ALSTON & BIRD

WWW.ALSTON.COM

CYBER ALERT ■

AUGUST 13, 2020

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

By Kim Peretti, Amy Mushahwar, and Jon Knight

More than five months have passed since the COVID-19 pandemic began sweeping through the United States, resulting in stay-at-home orders and the large-scale, sudden transition to remote work environments for many businesses. The cybersecurity risks raised by this transition are already well documented. For example, the United States and United Kingdom jointly warned that threat actors were taking advantage of vulnerabilities in common brands for remote work platforms such as Citrix, Pulse Secure, Fortinet, and Palo Alto; Interpol warned of increased cybersecurity threats due to COVID-19; and the FBI warned of increases in business email compromise, state-sponsored cyberattacks, and fraud due to the COVID-19 pandemic.

State and local governments have now been in various stages of relaxing pandemic-related restrictions. But not all employees can or should return to the office at this time, and spikes in cases have some areas reinstituting more significant restrictions or pausing reopening efforts. Remote work environments will need to remain operational, scalable, and capable of flexing with cycles of virus resurgence. Information security, IT, and business management teams should consider the following practical tips as they address this new reality.

Consider Basic Cyberhygiene

As personnel become more comfortable with working from anywhere, they are more likely to let their guard down and forget to use recommended cybersecurity practices. Consider providing periodic reminders 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 or that indicate a spoofed connection.
- 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 taking documents offsite only if necessary and ensuring all materials are destroyed with a cross-cut shredder or returned to the office for proper destruction.

Identify Security Blind Spots

While a long-term, work-from-home environment presents many significant cybersecurity challenges, identifying potential security blind spots should be a strong focus. First, while the network perimeter was already changing, the sudden shift to remote working accelerated the pace of this change. Instead of the old model of a defined perimeter, the network perimeter now needs the flexibility to expand and contract as health restrictions scale to the virus cycles. At a minimum, it will cover homes, apartments, and other remote locations where enterprise information security teams have not traditionally had visibility. So instead of residing behind the traditional firewalled security moat, businesses are faced with a permeable perimeter while bad actors have shifted to cyber guerilla warfare. Second, the workforce is changing. While some businesses may be expanding their workforce to accommodate new demand for services, others are facing furloughs or layoffs. If a remote-working employee is let go, a business may not have the same visibility into potential data loss when that employee is terminated as it had under the traditional network model.

With these challenges in mind, here are 10 questions that can help legal, information security, and other relevant business teams identify potential security blind spots.

1. Has the business identified all the new endpoints, the type of network used by those endpoints, and confirmed its ability to monitor the new endpoints?
2. Are any endpoints personal devices and, if so, is monitoring tailored to reduce any privacy concerns associated with monitoring personal devices?
3. How are remote connection capabilities routed and resourced?
4. Is IT making greater use of cloud resources?
5. Do existing security tools such as firewalls and proxies adequately inspect remote work paths, including cloud resources?
6. Does the business lose visibility on potential endpoint vulnerabilities through using a split-tunnel virtual private network (VPN)?
7. Is the business logging and reviewing the right data for the expanded network perimeter? For example, consider:
    - Does it have the ability to collect logs from all expanded endpoints?
    - If the business uses a security information and event management (SIEM) system, is it tuned to account for new traffic flows or the remote workforce?

8. Can teams address alerts in a timely manner? For example:
   - Is there staffing or a managed services contract to sufficiently monitor alerts?
   - Do teams revisit alerts or automated reviews for the new network perimeter to ensure that alerting is appropriate?
9. Does the business manage or limit network access for furloughed workers?
10. If a remote-working employee is let go, how will the business protect against data loss or an insider threat from that former employee?

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

The coronavirus pandemic has been unlikely to directly impact a company's IT systems. However, it is possible that a severe resurgence will impact the availability of personnel assigned to monitor or use those systems. 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 a company uses managed security service providers or other security vendors for critical parts of its information security program, it should verify that those vendors have similar plans, redundancies, and current capacity to help. 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, crime fraud, technology errors and omissions, or network-interruption insurance policies. These policies or plans may need to be revised to include backup personnel if key personnel such as a chief technology officer, chief information security officer, or privacy officer are incapacitated or otherwise unavailable. Also, businesses 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. It may also be time to consider what key elements of an incident response plan could be reduced to a diagrammed flow for teams to have in front of them in a crisis.

Remain Vigilant for Scams and Phishing Attacks

Scammers and cyberthreat 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. Threat actors are stealing credentials by spoofing email addresses for corporate IT help desks and sending links to fake Office 365 sites. A recently published report found that about 13 percent of all phishing attacks in Q1 2020 related to COVID-19, and this number is only likely to grow. 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 and potential treatments.
- 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 whom 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.

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, the Financial Industry Regulatory Authority (FINRA) has shared best practices for financial firms that have transitioned to remote work environments and the cybersecurity considerations for these environments. Similarly, the U.S. Securities and Exchange Commission (SEC) has issued guidance on the disclosures companies should consider regarding business disruption due to COVID-19. It encourages companies to internally evaluate several questions, including whether the remote work arrangements have adversely affected the ability to maintain operations, including financial reporting systems, internal control over financial reporting, and disclosure controls and procedures. And the New York Department of Financial Services reminded all its regulated entities that COVID-19 is not a free pass for privacy and security compliance. It specifically notes that the remote-working environment causes heightened cybersecurity risks in seven key areas: (1) maintaining secure connections for remote workers; (2) properly securing company-issued devices; (3) expanding bring your own device (BYOD) policies; (4) securing methods of remote work communications; (5) preventing data loss; (6) guarding against increased phishing and fraud; and (7) managing risks stemming from third-party vendors. This regulatory guidance emphasizes how businesses must remain alert to any guidance specific to their fields for remote work environments.

Revisit Risk Exceptions

It is likely that companies will have had no choice but to make risk exceptions to get work done while rolling out a more robust work-from-home environment. Consider taking the time now to review the risk-exception process. While doing this, remember that risk exceptions come from all aspects of your business. Software development, product development, daily IT management, HR, and finance/operations have all been impacted by increased remote work and may need to be reviewed for risk exceptions. If companies find exceptions that still need to be documented and approved, then prioritize the risks and build a plan to address them. Should a regulator or auditor take interest, it is important that businesses be able to show proactive steps that have already been taken to address the exceptions and plan for remediation.

It may also be the case that a long-term remote work environment means internal policies need to be modified. In other words, the exception may need to become the standard. If so, take care to involve all relevant stakeholders and follow good change-management procedure to document the necessary policy changes.

Alston & Bird has formed a multidisciplinary response and relief team 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