ASPR TRACIE Technical Assistance Request

Requestor:
Requestor Phone:
Requestor Email:
Request Receipt Date: 31 August 2016
Response Date: 1 September 2016
Type of TA Request: Standard

Request:

The requestor is requesting cybersecurity/ cyberattack prevention plans or templates for hospitals. She is requesting on behalf of a hospital system that was recently hit by ransomware.

Response:

The ASPR TRACIE team was unable to find publically available facility plans for how to prevent and/or respond to cybersecurity threats, likely due to the security issues it may pose for the facilities. However, the resources below include sample plan templates, guidance documents, and lessons learned that may be helpful in developing a cybersecurity/ cyberattack prevention plan. Please see the ASPR TRACIE Cybersecurity Topic Collection for additional resources.

Additionally, Craig DeAtley (Director for the Institute for Public Health Emergency Readiness at MedStar Washington Hospital Center), has offered to talk with the facility directly to provide his lessons learned and recommendations for planning and response to an attack, based on a cyberattack that occurred in his facility in March 2016. He also shared his experiences in Issue 2 of the ASPR TRACIE newsletter, *The Exchange*, and during a roundtable discussion as noted below.

The ASPR TRACIE team recently released the following general resources discussing cybersecurity and healthcare:

- ASPR TRACIE Cybersecurity and Healthcare Facilities Roundtable with speakers from the public and private sectors.
- ASPR TRACIE newsletter dedicated to cybersecurity issues featuring articles from Craig DeAtley (describes the cybersecurity attack on MedStar Health System), the American Hospital Association (overview of the cyber hygiene efforts underway in hospitals across the US), Food and Drug Administration (overview of the risks and highlights pre and postmarket manufacturer guidance), and CMS (overview of the Health Care Industry Task Force established to support the Cybersecurity Act of 2015).
- Cybersecurity Topic Collection includes annotated resources reviewed and approved by a variety of subject matter experts.

I. Sample Plan Templates and Procedures

California Department of Technology. (n.d.). Sample Intrusion Detection Incident Response Plan.

This template provides considerations for writing an intrusion detection incident response plan. It is general in scope but can be adapted for use by hospitals/ healthcare organizations.

DeVoe, C., Rahman, S. (2013). Incident Response Plan for a Small to Medium Sized Hospital. International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.2.

This article provides recommendations for how to develop a Computer Incident Response Team (CIRT) using the traditional Incident Command System model. It also provides example tools and trainings that the CIRT will need.

New York-Presbyterian Hospital. (n.d.). Information Security Incident Procedure.

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

University of Tennessee Health Science Center. (2010). Computer Security Incident Response Procedures.

Though not specific to a healthcare facility, this plan provides recommendations for how to set up an incident response team, roles/responsibilities, and notification steps.

II. Guidance/ Tools

American Hospital Association. (2014). Cybersecurity and Hospitals: What Hospital Trustees Need to Know About Managing Cybersecurity Risk and Response.

This document is geared towards helping hospital trustees better understand the hospital's plan for managing cybersecurity risk. For example: what the cybersecurity plan for the facility is, who is accountable for developing and implementing the plan, and if there is appropriate board oversight over the plan. It also includes a sample list of questions that the directors or trustees can ask.

American Health Information Management Association. (2008). Data Breach Investigation and Mitigation Checklist. Journal of AHIMA.

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

Centers for Disease Control and Prevention. (2016). Healthcare Organization and Hospital Discussion Guide for Cybersecurity.

This guide can help those whose job responsibilities include healthcare cybersecurity preparedness and response planning develop and conduct discussion-based exercises. It includes scenarios and discussion questions specific to response capabilities, communications, and information sharing.

Dietrich, T. and Schuler, K. (2016). The Business Case for Information Governance in Healthcare. BDO.

The authors explain the need for information governance programs in healthcare, and highlight the associated benefits (e.g., improved quality of care, increased operational effectiveness, reduced cost and risk).

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.

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.

Health Information Trust Alliance. (2014). Healthcare's Model Approach to Critical Infrastructure Cybersecurity.

This white paper provides an overview of cybersecurity, including how it is being addressed in the healthcare enterprise, and the key elements of a cybersecurity program. Also included is a highly detailed mapping of how healthcare can implement the NIST Cybersecurity Framework, and how to best use threat intelligence.

IAPP. (2016). Security Breach Response Plan Toolkit.

This toolkit can help healthcare facility cybersecurity planners create a security breach response plan and lower the risk of a breach that could compromise patient health and the reputation of the facility.

Independent Security Evaluators. (2016). Securing Hospitals: A Research Study and Blueprint.

The authors describe research conducted on a variety of hospital and healthcare-related infrastructures and systems; identify industry-specific challenges; and create a blueprint for improving healthcare facility security.

Johnson, C., Badger, L., and Waltermire, D., et al. (2014). Guide to Cyber Threat Information Sharing (Second Draft). (NIST SP 800-150.) National Institute of Standards and Technology, U.S. Department of Commerce.

This publication can help cyber professionals in the healthcare system establish and participate in cyber threat information sharing relationships. It contains information on developing information sharing goals, identifying threat sources, engaging with existing information sharing communities, and effectively using threat information, which can help health systems share threat information in a structured fashion.

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.

National Institute of Standards and Technology. (2015). National Cybersecurity Workforce Framework.

The National Cybersecurity Workforce Framework was developed to provide employers, staff, training providers, and participants with a common set of skills and tasks (based on common language) to define and perform cybersecurity work. This webpage includes links to various framework materials which feature with tasks and skills tied to job categories.

United States Computer Emergency Readiness Team. (n.d.). Resources for Business. (Accessed 6/10/2016.) U.S. Department of Homeland Security.

This webpage (known by the acronym US-CERT) features links to cybersecurity resources for businesses (e.g., healthcare facilities) grouped into the following categories: Resources to Identify, Resources to Protect, Resources to Detect, and Resources to Recover.

U.S. Department of Energy. (2014). Cybersecurity Capability Maturity Model (C2M2).

The C2M2 model can help healthcare facilities evaluate their cybersecurity capabilities. Sections of this document are geared towards decision makers, leaders/managers, practitioners, and facilitators.

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.). Cyber Resilience Review & Cyber Security Evaluation Tool. (Accessed 6/10/2016.)

This factsheet 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.

III. Ransomware Resources

Callahan, M. (2016). What Hospitals Need to Know about Ransomware. American Hospital Association.

The author provides a brief introduction and overview of ransomware, how it can be used to infect mobile and desktop devices, and the importance of security and regularly backing up patient and facility data.

Shaghaghi, S. and Pilch, P. (2016). HIT Think Ransomware: What Providers Should do now. Health Data Management. (Registration required to access entire article.)

The authors discuss steps facilities can take to prevent and mitigate the effects of a ransomware attack.

Shaghaghi, S. and Pilch, P. (2016). Preparing For and Responding To Hospital Ransomware Attacks. BDO.

The authors illustrate the actual and projected rise of ransomware attacks on all industries, and share related preparedness and response strategies for healthcare facilities.

United States Computer Emergency Readiness Team. (2016). Ransomware and Recent Variants. U.S. Department of Homeland Security.

This factsheet provides an overview of ransomware and shares how the variants Locky and Samas were recently used to compromise healthcare networks.

Zetter, K. (2016). Why Hospitals are the Perfect Targets for Ransomware. Wired.

According to the author, hospitals make "good" targets because delays in paying ransom could result in the death of a patient or lawsuit. Lack of staff training on cybersecurity awareness was another reason experts listed.

IV. Articles/ Other Resources

Koppel, R., Smith, S., Blythe, J., and Kothari, V. (2015). Workarounds to Computer Access in Healthcare Organizations: You Want my Password or a Dead Patient? (Abstract only.) Studies in Health Technology and Informatics. 208: 215-220.

The authors examine the methods some healthcare providers use to circumvent cybersecurity. These "creative, flexible, and motivated" employees did not have criminal intention—they were presumably focused on providing patient care in a fast-paced environment.

Pilch, P. and Shaghaghi, S. (2016). Cybercrime: How the Healthcare Sector Can Protect Itself. (Registration required to access entire article.) Private Healthcare Investor.

The authors provide an overview of the cyber threat to the healthcare industry and tips for guarding against future attacks.

Perakslis, E.D. and Stanley, M. (2016). A Cybersecurity Primer for Translational Research, Science Translational Medicine. Science Translational Medicine. 8(322): 2.

The authors discuss recent healthcare-related data breaches and how they could have been prevented. They also highlight the differences between compliance and security (and how they overlap)—particularly in the research arena—and share tips for improving cybersecurity.

Quick, B. (2016). Breach Control: Best Practices in Health Care Application Security.

The author examines the threat landscape for patient medical devices and personal mobile devices and discusses best practices in application security and the software development lifecycle.

US Department of Homeland Security. (2012). Cyber Tabletop Exercise for the Healthcare Industry Situation Manual.

This SitMan template can be adapted for use by healthcare facilities seeking to validate their detection, response actions, and processes to information security threats and vulnerabilities through an HSEEP compliant table top exercise. This SitMan includes four types of vignettes/ scenarios: compromise of electronic protected health information data, corrupted electronic health records, billing system disruption, and medical device malfunction.