(Last Updated March 16, 2020)

Cyber Hygiene During COVID-19 Pandemic

In the wake of the COVID-19 pandemic, interim self-isolation and other forms of social distancing are becoming increasingly practiced in order to slow the spread of the underlying novel coronavirus. Numerous organizations have already reacted to the global health emergency by restricting employee travel, closing offices, and implementing remote work protocols. This new work environment presents new opportunities and challenges, especially for employees not accustomed to working from home or other remote locations. A remote workforce is by nature easier for an adversary to impersonate. Maintaining a robust and defensive cybersecurity posture is critical. Kutak Rock urges its clients and other businesses to review and carefully consider the following information security controls.

1. Multi-Factor Authentication

By now most organizations have implemented or at least considered multi-factor authentication. Multi-factor authentication works by requiring a user to present two or more "factors" or credentials:[1] (a) something a user knows (e.g. a password or passphrase); (b) something a user has (e.g. a mobile phone or physical key); (c) something a user is (e.g. a biometric identifier). This control provides an additional layer of protection that thwarts the vast majority of attacks that would otherwise be effective against a password-only approach. Multi-factor authentication has become considerably easier to implement over the last several years due to a wide variety of commercially available tools. Security teams should verify that all critical systems and all access to confidential (including any personal) information is protected by multi-factor authentication. Organizations should always use a second factor, such as a phone call to the requesting party, to verify new or changed payment information.

2. Email Security Policies

Unfortunately, as with any crisis, scammers and other attackers have already begun to exploit the COVID-19 pandemic. Email security filters and other policies can dramatically reduce the quantity and effectiveness of phishing and business email compromise attacks. In each case, attackers imitate a real and, in many cases, known sender in order to steal login credentials, personal information, or valuable business information. Phishing emails typically either deliver malicious payloads designed to infect and exploit vulnerable computer networks and systems or induce the recipient to click a link, provide information, etc. In business email compromise attacks, the attackers typically intercept emails related to financial transactions and attempt to insert themselves into the transaction by changing payment information or other methods. Controls that automatically verify the identity, authenticity, and authority of emails are basic but effective measures to limit unnecessary exposure to these attacks. Organizations can also implement controls that automatically warn their users of potentially suspicious emails that originate outside the organization's domain or match known phishing email patterns. Organizations should take steps to implement those controls and clearly communicate with employees about COVID-19 and their organizational response.

[1] The username or other user identifier is typically not counted as a "factor."

3. "Shadow Information Technology ("IT")" Prevention

Typically, an organization's security and information security teams thoroughly vet, patch, and monitor all hardware and software in their environment. When employees become frustrated by a lack of available technology or their ability to use it, they may sometimes take matters into their own hands. "Shadow IT" is the unauthorized use of IT-related hardware and software, including cloud-based services. The use of Shadow IT creates gaps in security coverage and increases an organization's exposure to preventable risks. In one common example, an employee might set up a cloud-based storage instance in order to more easily share a file with an outside party. Organizations should educate all computer users about current digital capabilities, with a particular focus on establishing remote access to the organization's environment, including through use of a Virtual Private Network ("VPN") if enabled. Organizations should also determine whether to provide employees with alternate means of telephonic communication if they normally rely on infrastructure within their offices for that purpose. If employees require additional software and hardware to function outside of the office environment, organizations should listen and proactively respond to those requests.

4. Suspected or Actual Security Breach Protocol

Organizations should take additional steps to familiarize newly remote employees with their security incident reporting procedures and protocols. The California Consumer Privacy Act ("CCPA") gives some consumers a private right of action against businesses regulated by CCPA that fail to adequately secure personal information during a breach. Organizations should emphasize that security is a collective responsibility, explain the value in rapid reporting, and incentivize employees to report incidents as appropriate. In the event of a suspected or actual breach in security, organizations should immediately contact legal counsel and follow their predetermined breach response plan.

Additional Information

Kutak Rock's Privacy & Data Security team continues to assist organizations ranging from Fortune 100 business to startups protect the privacy and security of their sensitive data across a broad range of industries. We leverage our unique and comprehensive experience to advice clients on a plethora issues including pro-active risk management privacy and security policy development, legal compliance, breach response and recovery, and, when necessary, litigation.

Contacts			
Jon Breyer	Minneapolis	(612) 334-5057	Jon.Breyer@KutakRock.com
Nicole Moriarty	Washington, D.C.	(202) 828-2446	Nicole.Moriarty@KutakRock.com
Todd Kinney	Omaha	(402) 231-8968	Todd.Kinney@KutakRock.com
Jacob Tewes	Omaha	(402) 661-8611	Jacob.Tewes@KutakRock.com

This Client Alert is a publication of Kutak Rock LLP. It is intended to notify our clients and friends of current events and provide general information about privacy and data security issues. This Client Alert is not intended, nor should it be used, as specific legal advice, and it does not create an attorney-client relationship.

This communication could be considered advertising in some jurisdictions. The choice of a lawyer is an important decision and should not be based solely upon advertisements.