ASPR TRACIE Technical Assistance Request

Request Receipt Date (by ASPR TRACIE): 24 July 2019
Response Date: 25 July 2019
Type of TA Request: Standard

Request:

The requestor asked ASPR TRACIE and ASPR staff from multiple departments for technical assistance in identifying checklists that healthcare facilities can use once they have been faced with a cyberattack.

Response:

The ASPR TRACIE Team reviewed our existing Cybersecurity Topic Collection and conducted a search online for relevant materials. We synthesized what we and other ASPR staff located; all materials are included in this document.

Section I in this document includes feedback from ASPR TRACIE Subject Matter Expert (SME) cadre members. Section II provides checklists that healthcare facilities can use if they are faced with a cybersecurity attack. Finally, Section III includes additional relevant materials that may be helpful to this request.

I. ASPR TRACIE SME Cadre Member Comments

Please note: These are direct quotes or paraphrased comments from emails and other correspondence provided by an ASPR TRACIE SME Cadre member in response to this specific request. They do not necessarily express the views of ASPR or ASPR TRACIE.

SME Cadre Member 1:

- If the entity believes that they are under attack or have been attacked, they should contact HC3 SOC which has been specifically put in place to provide assistance: **HC3@hhs.gov**.
- HC3 is setup to support the health sector, including the private and public sector and not HHS internal.
- The HC3 team will also be able to provide general guidance and help.

II. Cybersecurity Checklists for Healthcare Facilities

American Health Information Management Association. (2008). Data Breach Investigation and Mitigation Checklist. Journal of AHIMA. (**NOTE**: some users may need to copy and paste the URLs into their browsers to access the checklist and form.)

This checklist can be used by healthcare facilities to determine the actions that need to be taken immediately upon identification of an incident, and follow-up activities. It can also be used in conjunction with the sample security incident response report form.

Healthcare and Public Health Sector Coordinating Councils. (2014). Protecting the Digital Infrastructure: Cybersecurity Checklist.

This short (introductory) checklist can help healthcare providers protect their digital infrastructure.

New York-Presbyterian Hospital. (n.d.). Information Security Incident Procedure. (Accessed 7/25/2019).

This hospital policy document provides the steps for responding to a suspected or known information security incident.

U.S. Department of Health and Human Services, and Healthcare & Public Health Sector Coordinating Councils. (2018). Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients.

This guidance document: provides an overview of the current cybersecurity threats faced by the healthcare and public health (HPH) sector; highlights challenges and weaknesses that increase HPH organizational vulnerability; and shares promising practices ranked by cybersecurity experts as the most effective to mitigate the threats. **NOTE**: Additional technical volumes, resources and templates can be found on the following link: https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx

U.S. Department of Health and Human Services, Office for Civil Rights. (2017). My Entity Just Experienced a Cyber-Attack! What Do We Do Now? A Quick-Response Checklist from the HHS, Office for Civil Rights (OCR).

This checklist provides information on what a healthcare facility should do in the event of a cyberattack, and who to report specific information to.

III. Additional Relevant Resources

Healthcare and Public Health Sector Cybersecurity Working Group. (2013). Healthcare and Public Health Cybersecurity Primer: Cybersecurity 101.

This primer can help healthcare providers learn more about the basics of cybersecurity, common vulnerabilities and threats, and how to manage risk. Also included is a matrix of threats with consequences that can be helpful to administrators.

Joint HPH Cybersecurity Working Group. (2016). Healthcare Sector Cybersecurity Framework Implementation Guide.

This guide was developed in consultation with the Healthcare and Public Health (HPH) Sector Coordinating Council and Government Coordinating Council, along with input from other sector members and the U.S. Department of Homeland Security Critical Infrastructure Cyber Community. The goal of the guide is to help HPH Sector organizations understand and use the HITRUST Risk Management Framework—consisting of the HITRUST CSF, CSF Assurance Program, and supporting

methodologies—to implement the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity in the HPH Sector and meet its objectives for critical infrastructure protection.

Rossi, B. (2015). 6 Critical Steps for Responding to a Cyber Attack. Information Age.

The author of this article identifies six steps that a healthcare facility should take if their organization is faced with a cyberattack.

U.S. Department of Health and Human Services, Office of the Assistant Secretary for Preparedness and Response. (2018). Healthcare and Public Health (HPH) Risk Identification and Site Criticality (RISC) Toolkit.

This objective, data-driven all hazards risk assessment can be used to inform emergency preparedness planning and risk management activities. The toolkit consists of three self-assessment modules allowing healthcare facilities to: identify site-specific threats and hazards; assess site-specific vulnerabilities; and evaluate criticality and consequences. (A related webinar explains the toolkit in more detail: https://files.asprtracie.hhs.gov/documents/aspr-risc-toolkit-webinar-slides-final-508.pdf.)

U.S. Department of Health and Human Services, Office for Civil Rights. (2016). HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework.

This document maps paths between two seminal healthcare cybersecurity documents. It can help healthcare planners use the Cybersecurity Framework as a "common language" and identify gaps to boost compliance with the Security Rule.

U.S. Department of Homeland Security. (n.d.). Assessments: Cyber Resilience Review (CRR). (Accessed 7/25/2019.)

This website explains the (free) cyber resilience review process and lists benefits and variables measured. It also explains the cyber security evaluation tool and its benefits. Important links for getting started and requesting reviews are also included.

United States Computer Emergency Readiness Team. (2016). The National Cyber Incident Response Plan (NCIRP).

This plan applies to significant cyber incidents that have the potential to cause significant harm to national security interests, foreign relations, economy, or public health and safety. Sections include Roles and Responsibilities; Core Capabilities; and Coordinating Structures and Integration. Additional guidance is provided in the appendices.

Valderrama, A., Lee, S., Batts, D., et al. (2016). Healthcare Organization and Hospital Discussion Guide For Cybersecurity. Centers for Disease Control and Prevention.

Healthcare facility staff can use this document--presented as a discussion-based exercise--to identify their cybersecurity challenges, needs, and strengths.