ALSTON & BIRD

WWW.ALSTON.COM

CYBER ALERT ■

MARCH 18, 2020

Six Practical Tips for Practicing Cyberhygiene in the Middle of a Global Pandemic

By Kim Peretti, Amy Mushahwar and Jon Knight

Businesses large and small are encouraging (or requiring) employees to work remotely or cancel work travel as part of the response to COVID-19. But suddenly expanding the number of employees working remotely comes with increased cybersecurity and information technology risks. A cybercriminal (including malicious insiders) will have a target-rich environment during this time since more devices will be used for company business and more company data will be sent, located, or stored outside the protections of the company infrastructure and activity logging. It will also be easier for devices to be lost, stolen, or compromised, particularly if employees are not familiar with company policies on how to securely work from home. Information Security and IT teams should consider the following practical tips as they prepare for these risks.

1. Prepare for a Strain on Existing Resources

Increasing the number of remote employees increases the number of people or devices using your remote access resources, such as virtual desktop environments and virtual private networks. Continue to actively monitor these resources to ensure that they are properly updated and resourced (bandwidth, computing power, and storage capacity). This is a unique opportunity to fully test your infrastructure and remote capabilities. Also, companies may want to reevaluate how employees will be authenticated when connecting remotely. Utilizing multifactor authentication should be the goal. The Department of Homeland Security's recent alert on enterprise VPN security may also be a useful resource here.

Consider also expanding your help desk staffing. More employees working from home will likely result in increased calls for IT support since these employees may have connectivity or other technical issues in a remote environment. Similarly, some employees may be forced to use personal devices during this period. It will be important to have help desk staff and software resources available to ensure that antivirus software can be downloaded to personal devices and that the devices are encrypted.

This advisory is published by Alston & Bird LLP to provide a summary of significant developments to our clients and friends. It is intended to be informational and does not constitute legal advice regarding any specific situation. This material may also be considered attorney advertising under court rules of certain jurisdictions.

2. Review and Update Business Continuity, Disaster Recovery, and Incident Response Plans

The coronavirus pandemic is unlikely to directly impact your IT infrastructure. However, it is possible that a severe outbreak will impact the availability of personnel assigned to monitor or use that infrastructure. Companies should review their business continuity and disaster recovery plans (with their related IT and Security roles and responsibilities) to ensure they appropriately cover scenarios that might arise if multiple key personnel are ill or incapacitated. Similarly, if you use Managed Security Service Providers or other security vendors for critical parts of your program, you should verify that those vendors have similar plans, redundancies, and current capacity to help (you may want to verify and secure this help now while we are still in the early stages of this crisis). Ultimately, this is the perfect opportunity to ensure that all key players have recently reviewed these plans, there is necessary expertise redundancy, and staff have engaged in tabletop simulations relating to business continuity.

Companies should also consider conducting a similar assessment for their incident response plans as well as their cyber insurance, crime fraud, technical E&O, or network interruption policies. Such policies or plans may need to be revised to include backup personnel if key personnel such as a CTO, CISO, or privacy officer are incapacitated or otherwise unavailable. Also, you may want to consider cross-training appropriate personnel in all aspects of the incident response, reporting, and claims process, including the location of core documents and notice templates that would be used in an incident. If you have not already, consider what key elements of your incident response plan could be reduced to a diagrammed flow for your team to have in front of them in a crisis.

3. Warn Employees of the Security Risks of Working from Home

In times of crisis, increased work, or nonstandard work routines, personnel are more likely to forget to use recommended cybersecurity practices, but warning them now may help with security awareness during unfamiliar times. This will be particularly true for mission-critical services since employees may feel pressure to forgo security to get work done. All employees should be reminded of the corporate resources that are available, such as cloud storage or other applications, the need for increased vigilance, and the following basic security principles:

- Secure home wireless networks with strong passwords and avoid using unsecured public networks when possible. If using an unsecured public network, be on the lookout for any certificate errors or warnings that a site may be misconfigured.

- Do not use personal devices for work without prior approval because these may lack the security controls that protect work devices.

- Do not use personal email or cloud storage accounts to transfer or store business information.

- Avoid downloading or printing sensitive information from email or other IT services to personal computers or other personal devices even if authorized to use the device for work purposes. If you must download data to personal devices, confirm with IT help desk staff that antivirus software is installed on your device and that it is properly encrypted.

- Practice good physical document management by only taking documents offsite if necessary and ensuring all materials are returned to the office for proper destruction.

4. Be Wary of Scams and Phishing Attacks

Scammers and cyber threat actors have always followed the headlines, using the public's heightened fear and desire for information or solutions as leverage to gain access to systems, data, and money. The current pandemic is no different. There are reports of schemes where malicious actors are stealing credentials from remote workers by supposedly offering updated company guidance on the COVID-19 response. And cyber researchers recently discovered a website of a map showing COVID-19 cases on a global scale that contained a hidden code that could steal usernames, passwords, credit card numbers, and other data stored in the user's browser. While the Food and Drug Administration (FDA) and Federal Trade Commission (FTC) are working to crack down on phony COVID-19 cures and requests for "donations" from fake charities, employees must be on the lookout for scams and phishing attacks. All employees should be reminded of the following recommended practices:

- Be careful opening attachments and links from distrusted or unknown sources. Phishing or other malicious emails can easily be disguised as alerts about COVID-19.
- Try to use only trusted sources, for example, the CDC's official COVID-19 website, for receiving up-to-date information about the outbreak.
- Never respond to emails or phone calls asking for personal or financial information, usernames, or passwords.
- Be careful making donations and reject any request for donations in cash, by gift card, or by wiring money.

This is also an excellent opportunity to remind employees of how to report security incidents within the company. Consider creating a short checklist for all employees detailing tips for how to detect suspicious activity, and what to do and who to contact if they believe they have been the victim of a security incident, scam, or phishing attack.

Additional resources from the FTC and U.S. Office of Personnel Management on working remotely and how to avoid scams and phishing attacks can be found here and here.

5. Be Aware of Applicable Industry-Specific Guidelines

Some heavily regulated industries (e.g., banking, financial services, and health) will have additional considerations at play. For example, FINRA has just released guidance that addressed telework arrangements with a section specifically related to cybersecurity risks posed by those arrangements. Additional commentary on this guidance can be found here. Similarly, HIPAA covered entities and business associates may face an increased risk of violating the HIPAA Privacy and Security rules. Best practices on how to address these risks and other HIPAA-specific guidance can be found here.

6. If Security Exceptions Must Occur Temporarily, Take Steps to Document Them

Your company may have no choice but to make security exceptions to get work done, especially if your industry is on the front lines of this crisis (e.g., health care and necessities supply chains). If this is the case, take steps to ensure that Security and IT document any security exceptions made so the company can resume its full security measures once volumes return to normal. If security exceptions are not documented, there is the potential for these items to be forgotten once the crisis passes.

Alston & Bird has formed a multidisciplinary task force to advise clients on the business and legal implications of the coronavirus (COVID-19). You can view all our work on the coronavirus across industries and subscribe to our future webinars and advisories.

Cybersecurity Preparedness & Response Team Co-Chairs

Kimberly Kiefer Peretti | 202.239.3720 | kimberly.peretti@alston.com
Jim Harvey | 404.881.7328 | jim.harvey@alston.com

Follow us: @AlstonPrivacy | www.AlstonPrivacy.com

www.alstonsecurity.com

ALSTON & BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ▪ 1201 West Peachtree Street ▪ Atlanta, Georgia, USA, 30309-3424 ▪ 404.881.7000 ▪ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ▪ Suite 21B2 ▪ No. 7 Guanghua Road ▪ Chaoyang District ▪ Beijing, 100004 CN ▪ +86 10 8592 7500
BRUSSELS: Level 20 Bastion Tower ▪ Place du Champ de Mars ▪ B-1050 Brussels, BE ▪ +32 2 550 3700 ▪ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ▪ 101 South Tryon Street ▪ Suite 4000 ▪ Charlotte, North Carolina, USA, 28280-4000 ▪ 704.444.1000 ▪ Fax: 704.444.1111
DALLAS: Chase Tower ▪ 2200 Ross Avenue ▪ Suite 2300 ▪ Dallas, TX 75201 ▪ 214.922.3400 ▪ Fax: 214.922.3899
LONDON: 5th Floor, Octagon Point, St. Paul's ▪ 5 Cheapside ▪ London, EC2V 6AA, UK ▪ +44.0.20.3823.2225
LOS ANGELES: 333 South Hope Street ▪ 16th Floor ▪ Los Angeles, California, USA, 90071-3004 ▪ 213.576.1000 ▪ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ▪ 15th Floor ▪ New York, New York, USA, 10016-1387 ▪ 212.210.9400 ▪ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ▪ Suite 600 ▪ Raleigh, North Carolina, USA, 27601-3034 ▪ 919.862.2200 ▪ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ▪ Suite 2100 ▪ San Francisco, California, USA, 94105-0912 ▪ 415.243.1000 ▪ Fax: 415.243.1001
SILICON VALLEY: 950 Page Mill Road ▪ Palo Alto, California USA, 94304-1012 ▪ 650.838.2000 ▪ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ▪ 950 F Street, NW ▪ Washington, DC, USA, 20004-1404 ▪ 202.239.3300 ▪ Fax: 202.239.3333