COVID-19: SYSTEM SECURITY WITH A REMOTE WORKFORCE

Date: 26 March 2020

U.S. Intellectual Property Alert

By: Tara C. Clancy, Joseph D. McClendon

COVID-19 has forced many businesses to quickly accommodate a significant portion of their employees working remotely. Having an employee base working away from established offices creates security vulnerabilities that many businesses may not be prepared to mitigate. "Security" as a concept is generally organized under three broad categories that a business must address to have and maintain an effective security program. The three categories of controls — administrative, physical, and technical controls — are the building blocks for every security policy. Utilizing each of them collectively will help you define a straightforward and practical security policy to protect your business' digital assets. Below are some high level ideas to consider as you have more employees working remotely.

ADMINISTRATIVE CONTROLS

The Massachusetts Institute of Technology defines administrative controls as "the human factors of security." In other words, administrative controls refer to the policies, procedures, or guidelines that determine which employees have access to network resources and assets, what level of access those employees have to those network resources and assets, and how to manage security within your business' framework.

Reminders

- Review your current policies regarding working remotely and using personal devices (BYOD or "bring your own device"). If your current policies lack specificity, consider sending guidelines on best practices to your employees to address security.
- Consider implementing information classifications to reduce access to confidential assets. Remote entry points increase your information technology ("IT") security risk footprint. Limiting access to confidential information to only those having a "need to know" helps reduce this footprint and risk.
- Review your procedures on how to contact your employees quickly, in the case of an emergency, including during a security breach. Your response plan needs to include communication methods outside of the computer network should the network become compromised. Update contact lists to take into account your remote workforce.
- Communicate with your employees often to maintain risk awareness. Outside of the normal work environment, an employee's work habits are altered and the normal office rigor may be relaxed. Remind employees about security policies and procedures and the increased risk of phishing attacks. The World Health Organization ("WHO") and the Federal Trade Commission ("FTC") have active websites reporting on trends in scams capitalizing on the COVID-19 pandemic and provide helpful tips:

- WHO: https://www.who.int/about/communications/cyber-security
- FTC: https://www.consumer.ftc.gov/blog/2020/02/coronavirus-scammers-follow-headlines https://www.consumer.ftc.gov/blog/2020/03/ftc-coronavirus-scams-part-2

PHYSICAL CONTROLS

Physical controls describe those tangible practices used to protect unauthorized access to physical areas, systems, or assets. A remote workforce must guard confidential information just as if they are in the office.

Reminders

- Procedures requiring shutting down a computer or closing out programs when they are not in use should still apply at home. Laptops and other mobile devices should not be left unattended in cars or public areas. Work devices should not be used by other family members. Employees should be reminded to be aware of their environment and not work on sensitive information in public areas where their papers or screens may be viewed or their conversations may be heard.
- Remind employees that company information should never be downloaded onto their personal devices or cloud services. Consider disabling drives that enable copying company information to removable media, such as USB devices.
- Institute regular monitoring of your premises and assets. Make sure server rooms and other confidential information repositories are locked and secured from physical access. Where necessary, monitor heating, ventilation, air conditioning, and humidity controls (e.g., in server rooms) to ensure your server rooms and network closets are operating in an optimal environment.

TECHNICAL CONTROLS

Technical controls describe the hardware and software used to protect assets. These controls are typically managed through IT, such as implementing firewalls, antivirus software, intrusion detection, and encryption protocols.

Reminders

- Verify you have, or implement now, "oversight" technologies for additional security, such as:
  - requiring two-factor authentication;
  - using a VPN (Virtual Private Network) and prohibiting access to company systems from public Wi-Fi connections (if a VPN is not possible, identifying how employees can better secure their home network); and
  - requiring security software on employee devices, including anti-virus software and mobile device management software (which permits remote wiping of devices, strong password enforcement, data encryption enforcement, and limitations on software and app installation).
- Additionally, make sure your IT group is available to handle the increased load that corresponds with more employees working from home.

CONCLUSION

Now more than ever, establishing strong company policies and procedures, and communicating those policies and procedures to your employees often is critical to maintaining the security of your company's digital assets. Taking the time now to review all of your security policies to identify any deficiencies and implement best security practices will help keep your business online and running as well as keep your (now) remote employees productive.

KEY CONTACTS

TARA C. CLANCY
PARTNER

BOSTON
+1.617.261.3121
TARA.CLANCY@KLGATES.COM