Best Practices for Protecting and Responding to Cybersecurity Threats

Updated: 10/30/20

Cybersecurity incidents and threats to the U.S. healthcare system technology infrastructure have never been higher. With that in mind, it is crucial for providers to act now – as early before an incident as possible – to protect themselves from emergent threats and bad actors actively working to compromise and gain access to healthcare infrastructure.

The Department of Homeland Security (DHS) Cybersecurity and Infrastructure & Security Agency (CISA) recommends the following steps to fortify your systems from attack, including:

- Patch operating systems, software, and firmware as soon as manufacturers release updates.
- Check configurations for every operating system version for Healthcare and Public Health (HPH) organization-owned assets to prevent issues from arising that local users are unable to fix due to having local administration disabled.
- Regularly change passwords to network systems and accounts and avoid reusing passwords for different accounts.
- Use multi-factor authentication where possible.
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.
- Implement application and remote access allow listings to only allow systems to execute programs known and permitted by the established security policy.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Audit logs to ensure new accounts are legitimate.
- Scan for open or listening ports and mediate those that are not needed.
- Identify critical assets such as patient database servers, medical records, and telehealth and telework infrastructure; create backups of these systems and house the backups offline from the network.
- Implement network segmentation. Sensitive data should not reside on the same server and network segment as the email environment.
- Set antivirus and anti-malware solutions to automatically update; conduct regular scans

Additional steps you should consider to secure your system:

- Utilize email protection to hamper phishing.
- Utilize an endpoint detection and response (EDR) agent on all managed systems to hamper attempts to gain persistence.
- Block personal browsing network traffic at your gateway, or virtualize it to hamper phishing via social media and personal email.
- Implement remote desktop (RDP) gateways and block peer-to-peer RDP with network tools to hamper adversary lateral movement.
- Stand up an out-of-band communication system with a cloud collab tool, configure it for mandatory two-factor authentication (2FA), and enroll your security, IT and business leaders in advance to facilitate continuity of communications during an emergency.

If you are a victim of a cyberattack or you witness suspicious activity you are recommended to contact the authorities immediately.

- Contact FBI 24/7 Cyber Watch (CyWatch): +1 (855) 292-3937 or by e-mail at CyWatch@fbi.gov.
- Contact your local FBI field office at www.fbi.gov/contact-us/field.
- Contact the CISA at Central@cisa.dhs.gov to report a threat or request incident response resources or technical assistance related to cyber threats.
- Utilize the CISA Information Reporting System https://uscert.cisa.gov/forms/report.
- Contact the FDA to report medical device problems at https://www.fda.gov/medical-devices/medical-device-safety/medical-device-reporting-mdr-how-report-medical-device-problems or Cybermed@fda.hhs.gov

Additional Resources:

- List of Free Federal Government Resources: https://chimecentral.org/wp-content/uploads/2014/10/Cyber-Resources-V3.pdf
- CISA Resources for Businesses: https://us-cert.cisa.gov/resources/business
- CISA Service Catalog: https://www.cisa.gov/publication/cisa-services-catalog
- HHS Critical Infrastructure Protection (CIP): https://www.phe.gov/preparedness/planning/cip/Pages/default.aspx