HEALTH CARE CYBERSECURITY

At a Glance

As technology's role in the delivery of health care grows, risks posed to individuals and organizations by other entities with nefarious objectives are increasing. As electronic health record (EHR) use increases, health care providers have worked diligently to mitigate breaches in patient health information (PHI). Likewise, organizations must now mitigate various and ever-changing cyberattacks, which include any type of offensive maneuver that targets computer information systems, infrastructures, networks and/or personal computer devices through malicious acts. These acts usually originate from an anonymous source that hacks into a susceptible system and steals, alters or destroys a specified target.

Each health care organization and provider must work with its information system management team to identify the necessary resources to develop a strong cybersecurity defense. CHA, the Hospital Council of Northern & Central California, Hospital Association of Southern California and Hospital Association of San Diego & Imperial Counties have compiled the following facts, check list and resources to assist in managing an effective cybersecurity program. While this information is current, we recognize the rapidly changing nature of cybersecurity and will update this document as needed; the most recent version will be available at www.calhospital.org/cybersecurity.

Did you know?

- Worldwide, the number of cyberattacks increased 40 percent[i]; in 2015, criminal attacks became the number one root cause of data breaches in health care.[ii] [iii]
- Cybercriminals are using cyberattack techniques, tools, tactics and scope that are changing at an exponential pace.

- Cyberattacks using malware or viruses can occur from internal or external sources. Common targets of health care cyberattacks include:
    - Medical devices such as radiology equipment (CT and MRI), picture archive and communications systems (PACS), blood gas analyzers, therapeutic equipment (infusion pumps, medical lasers and LASIK surgical machines), and life support equipment (heart-lung machines, medical ventilators, extracorporeal membrane oxygenation machines and dialysis machines)
    - Technology equipment, including computers, telephone systems, video conferencing, routers and firewalls
    - Clinical EHR software and equipment
    - Financial and employee information
    - Building control/plant operating systems
- Health care information is worth 10 times more than credit card numbers on the black market.[iv]

CYBERATTACK MITIGATION CHECKLIST

- ☑ Who in executive leadership is responsible for cybersecurity?
- ☑ Does your organization have a cybersecurity policy? Is it regularly updated? Does it address potential ransomware demands?
- ☑ Has your organization completed a cybersecurity gap analysis that addresses your vulnerabilities? If so, how often is it updated? Is this reported to the Board of Directors?
- ☑ Is cybersecurity part of your organization's disaster Hazard Vulnerability Analysis?
- ☑ Who assumes responsibility and liabilities for outsourced information technology services?
- ☑ Do you have cybersecurity insurance?
- ☑ What are the cybersecurity expectations of third party vendors, and how are these being monitored and audited?
- ☑ Do you have plans to ensure continuous quality patient care in the absence of electronic information, communications or data?
- ☑ What cybersecurity education and staff training have been completed?

RESOURCES

Background – Establishing the National Cybersecurity Initiative

- President's Executive Order on Improving Critical Infrastructure Cybersecurity
  www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
- Presidential Policy Directive 21: Critical Infrastructure Security and Resilience
  www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
- The White House Cybersecurity Office
  www.whitehouse.gov/cybersecurity

Resources for Implementing the President's Executive Order

- The Voluntary Critical Infrastructure Cybersecurity Program
  Created to provide incentives for private sector organizations that are part of the critical infrastructure to adopt the NIST Framework.
  www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework
  - See specific recommendations from:
    - Department of Homeland Security (DHS)
      www.dhs.gov/publication/summary-report-executive-order-13636-cybersecurity-incentives-study
    - Commerce
      www.ntia.doc.gov/files/ntia/Commerce_Incentives_Recommendations_Final.pdf
    - Treasury
      www.treasury.gov/press-center/Documents/Treasury%20Report%20(Summary)%20to%20the%20President%20on%20Cybersecurity%20Incentives_FINAL.pdf

- Department of Justice and Federal Trade Commission: Antitrust Policy Statement on Sharing of Cybersecurity Information
  Policy statement indicates that both FTC and DOJ do not view the antitrust laws as a barrier to sharing cybersecurity information, even among competitors.
  www.ftc.gov/public-statements/2014/04/department-justice-federal-trade-commission-antitrust-policy-statement

Resources Specific to the Health Care and Public Health Critical Infrastructure Sector

- FDA Resources about Medical Device Cybersecurity
  www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm

- Department of Homeland Security (DHS) - Cybersecurity Resources
  www.dhs.gov/topic/cybersecurity

- Healthcare and Public Health Sector: Background and General Information
  www.dhs.gov/healthcare-and-public-health-sector

Tools to Assist with Gap Analysis and California Support Systems

- National Institute of Standards and Technology's (NIST) Framework to Reduce Cyber Risks to Critical Infrastructure
  Framework being developed to help owners and operators of critical infrastructure identify, assess and manage the risk of cyber threats.
  www.nist.gov/itl/cyberframework.cfm

- Crosswalk between the NIST Framework and the HIPAA Security Rule from the HHS Office for Civil Rights (OCR)
  www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/index.html

- Healthcare Sector Cybersecurity Framework Implementation Guide
  This guide was developed by the Health Information Trust Alliance (HITRUST), the Healthcare and Public Health (HPH) Sector Coordinating Council (SCC) and Government Coordinating Council (GCC) to assist health care organizations in implementing the NIST Framework.
  https://hitrustalliance.net/documents/cybersecurity/HITRUST_Healthcare_Sector_Cybersecurity_Framework_Implementation_Guide.pdf

- HITRUST Common Security Framework (CSF)
  A comprehensive and flexible framework of prescriptive and scalable security controls developed to address the multitude of security, privacy and regulatory challenges facing health care organizations.
  http://hitrustalliance.net/common-security-framework/

- DHS' Control Systems Security Program (CSSP)
  Assists owners of networks and industrial control systems (ICS) in assessing and strengthening their organization's cybersecurity posture through a tiered system including the Cyber Security Evaluation Tool (CSET®) and onsite consultation options.
  http://ics-cert.us-cert.gov/Assessments

- Cyber Security Evaluation Tool CSET 7.1 - latest version from DHS's ICS-CERT (issued Feb. 22)
  A free desktop software tool that provides a systematic approach for evaluating an organization's cybersecurity posture.
  https://ics-cert.us-cert.gov/ICS-CERT-Releases-CSET-71

- Safer Guidelines
  The Office of the National Coordinator for Health Information Technology has developed SAFER Guides, which are designed to help healthcare organizations conduct self-assessments to optimize the safety and safe use of EHRs.
  www.chpso.org/sites/main/files/file-attachments/safer_contingencyplanning_sg003_form_0.pdf

- "Securing Hospitals"
  Independent Security Evaluators, a private security firm from Baltimore, completed a hospital industry assessment and a developed a white paper on "securing hospitals."
  https://securityevaluators.com/hospitalhack/securing_hospitals.pdf

- California Office of Emergency Services (Cal OES)
  The Cal OES State Threat Assessment Center has developed a For Official Use Only (FOUO) document on ransomware and cybersecurity; hospitals must register to obtain the document.
  www.calstas.org/(X(1)S(4frodry1toyalqigyvszp1iq))/default.aspx?MenuItemID=182&MenuGroup/CALSTAS+Home.html&AspxAutoDetectCookieSupport=1

- California Hospital Preparedness
  California hospitals have been actively engaged in continuity planning as an effort under the hospital preparedness grant program, as well as education and training conducted at CHA's annual disaster planning conference. Many resources and tools to assist in your planning are available on the CHA preparedness website.
  www.calhospitalprepare.org/continuity-planning

- Reporting of attacks to California Fusion Centers
  Cyberattacks are criminal acts and should be reported to local law enforcement as well as to an organization's respective fusion center/regional threat assessment center. A map and contact information for fusion centers are available on the State Threat Assessment Center website.
  www.calstas.org/default.aspx/MenuItemID/142/MenuGroup/CALSTAS+Home.html

Opportunities for Information Sharing

- Healthcare and Public Health Sector Coordinating Council (HPH SCC)
  www.dhs.gov/healthcare-and-public-health-sector-council-charters-membership
  - Council Charter: www.dhs.gov/sites/default/files/publications/Healthcare-SCC-Charter-2014-508.pdf

- National Health Information Sharing and Analysis Center (NH-ISAC)
  National Health ISAC (NH-ISAC), a nonprofit organization responsible for the public and private health care sector's cybersecurity in the United States, has developed a threat intelligence platform through which information on critical cyber threats and vulnerabilities both in cyberspace and medical devices can be shared between the private and public sectors. The organization holds an annual national summit on health care cybersecurity.
  www.nhisac.org/

- InfraGard
  A public/private partnership between the FBI and U.S. businesses that focuses on threats that could disrupt the national critical infrastructure.
  www.infragard.net/

- Health Information Trust Alliance (HITRUST)
  The Health Information Trust Alliance (HITRUST), in collaboration with health care, business, technology and information security leaders, has established the HITRUST CSF, a certifiable framework that can be used by any and all organizations that create, access, store or exchange personal health and financial information. HITRUST webinar series features real world examples from organizations using the HITRUST Assurance Program to manage their information security programs. In addition, they have released a new guide to help with implementation of the National Institute of Standards and Technology's Cybersecurity Framework.
  www.hitrustalliance.net/
  - HITRUST Cyber Threat XChange (CTX) - Now free for basic level subscription. HITRUST CTX automates collection, analysis and distribution of cyber threats information.
    https://hitrustalliance.net/cyber-threat-xchange/
  - To receive HITRUST C3 Alerts or participate in the monthly cyber threat briefings, register at www.hitrustalliance.net/cyberupdates/.
  - HITRUST encourages participating hospitals to provide feedback directly to the Alliance about the effectiveness of the content and format of these C3 Alerts and monthly threat briefings.

- Critical Infrastructure Cyber Community Voluntary Program (C^3 Voluntary Program)
  A program created to help support and promote use of the Cybersecurity Framework developed by NIST.
  www.us-cert.gov/ccubedvp

- The Homeland Security Information Network
  A national secure web-based portal for information sharing and collaboration.
  www.dhs.gov/homeland-security-information-network
  - The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
    http://ics-cert.us-cert.gov/

Other Relevant Resources

- Health Information Management Systems Society (HIMSS) resources:
  - National Cyber Security Awareness Month resources
    www.himss.org/NCSAM
  - Resources about information security and privacy
    www.himss.org/library/healthcare-privacy-security

- Centers for Medicare & Medicaid Services (CMS) - Information Security Policies for Hospitals www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/IS_Policy-.pdf
    - Series to be updated to address cybersecurity issues

- The Securities and Exchange Commission's guidance for publicly-traded hospitals (October 2011) www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm
    - Recommends disclosure to the public of both cybersecurity vulnerabilities and intrusions

---

[i] http://www.healthcareitnews.com/news/criminal-attacks-healthcare-become-no-1-cause-data-breaches

[ii] http://www.beckershospitalreview.com/healthcare-information-technology/criminal-attacks-no-1-cause-of-healthcare-data-breaches-5-things-to-know.html

[iii] The Ponemon Institute. "What was the root cause of the healthcare organizations' data breach." Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data. May 2015.

[iv] http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924