READY READER

Kansas CMS Emergency Preparedness CoP Newsletter | Issue 17: 5 September 2017

All Hazards Preparedness Planning: Introduction to Cyber

The CMS Emergency Preparedness Final Rule has directed an all-hazards approach to emergency preparedness but has also singled out equipment and power failure, interruptions in communications and loss of a portion of your facility. All of this could be attributed to a cyber attack.

In 2016, the Healthcare Sector experienced more cyber incidents resulting in data breaches than any of the other 15 critical infrastructure sectors across the country. This is in part due to the healthcare industries lack of information systems security preparedness planning and budgetary support to information technology across the sector. The current increased focus on cybersecurity provides an opportunity for the health care industry to adapt and improve.

Healthcare facilities across our state are diverse, complex and vary from very small to massive health systems. Discussions from across the country agree that there isn't one plan or template that would work for cyber attack preparedness planning. But hopefully this article will give you some ideas on how to develop your plan, some may work some may not.

First, a cyber security plan isn't like your normal all-hazard plan. Different personnel within your organization will need to be notified that are not part of your normal ICS or notification plan. Inventory of systems and prioritization of response and recovery will need to be reviewed. Legal ramifications and publicly allowed information will have to be discussed. Supporting organizations will be different than a normal COOP or preparedness plan.

Scenario—you walk in on Tuesday morning and none of the systems work; no phones, no printers, no email. HVAC is partially working. Networked medical devices are giving inaccurate information. What do you do? This real-world scenario has actually occurred several times across the U.S.

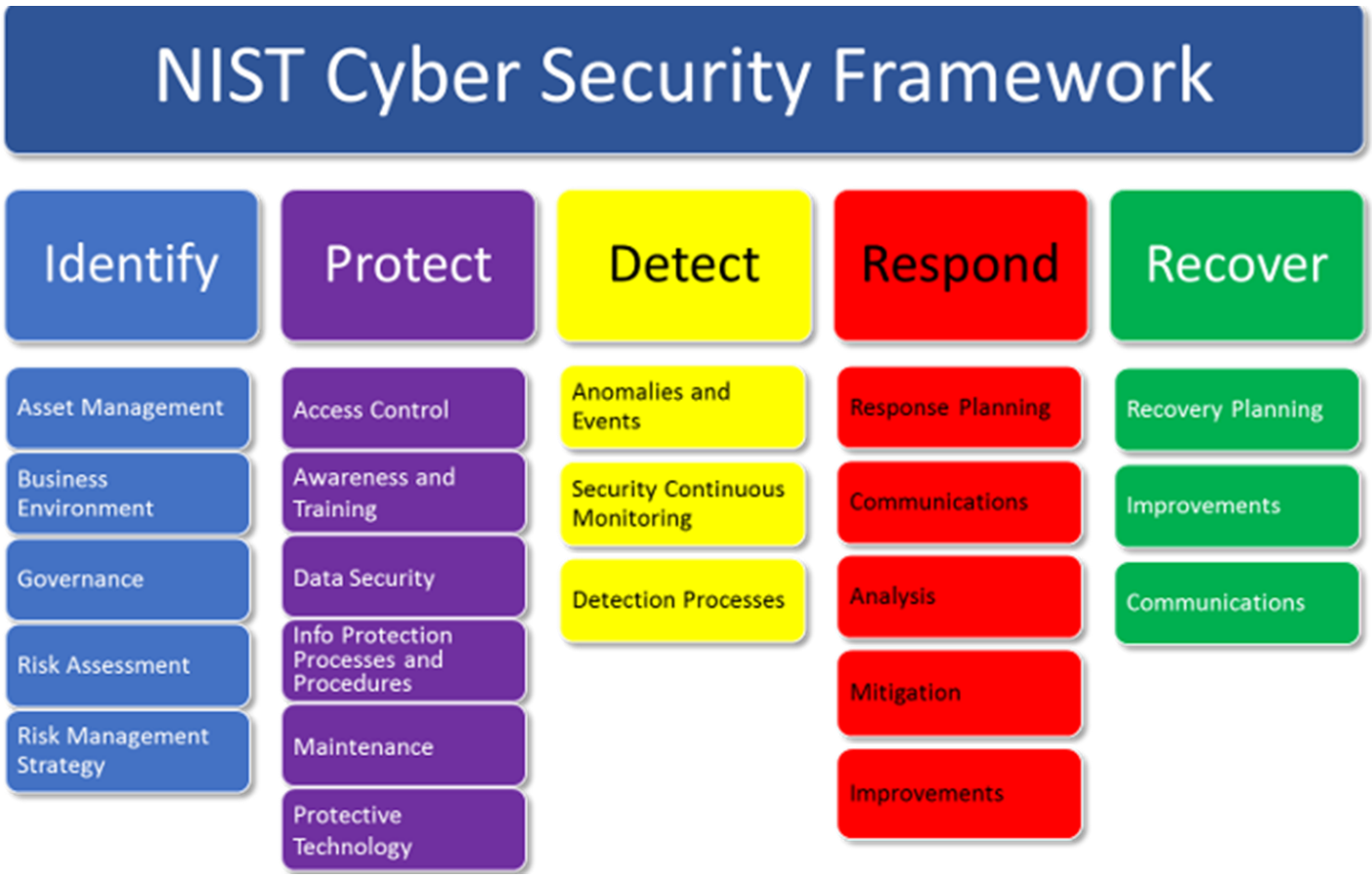
In This Issue

Previous issues of the Ready Reader available at http://www.kdheks.gov/cphp/providers.htm

National Policy

In 2003, the Federal government established the Healthcare and Public Health (HPH) Sector as a Critical Infrastructure (CI) sector in the United States, recognizing that its security and resilience are essential to national security, the economy, and public health and safety. In 2013, President Obama issued Executive Order 13636, “Improving Critical Infrastructure Cybersecurity”. The order called for the development of a Cybersecurity Framework that organizations can use to help reduce and manage their cyber security risks.

In 2016 the HPH Sector Coordinating Council (SCC) and Government Coordinating Council (GCC) jointly developed the critical infrastructure Sector-Specific Plan (https://www.phe.gov/Preparedness/planning/cip/Documents/2016-hph-ssp.pdf) goals, priorities, and activities to reflect the overall strategic direction for the HPH sector. The Sector goals support he critical infrastructure joint national priorities developed in 2014 and the National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience (NIPP 2013). Since the release of the 2016 HPH plan, a more detailed report on Improving Cybersecurity in the Health Care Industry was released June of 2017 by the Health Care Industry CyberSecurity Task Force (https://www.phe.gov/preparedness/planning/CyberTF/Pages/default.aspx). This report demonstrates the urgency and complexity of the cybersecurity risks facing the healthcare industry and calls for collaborative public and private sector campaign to protect our systems and patients from cyber threats.



The National Institute of Standards and Technology has developed a generic framework, health care has many unique aspects such as its diverse resource capabilities, legacy systems that will persist for years, and the burden of the need to shared data that is essential for collaborative patient-oriented care.

Identify: Inventory your systems

- Do you know what software systems you have? All of them?
- What operating system are they running on?
- Are they up to date? Patched?
- Is your network segregated? Does your health records need to be on the same network as your cafeteria point of sale or your Industrial Controls (HVAC).

Protect: Information Protection Process and Procedures

- Are your systems up to date? Patched?
- Employee Training

Detect: Computer Anomaly Detection

- Computer performance issues
- Continuous malicious activity detection

Respond: Planning & Communication

- Short-Term, Long-term downtime plans
- Is the anomaly contributed to an external threat or internal IT failure?
- Identification of which systems are affected? HVAC, Backup Power, Water
- Contingency Plans (i.e. paper charting)?
- Communication and Information Sharing - communication both vertically through the hospital and horizontally to standalone facilities?
- HICS? Do you activate? COOP Plans? What are the triggers for activation due to a cyber-attack?
- Notification of cyber activity. Some of the people you may or may not normally think of to contact first during a typical hazard event. Such as:
    - IT Director
    - Legal Officer—Is this an Internal Threat or an External Threat?, Management of co-investigation with IT Director will assist in remediation under work-product privilege., Reporting to State and Federal agencies., Contact with patients and other who feel aggrieved.
- Local law enforcement & FBI Cyber Unit cywatch@ic.fbi.gov or 855-292-3937, https://www.ic3.gov/default.aspx; Regional FBI Field Office – KC (816) 512-8200

Recover: Prioritization, Communication of the Recovery

- Does your staff know which systems they use daily and would prioritize?
  Systems?
- Prioritize individually or Group (i.e. clinical, administrative, logistic, fiscal)?
- Facilities and areas (i.e... Clinics, ER, ICU, surgical areas, Lab, Pharmacy, MRI)
- Communication—Recovery update to staff and vendors.
- Communication to patients and public—what do provide? Legal, Reputation ramifications?
- Paper Charting?
- Payroll? How would you pay your employees if you can't access the payroll system?

Additional Information

The CMS Final Rule (https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertEmergPrep/Emergency-Prep-Rule.html) has highlighted cyber on page (11).

An example of a Cyber Annex which would be part of your overall Emergency Operations Plan can be viewed at the KDHE Preparedness Standard Operating Guide webpage http://www.kdheks.gov/cphp/operating_guides.htm.

New CMS Response and Recovery Resources

New CMS Emergency Response and Recovery page for a variety of CMS response resources.

Contact Us

KDHE Health Facilities
P—785.296.0131
Jim.Perkins@ks.gov

KDHE Preparedness
P-785.296.7100
KDHE.Preparedness@ks.gov

Kansas Division of Emergency Management
Bryan.D.Murdie.nfg@mail.mil

Kansas Department on Aging and Disability Services
Denise.German@ks.gov

Office of the State Fire Marshal
Brenda.McNorton@ks.gov

Kansas Hospital Association
P– 785.276.3125
rmarshall@kha-net.org

Kansas Home Care Association
P– 785.478.3640
khca@kshomecare.org

Centers for Medicare & Medicaid Services
victoria.vachon@cms.hhs.gov

State ADA Coordinator
P– 785.296.1389
Anthony.Fadale@ks.gov

Kansas Health Care Association
P– 785.267.6003