2018 DHS Cybersecurity Strategy and Resources

In May, the Department of Homeland Security (DHS) released their 2018 Cybersecurity Strategy, which will span the next five years. DHS is tasked with working to better defend the 16 critical infrastructure sectors of the United States and healthcare is one of them. Although the Department of Health and Human Services (HHS) is formally designated as the Sector-Specific Agency for healthcare, DHS plays an important role as well. Their strategy pertains to healthcare and has five pillars and seven goals underneath these pillars.

1. Risk Identification
   a. Assess Evolving Cybersecurity Risks
2. Vulnerability Reduction
   a. Protect Federal Government Information Systems
   b. Protect Critical Infrastructure
3. Threat Reduction
   a. Prevent and Disrupt Criminal Use of Cyberspace
4. Consequence Mitigation
   a. Respond Effectively to Cyber Incidents
5. Enable Cybersecurity Outcomes
   a. Strengthen the Security and Reliability of the Cyber Ecosystem
   b. Improve Management of DHS Cybersecurity Activities

Resources

There are many unique challenges that the healthcare sector faces as the frequency and severity of attacks continues to threaten patient safety and sensitive health information. On May 29, DHS held a webinar on cybersecurity within the healthcare sector and discussed a number of resources that can help increase cybersecurity resiliency. These resources include:

- National Cybersecurity and Communications Integration Center (NCCIC), which is housed under DHS. The NCCIC involves cyber threat hunting and incident response teams with 24/7 real time threat analysis and incident reporting. It is in place to increase information sharing but the mission will continue to evolve along with the threats at hand.
- Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR) program, which creates public-private partnerships to increase cyber education and awareness.
- The National Initiative for Cybersecurity Careers and Studies (NICCS) provides over 3,000 courses that are cyber related. The website, along with the National Initiative for Cybersecurity Education (NICE), includes an interactive "National Cybersecurity Workforce Framework" to help identify different cybersecurity roles in an organization as well as the skills that are required to perform them.

Cybersecurity Assessment Resources:

- Stakeholder Risk Assessment and Mitigation, a resource with Cybersecurity Advisors (CSAs) that are put in place "to provide direct coordination, outreach, and regional support and assistance in the protection of cyber components essential to the Nation's Critical Infrastructure."
- United States Computer Emergency Readiness Team (US-CERT) has a number of other cybersecurity assessments available, with many listed below. However, if you'd like more information on these cybersecurity assessments, and others, please visit the DHS Cybersecurity Services Catalog for State, Local, Tribal and Territorial Governments.
    - Cyber Resilience Review (CRR): The CRR is a free, voluntary, non-technical assessment that evaluates an organization's operational resilience and cybersecurity practices of its critical services. This test can be administered or self-assessed and will measure an organizations' practices against the Cybersecurity Framework (CSF) from the National Institute of Standards and Technology (NIST).
        - Cybersecurity Infrastructure Survey Tool (C-IST): This assessment was put together as a supplemental resource to the CRR and was organized through Carnegie Mellon University as part of a DHS research and development grant. The assessment must be administered by DHS and is a performance summary of cybersecurity capabilities. Once you have completed the test, your results will be compared to other participants, so you know where your organization stands.
    - Cybersecurity Evaluations Tool (CSET): This tool can help organizations customize scenarios that would test how their current cybersecurity mechanisms would be able to handle said scenario. It will then assist in purchasing decisions to further the goal of cybersecurity.
    - National Cybersecurity Assessments and Technical Services (NCATS) include the following evaluations:
        - Cyber Hygiene: Vulnerability Scanning: Through this program, DHS will perform regular network and vulnerability scans to deliver a weekly report for the organization's review. After the application is submitted, the scans will start within three days and require little direct interaction with DHS. A sample report can be found here.
        - Phishing Campaign Assessment (PCA): This assessment is administered by DHS over a period of six weeks with each week becoming more complex of an attempt. At the end of the period, there will be a report that includes the percentage who clicked the links, broken down by week/complexity. You can find a sample report here.
        - Risk and Vulnerability Assessment (RVA): The RVA offers a number of network security services such as network mapping

and vulnerability scanning, phishing engagements, web application or database evaluations, and a full penetration test. The test usually takes two weeks but unfortunately, there is an 8-12 month waiting period because the demand is so high.

- Validated Architecture Design Review (VADR): VADR "evaluates your systems, networks, and security services to determine if they are designed, built, and operated in a reliable and resilient manner."