TRACIE

HEALTHCARE EMERGENCY PREPAREDNESS
INFORMATION GATEWAY

Cybersecurity Topic Collection

1/6/2017

ASPR
ASSISTANT SECRETARY FOR
PREPAREDNESS AND RESPONSE

Topic Collection: Cybersecurity

Recent cyberattacks on healthcare facilities have had significant effects on every aspect of patient care and organizational continuity. They highlight the need for healthcare organizations of all sizes and types to implement cybersecurity best practices and conduct robust planning and exercising for cyber incident response and consequence management. As the number of cyberattacks on this sector increases, healthcare practitioners, facility executives, information technology professionals, and emergency managers must remain current on the ever-changing nature and type of threats to their facilities, systems, patients, and staff. The resources in this Topic Collection can help stakeholders better protect against, mitigate, respond to, and recover from cyber threats, ensuring patient safety and operational continuity.

Each resource in this Topic Collection is placed into one or more of the following categories (click on the category name to be taken directly to that set of resources). Resources marked with an asterisk (*) appear in more than one category.

Must Reads

Cybersecurity Unit. (2015). Best Practices for Victim Response and Reporting of Cyber Incidents. U.S. Department of Justice.

This document provides planning and response guidance based on lessons learned by federal prosecutors while handling cyber investigations and prosecutions. The authors drafted the document with smaller organizations (with fewer resources) in mind, but larger organizations should also find it useful.

Filkins, B. (2014). Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon. SANS Institute.

The project team analyzed a year's worth of healthcare intelligence data and provide an overview of the sector's vulnerabilities (including the "Internet of Things" and challenges related to compliance). The author shares three case studies that demonstrate traffic and how healthcare networks were attacked and concludes with preparedness tips useful to both information technology professionals and emergency planners.

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.

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.

National Institute of Standards and Technology. (2014). Framework for Improving Critical Infrastructure Cybersecurity. (V. 1.0).

This document provides a detailed framework to protect critical infrastructure and a set of activities to achieve specific cybersecurity outcomes. The Core Functions include: Identify, Protect, Detect, Respond, and Recover, and Section 3 of the guide includes examples of how the framework can be employed when creating a cybersecurity program.

Perakslis, E.D. and Stanley, M. (2016). A Cybersecurity Primer for Translational Research, 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.

United States Computer Emergency Readiness Team. (n.d.). Resources for Business. U.S. Department of Homeland Security. (Accessed 6/9/2016.)

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.

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.

U.S. Department of Health and Human Services, Office for Civil Rights. (n.d.). Security Rule Guidance Material. (Accessed 6/10/2016.)

This webpage assists healthcare professionals find information about the HIPAA Security Rule and provides links to other standards and resources on safeguarding electronic protected health information.

* U.S. Department of Health and Human Services, Office for Civil Rights and Office of the National Coordinator for Health Information Technology. (2015). Security Risk Assessment (SRA) Tool.

The Security Risk Assessment tool was designed to help guide healthcare providers in small to medium-sized offices conduct risk assessments of their organizations. This webpage contains a user guide and tutorial video. Users can download the app to their computers or iPads.

Williams, P.A. and Woodward, A.J. (2015). Cybersecurity Vulnerabilities in Medical Devices: A Complex Environment and Multifaceted Problem. Medical Devices. 8:305-16.

The authors review the factors that can contribute to cybersecurity vulnerabilities in medical devices and provide guidance regarding protection mechanisms, mitigations, and processes.

Education and Training

Grance, T., Nolan, T., Burke, K., et al. (2006). Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities. (NIST SP 800-84.) National Institute of Standards and Technology, U.S. Department of Commerce.

This guide can help staff in healthcare facilities design, develop, conduct and evaluate cybersecurity tests, training, and exercise events.

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.

Industrial Control Systems Cyber Emergency Response Team. (n.d.) Training Available through ICS-CERT. U.S. Department of Homeland Security. (Accessed 6/10/2016).

This webpage includes links to scheduled web-based and instructor-led cybersecurity training on the ICS-CERT calendar. These programs are geared toward industrial control system protection.

National Initiative for Cybersecurity Careers and Studies. (n.d.). Training. U.S. Department of Homeland Security. (Accessed 6/10/2016).

From this webpage, visitors can search for offered trainings by focus area, offering entity, level of training, location of training, and other factors as well as access various on-line training sites.

*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.

* U.S. Department of Health and Human Services, Office for Civil Rights. (n.d.). HIPAA Training & Resources. (Accessed 6/10/2016.)

These training and resource materials were developed to help entities implement privacy and security protections. This webpage includes videos and slides from state attorneys general training and educational programs for healthcare providers.

Education and Training: HHS-Specific

U.S. Department of Health and Human Services, Office of the Chief Information Officer. (2013). Rules of Behavior for Use of HHS Information Resources.

These rules apply to government employees, contractors, and other system users and must be read by all new users prior to accessing HHS data, systems, or networks. The policies may serve as a helpful template for private sector entities.

U.S. Department of Health and Human Services, Office of the Chief Information Officer. (2015). Information Security for Executives: Fiscal Year 2015.

This training course defines the security responsibilities for senior executives within HHS.

U.S. Department of Health and Human Services, Office of the Chief Information Officer. (2015). Information Security for IT Administrators, Fiscal Year 2015.

This training course defines the security responsibilities for IT Administrators within HHS.

U.S. Department of Health and Human Services, Office of the Chief Information Officer. (2015). Information Security for Managers: Fiscal Year 2015.

This training course defines the security responsibilities for information technology and program managers within HHS.

U.S. Department of Health and Human Services, Office of the Chief Information Officer. (2016). Cybersecurity Awareness Training: Fiscal Year 2016.

This training course provides general guidelines for securing information and information systems for federal employees though it may be a valuable outline for private sector employee learning.

Guidance

Cichonski, P., Millar, T., Grance, T., and Scarfone, K. (2012). Computer Security Incident Handling Guide. (NIST SP 800-61.) National Institute of Standards and Technology, U.S. Department of Commerce.

This guide can help healthcare organizations develop cybersecurity incident response capabilities. It includes guidelines for handling incidents (focusing on analyzing incident-related data and determining the appropriate response to each incident), and detailed incident management information and checklists. The authors note that the guidelines can be followed regardless of hardware platforms, operating systems, protocols, or applications.

Clark, D., Berson, T., and Lin, H.S. (Eds.) (2014). At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues. (Free download.) The National Academies Press.

This book “is a call for action to make cybersecurity a public safety priority.” It provides a comprehensive overview of the field and approaches for assessing and improving cybersecurity.

Cybersecurity Unit. (2015). Best Practices for Victim Response and Reporting of Cyber Incidents. U.S. Department of Justice.

This document provides planning and response guidance based on lessons learned by federal prosecutors while handling cyber investigations and prosecutions. The authors drafted the document with smaller organizations (with fewer resources), but larger organizations may also find it useful.

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). Though this reference is located on a commercial website, the information governance conceptual framework is a helpful construct for the ASPR TRACIE audience.

Filkins, B. (2014). Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon. SANS Institute.

The project team analyzed a year's worth of healthcare intelligence data and provide an overview of the sector's vulnerabilities (including the "Internet of Things" and challenges related to compliance). The author shares three case studies that demonstrate traffic and how healthcare networks were attacked and concludes with preparedness tips useful to both information technology professionals and emergency planners.

Filkins, B. (2014). New Threats Drive Improved Practices: State of Cybersecurity in Health Care Organizations. SANS Institute.

The author presents results from a SANS 2014 State of Cybersecurity in Health Care Organizations survey. Overall, 41% of respondents ranked current data breach detection strategies as ineffective and more than half found the "negligent insider" to be the primary threat to security.

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.

Homeland Security Information Network. (2016). Cyber Threats Library. (Registration required.)

This library includes information on potential cybersecurity threats grouped into several categories: FBI Flash (information from the Liaison Alert System); HHS Cyber Threat Intelligence Program Product; DHS Weekly Analytic Synopsis; Ransomware; and other sources.

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.

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.

* 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.

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.

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

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

Scarfone, K. and Mell, P. (2012). Guide to Intrusion Detection and Prevention Systems (IDPS) (Draft). (NIST SP 800-94). National Institute of Standards and Technology, U.S. Department of Commerce.

This report provides an overview of four intrusion detection and prevention technologies: network-based, wireless, network behavior analysis (NBA), and host-based.

U.S. Department of Health and Human Services, Office for Civil Rights. (n.d.). Security Rule Guidance Material. (Accessed 6/10/2016.)

This webpage assists healthcare professionals find information about the HIPAA Security Rule and provides links to other standards and resources on safeguarding electronic protected health information.

United States Computer Emergency Readiness Team. (n.d.). Resources for Business. U.S. Department of Homeland Security. (Accessed 6/9/2016.)

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.

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.

Incident Management

Forum of Incident Response and Security Teams. (2016). FIRST.

This membership organization is comprised of computer security incident response teams from government, educational, and commercial organizations. FIRST's goals include encouraging cooperation and coordination in incident prevention, rapid incident response, and the promotion of information sharing among members and the community at large.

ISACA. (2012). Incident Management and Response White Paper. (Free registration required.)

This document provides an overview of incident management and response as it relates to information security threats and incidents.

Mell, P., Kent, K., and Nusbaum, J. (2005). Guide to Malware Incident Prevention and Handling. (NIST SP 800-83.) National Institute of Standards and Technology, U.S. Department of Commerce.

The authors provide recommendations that can help an organization prevent, prepare for, respond to, and recover from malware incidents, especially widespread ones. Several types of malware are addressed (e.g., worms, viruses, and Trojan horses) and Appendix B provides malware incident handling scenarios that can help identify strengths and gaps in a facility's cybersecurity plans.

The International Organization for Standardization. (n.d.). Information Security Incident Management. (ISO/IEC 27035; accessed 5/19/2016. First three sections provided for free; the rest of the document may be purchased.)

Cybersecurity professionals can use the guidance in this International Standard to "a) detect, report and assess information security incidents; b) respond to and manage information security incidents; c) detect, assess and manage information security vulnerabilities; and d) continuously improve information security and incident management as a result of managing information security incidents and vulnerabilities."

* U.S. Department of Health and Human Services, Office for Civil Rights and Office of the National Coordinator for Health Information Technology. (2015). Security Risk Assessment (SRA) Tool.

The Security Risk Assessment tool was designed to help guide healthcare providers in small to medium-sized offices conduct risk assessments of their organizations. This webpage contains a user guide and tutorial video. Users can download the app to their computers or iPads.

Legal / Regulatory Resources

Kent, K., Chevalier, S., Grance, T., and Dang, H. (2006). Guide to Integrating Forensic Techniques into Incident Response. (NIST SP 800-86). National Institute of Standards and Technology, U.S. Department of Commerce.

The guidance in this document can help cyber professionals develop digital forensic capabilities that complements local regulations. The authors provide comprehensive information on using the analysis process with four data categories (network traffic, files, operating systems, and applications).

* U.S. Department of Health and Human Services, Office for Civil Rights. (n.d.). HIPAA Training & Resources. (Accessed 6/10/2016.)

These training and resource materials were developed to help entities implement privacy and security protections. This webpage includes videos and slides from state attorneys general training and educational programs for healthcare providers.

The White House. (2013). Executive Order -- Improving Critical Infrastructure Cybersecurity.

This Executive Order directs the U.S. government to “increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats.”

The White House. (2015). Executive Order -- Promoting Private Sector Cybersecurity Information Sharing.

This Executive Order builds upon the 2013 directive and Presidential Policy Directive-21, and calls for the U.S. Secretary of Homeland Security to “encourage the development and formation of Information Sharing and Analysis Organizations.” The organizations may include members from the public or private sectors and can operate as for-profit or nonprofit entities.

United States Congress. (2015). S.754 - Cybersecurity Information Sharing Act of 2015.

This bill requires the Director of National Intelligence and the U.S. Departments of Homeland Security, Defense, and Justice to develop strategies to share cybersecurity threat information with all entities under threats (e.g., private, nonfederal government agencies, state, tribal, and local governments, and the public). This includes information that could prevent/mitigate adverse effects and best practices.

U.S. Department of Health and Human Services, Office for Civil Rights. (n.d.). HIPAA for Professionals. (Accessed 6/10/2016.)

Cybersecurity professionals can locate information about HIPAA rules, guidance on compliance, the Office for Civil Rights' enforcement activities, frequently asked questions, and more on this webpage. This site also contains a variety of compliance and security resources relative to patient information.

Lessons Learned

ASPR TRACIE. (2016). Cybersecurity and Healthcare Facilities. U.S. Department of Health and Human Services, Office of the Assistant Secretary for Preparedness and Response.

Cybersecurity is a critical issue facing the ASPR TRACIE audience. In this webinar, a distinguished panel of experts describe lessons learned from recent experiences, planning considerations, and steps the federal government is taking to address cybersecurity and cyber hygiene.

Davis, J. (2016). Human Element the Weakest Link in Healthcare Security, Says Verizon Report. Healthcare IT News.

Verizon examined more than 100,000 security incidents and found that of the 166 healthcare breaches, 115 had confirmed data loss, 32% were caused by stolen assets, and 23% were a result of privilege misuse. The report also found reuse of credentials to be a healthcare-specific risk.

Duncan, I., McDaniels, A.K., and Campbell, C. (2016). Hackers Offering Bulk Discount to Unlock Encrypted MedStar Data. The Baltimore Sun.

The authors provide an overview of a recent attack on MedStar (a system in the Baltimore-Washington, DC region), highlighting the need for newer employees to also be familiar with more traditional (non-electronic) paper-pencil methods for maintaining records.

Stone, J. (2016). Hackers' Ransom Attack on California Hospital More Proof Healthcare Cybersecurity Is Floundering. International Business Times.

The author provides an overview of the cyberattack on Hollywood Presbyterian Medical Center (CA).

U.S. Department of Homeland Security. (2016). Cyber Storm: Securing Cyber Space.

Cyber Storm is the U.S. Department of Homeland Security's biennial cybersecurity exercise. This webpage includes highlights and lessons learned from exercises and links for more information.

Verizon. (2016). 2016 Data Breach Investigations Report.

This comprehensive report details data from over 100,000 incidents affecting various industries, including healthcare. Victim demographics, vulnerabilities, phishing, and incident classification patterns are discussed and an entire appendix is devoted to “attack graphs.”

Medical Devices

Armstrong, D.G. Kleidermacher, D.N., Klonoff, D.C., and Slepian, M.J. (2015). Cybersecurity Regulation of Wireless Devices for Performance and Assurance in the Age of "Medjacking." (Abstract only.) Journal of Diabetes Science and Technology. 10(2): 435-438.

The authors outline a framework for securing wireless health devices to minimize the occurrence of “medjacking,” or the hacking medical devices.

Gerard, P., Kapadia, N., Acharya, J., et al. (2013). Cybersecurity in Radiology: Access of Public Hot Spots and Public Wi-Fi and Prevention of Cybercrimes and HIPAA Violations. (Abstract only.) American Journal of Roentgenology. 201(6): 1186-1189.

The authors list steps that can be taken to protect sensitive information while transferring medical information over public and home networks. They emphasize the importance of these steps and strategies as the role of information technology in modern radiology practice increases.

Klonoff, D.C. (2015). Cybersecurity for Connected Diabetes Devices. Journal of Diabetes Science and Technology. 9(5):1143-7.

The author provides an overview of the “CIA Triad” for information security, where C stands for confidentiality, I stands for integrity, and A stands for availability. The author explains how a cybersecurity standard designed specifically for connected diabetes devices will improve device safety and increase security.

Kramer, D.B., Baker, M., Ransford, B., et al. (2012). Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance. PLoS One. 7(7):e40200.

The authors evaluated recalls and adverse events related to security and privacy risks of medical devices and found “sharp inconsistencies” in the way individual providers secured devices. The authors challenged manufacturers and regulators to consider the security and privacy elements of their devices and systems and to build the ability to collect cybersecurity threat indicators into their medical devices.

U.S. Food and Drug Administration. (2014). Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff. U.S. Department of Health and Human Services.

This guidance provides recommendations to consider and information to include in FDA medical device premarket submissions for effective cybersecurity management. Effective cybersecurity management is intended to reduce the risk to patients by decreasing the likelihood that device functionality is intentionally or unintentionally compromised by inadequate cybersecurity.

U.S. Food and Drug Administration. (2016). Moving Forward: Collaborative Approaches to Medical Device Cybersecurity, January 20-21, 2016. U.S. Department of Health and Human Services.

Users can access webcasts, presentations, transcripts, and a program book from this meeting held in 2016 as well as the new January 2016 draft guidance on medical devices (updated from 2014). Speakers in the workshop highlighted collaborative efforts and shared information about existing frameworks that can help assess an organization's cybersecurity processes.

Williams, P.A. and Woodward, A.J. (2015). Cybersecurity Vulnerabilities in Medical Devices: A Complex Environment and Multifaceted Problem. Medical Devices. 8:305-16.

The authors review the factors that can contribute to cybersecurity vulnerabilities in medical devices and provide guidance regarding protection mechanisms, mitigations, and processes.

Plans, Tools, and Templates

* Health Information Trust Alliance. (2014). HITRUST De-Identification Framework. (Free registration required.)

Developed in collaboration with healthcare, information security, and de-identification professionals, the HITRUST De-Identification Framework provides a consistent, managed methodology for the contextual de-identification of data and the sharing of compliance and risk information amongst entities and their key stakeholders. The Framework provides 12 criteria for a successful de-identification program and methodology that can be scaled to any organization: the first four criteria address the programmatic and administrative controls that an organization should have in place to govern de-identification, and the remaining eight criteria may be used to derive a de-identified data set, either on an ad hoc basis or by instituting a process that will deliver de-identified data sets.

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.

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.

* 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.

Kent, K. and Souppaya, M. (2006). Guide to Computer Security Log Management. (NIST SP 800-92). National Institute of Standards and Technology, U.S. Department of Commerce.

The authors emphasize the need for log management and provide guidelines that can help healthcare facility cyber professionals establish related robust policies and procedures.

National Council of Information Sharing and Analysis Centers. (2016). Information Sharing and Analysis Centers and Their Role in Critical Infrastructure Protection.

This factsheet provides an explanation of Information Sharing and Analysis Centers and highlights recent accomplishments.

National Institute of Standards and Technology. (2014). Framework for Improving Critical Infrastructure Cybersecurity. (V. 1.0).

This document provides a detailed framework to protect critical infrastructure and a set of activities to achieve specific cybersecurity outcomes. The Core Functions include: Identify, Protect, Detect, Respond, and Recover, and Section 3 of the guide includes examples of how the framework can be employed when creating a cybersecurity program.

* 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.

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

This model program is a result of a public-private partnership established to improve electricity subsector cybersecurity capabilities, and to examine and better understand the cybersecurity posture of the grid. Links to related resources are also provided on this webpage.

* 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 Health and Human Services, Office for Civil Rights and Office of the National Coordinator for Health Information Technology. (2015). Security Risk Assessment (SRA) Tool.

The Security Risk Assessment tool was designed to help guide healthcare providers in small to medium-sized offices conduct risk assessments of their organizations’ HIPPA compliance. This webpage contains a user guide and tutorial video. Users can download the 156 question app to their computers or iPads.

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.

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.

U.S. Department of Homeland Security. (2016). HSIN-HPH Bulletin: Ransomware (Locky Variant). (Subscription required.)

This bulletin includes an overview of Locky ransomware, how it has traditionally been delivered, and mitigation steps 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.

Risk and Threat

Anti-Phishing Work Group. (2016). APWG.

The Anti-Phishing Working Group (AFWG) is a coalition whose goal is to unify "the global response to cybercrime across industry, government, and law enforcement sectors and NGO communities." Their website includes links to helpful resources, reporting mechanisms, programming options, and the like.

Financial Services Sector Coordinating Council. (2015). Automated Cybersecurity Assessment Tool. (Located at the bottom of the page.)

This tool—available in Excel—can help healthcare institutions identify their risks, assess their cybersecurity preparedness, and inform related risk management plans and strategies.

Healthcare Information and Management Systems Society. (2015). 2015 HIMSS Cybersecurity Survey. (Executive summary only.)

Nearly 300 individuals from the healthcare field completed this cybersecurity survey, and 87% indicated that information security had gained ground as a business priority over the past year. Sixty-four percent of respondents reported incidents committed by external actors (e.g., hackers or scam artists). Approximately 20% of these events led to the loss of patient, financial, or operational data.

Healthcare IT News. (2015). Infographic: Greatest Areas of Improvement in Cybersecurity.

This infographic—based on findings from the 2015 Healthcare Information and Management Systems Society survey—shows that survey respondents chose cybersecurity and network security as the two areas that have seen the greatest amount of improvement.

Healthcare IT News. (2015). Infographic: Top 10 Cybersecurity Threats of the Future.

Healthcare Information and Management Systems Society survey respondents listed ten cybersecurity threats they will be challenged by in the future. Some of these threats include: phishing attacks, known software vulnerabilities, denial of service attacks, and negligent insiders.

InfraGuard. (n.d.). InfraGuard: Partnership for Prevention. (Accessed 6/15/2016.)

InfraGard is a partnership between the private sector and the Federal Bureau of Investigation, and includes members from businesses, academic institutions, state and local law enforcement agencies, and other participants who represent 16 critical infrastructures (including emergency services and healthcare and public health). Interested parties can apply to join online, and the open-access part of the webpage includes links to state and local chapters and a calendar of events.

Internet Storm Center. (2016). Internet Storm Center (ISC).

This volunteer-run webpage was created in 2001 and features free warning and analysis to Internet users while working closely with Internet service providers to combat cyberattacks. The webpage features daily “Stormcasts” and links to articles, patches, podcasts, tools, and other helpful information.

Ipswitch. (2016). Sponsored: Report Reveals Only 30 percent of Healthcare IT Teams are Restricting Insecure Cloud File Sharing. Healthcare IT News.

In a vendor-sponsored survey, 38% of healthcare information technology respondents indicated that they use cloud file sharing services (for patient records and medical data). Just 40% of U.S. respondents (and 20% of European respondents) reported having related restrictive policies.

McCann, E. (2012). Healthcare Data Breaches on the Rise, with Potential $7B Price Tag. Healthcare IT News.

According to the author, the third annual “Benchmark Study on Patient Privacy and Data Security" found that 94 % of hospitals reported experiencing data breaches over the past two years (involving medical files, billing, and insurance records). Many breaches are a result of preventable incidents (e.g., loss of equipment, employee errors). The associated cost to healthcare facilities is staggering.

Siwicki, B. (2016). Ponemon: 89 Percent of Healthcare Entities Experienced Data Breaches. Healthcare IT News.

Findings from the Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data highlighted that, so far in 2016, half of data breaches in healthcare are due to criminal activity. The other half are due to mistakes.

U.S. Department of Health and Human Services, Office for Civil Rights. (n.d.). OCR Cyber Awareness Newsletters. (Accessed 6/10/2016.)

The Office for Civil Rights issues periodic newsletters share knowledge about the various security threats and vulnerabilities that currently exist in the healthcare sector, helping stakeholders understand what security measures can be taken to decrease the possibility of being exposed by these threats, and how to reduce breaches of electronic protected health information.

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.

Agencies and Organizations

Note: The agencies and organizations listed in this section have a page, program, or specific research dedicated to this topic area.

Anti-Phishing Work Group.

Federal Bureau of Investigation. Cyber Crime.

Forum of Incident Response and Security Teams.

Health Information Trust Alliance.

Healthcare Information and Management Systems Society. HIMSS Healthcare Cybersecurity Environmental Scan Reports.

HealthcareITNews. Privacy and Security.

InfraGuard.

Internet Storm Center.

National Cybersecurity and Communications Integration Center.

National Health Information Sharing and Analysis Center.

National Healthcare & Public Health Critical Infrastructure Protection.

U.S. Department of Health and Human Services. Office for Civil Rights.

U.S. Department of Health and Human Services, Office for Civil Rights. HIPAA for Professionals.

U.S. Department of Homeland Security. United States Computer Emergency Response Team.

This ASPR TRACIE Topic Collection was comprehensively reviewed in May 2016 by the following subject matter experts (listed in alphabetical order):

***Bryan Cline,** Ph.D., Vice President, Standards & Analytics, Health Information Trust Alliance; **Scott Cormier**, Vice President, Emergency Management, EC, and Safety, Medxcel; **Steve Curren,** MSFS, Director, Division of Resilience, Office of Emergency Management, HHS ASPR; **Andrea Geiger**, Health Information Privacy and Security Specialist, U.S. Department of Health and Human Services, Office for Civil Rights; **John Hick**, MD, HHS ASPR and Hennepin County*

Medical Center; ***Iliana Peters****, Senior Health Information Privacy Specialist, U.S. Department of Health and Human Services, Office for Civil Rights;* ***Patrick Pilch****, CPA, MBA, Managing Director and National Healthcare Advisory Leader, BDO;* ***Shahryar Shaghaghi****, MS, Technology Advisory Services National Leader and Head of International Cybersecurity, BDO; and* ***Staff from the Office of Information Security****, HHS.*