Author: **Sarah Spurlock**
Stites & Harbison, PLLC

Title: **Help! They've Hijacked our Network and They Want Money – Now What? Strategies for Managing the Cyber-Attack**

Session: **IADC Annual Meeting 2021**

"No company is safe." White House urges private sector action to harden defenses against growing ransomware threat.

Following a slew of high-profile ransomware attacks, the White House deputy national security adviser for cyber and emerging technology, Anne Neuberger, issued an open letter[1] to the private sector on June 2, 2021 urging action to increase cyber defenses to match the nation's increasing ransomware threat. The letter to corporate executives and business leaders outlines a number of practices businesses can implement to drive down risk, warning that "[a]ll organizations must recognize that no company is safe from being targeted by ransomware, regardless of size or location."

Neuberger's June 2nd letter is one of a number of recent actions underscoring the Biden Administration's view that cybersecurity risks in both the private and public sector present threats to U.S. national and economic security. Neuberger's letter followed on the heels of President Biden's May 12, 2021 Executive Order on Improving the Nation's Cybersecurity[2] announcing that the "prevention, detection, assessment, and remediation of cyber incidents" is a top priority. In an effort to lead by example, the Executive Order states that "[a]ll Federal Information Systems should meet or exceed the standards and requirements for cybersecurity set forth and issued pursuant to this order."

Neuberger's letter urges the private sector to implement "five best practices" currently being implemented across the Federal Government to reduce the risk of a cyber-attack:

1) Use of multifactor authentication;
2) Endpoint detection and response;
3) Encryption;
4) A skilled security team; and
5) Sharing and incorporating threat information into your defenses.

In addition to implementing the practices above, Neuberger's letter urges businesses to take the following actions:

- Backup your data, system images, and configurations, regularly test them, and keep the backups offline;
- Update and patch systems promptly;
- Test your incident response plan;
- Use a third-party pen tester to check your security team's work; and
- Segment your networks.

Given the increasing frequency and sophistication of cyber-attacks, it is prudent for companies to assess (or reassess) the risk of a ransomware attack, develop an action plan to mitigate that risk, and plan for an incident in case an attack occurs. A ransomware response plan should include steps to seek professional assistance. Victims should not go it alone. There are many benefits to

[1] Anne Neuberger's June 2, 2021 open letter is attached as Attachment A.
[2] President Biden's May 12, 2021 Executive Order is attached as Attachment B.

seeking professional help, including gaining information on the type of ransomware infection at issue and obtaining assistance in identifying your attacker to better direct your response efforts. Paying a ransom without due consideration of the specific circumstances of your attack can leave you vulnerable to future attacks and may lead to additional legal woes. In October 2020, the Office of Foreign Asset Controls (OFAC) issued guidance that any company paying a ransom to a criminal threat actor that is a sanctioned entity or that operates in a sanctioned jurisdiction, and any entities that facilitate such payment (including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response) may face penalties for violations of OFAC regulations.[3] The OFAC warning increases the risk of making a ransom payment and necessitates due diligence into where your payment may be going.

Working with professionals, including breach counsel, experienced cyber professionals, and ransomware negotiators, can not only improve your response and ability to recover from an attack, but can also help you navigate the increasingly complex process of paying a ransom if no viable alternatives exist and assess whether you have legal data breach reporting obligations stemming from the attack. Additional resources on ransomware prevention and response are available at https://www.cisa.gov/ransomware. Among these resources is the Cybersecurity & Infrastructure Security Agency's September 2020 Ransomware Guide including a Ransomware Prevention Best Practices and Ransomware Response Checklist.

[3] The Office of Foreign Asset Controls October 2020 guidance is available at https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf (Last visited July 9, 2021).