranking position in the division. In that role, he managed the division's more than 700 federal prosecutors who conducted nationally significant investigations and prosecutions in cases involving white collar crime, money laundering, public corruption, cybercrime and cryptocurrencies, intellectual property, and organized and transnational crime, among other areas. Together with other senior DOJ leaders, he oversaw the department's most significant investigations and prosecutions of corporate wrongdoing, including financial institution fraud, FCPA violations, sanctions evasion and corporate health-care fraud.