March 10th, 2020

TLP White

In this edition of Hacking Healthcare, we begin by breaking down new guidance from the Department of Justice (DOJ) on the legal considerations of engaging in cyber threat intelligence activities. Next, we look at the European Union Agency for Cybersecurity's (ENISA) 51-page report on procurement cybersecurity for hospitals that provides comprehensive guidance applicable to many organizations in the healthcare sector. Finally, we explore a Government Accountability Office (GAO) report that recommends NIST Cybersecurity Framework adoption and assessment across all critical infrastructure sectors. Welcome back to *Hacking Healthcare*.

1. **DOJ Releases Guidance on Gathering Cyber Threat Intelligence.** Last week, the U.S. Department of Justice released a document entitled *Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources*.[1] The guidance comes as a response to private sector inquiries for more clarity on the legal issues surrounding the practice of gathering cyber threat intelligence, which is routinely cited as being significantly beneficial in preventing or mitigating cyber threats. Most of the guidance is straightforward and is specifically premised on activities conducted within U.S. jurisdiction. While DOJ does spotlight certain threat intelligence activities that they consider illegal, they stop short of guaranteeing legal protection or safe harbor for any specific activity.

   The guidance is broken down into several scenarios, uses, best practices, and tips that give a snapshot of the most common types of activities that take place in gathering cyber threat intelligence. The document suggests that while passive intelligence collection using a fictitious persona is unlikely to bring legal repercussions, impersonating an actual individual, actively engaging in criminal forums, unauthorized access of criminal forums, and purchasing of stolen data can considerably raise the risk of legal culpability. One notable concern called out in the paper is cybersecurity researchers who may seek to engage with criminal forums or individuals as part of their work. DOJ is very clear that under no circumstances is this behavior justified or legal.

   To minimize the potential legal liability associated with cyber intelligence gathering, the DOJ sets forth a number of recommendations and best practices. Foremost is the recommendation that organizations and researchers cultivate relationships with relevant law enforcement authorities, which include the local FBI field office or Cyber

Task Force and the local U.S. Secret Service field office or Electronic Crimes Task Force (ECTFs). Early engagement with these authorities can help establish credibility in the event of a future investigation and can lessen the potential of accidental interference with ongoing investigations. Additionally, DOJ recommends organizations establish and document rules of engagement, operational planning, and seek advice from legal counsel before engaging in cyber intelligence gathering.

2. **ENISA Releases Hospital Procurement Guidelines.** Late last month, ENISA released a report entitled *Procurement Guidelines for Cybersecurity in Hospitals*.[2] The guidance recognizes the importance of securing every aspect of the healthcare information and communications technology ecosystem, including the sometimes-overlooked procurement step, and it strives to provide a "comprehensive set of tools and good practices that can be adapted to the hospitals' procurement process."[3] The 51-page guidance is targeted at senior executives, IT professionals, and procurement officers and is narrowly focused on the hospital environment. Nevertheless, much of the guidance and recommendations are applicable throughout the healthcare sector.

   Written in an accessible and non-technical format, the guidance takes a holistic approach to procurement starting from the initial planning phase, working through the sourcing phase, and concluding with a management and review phase. In the report, each phase has a dedicated section that breaks down and describes the activities associated with mature cybersecurity procurement programs. These sections follow a uniform structure and detail individual activities by listing examples and evidence, the related procurement types associated with the activity, and the threats each activity seeks to address.

3. **GAO Releases Study on Critical Infrastructure Adoption of NIST Cybersecurity Framework.** Toward the end of last month, the U.S. Government Accountability Office (GAO) released a report entitled *Critical Infrastructure Protection – Additional Actions Needed to Identify Framework Adoption and Resulting Improvements*. The objectives of the report were to "determine the extent to which (1) Sector Specific Agencies (SSAs) have developed methods to determine framework adoption [within their sector] and (2) implementation of the framework has led to improvements in the protection of critical infrastructure from cyber threats."[4] The catalyst for the report appears to be a mandate by the Cybersecurity Advancement Act 2014, which requires GAO to track the promotion and sector-wide adoption of the NIST Cybersecurity Framework (CSF), as well as assess the success of that adoption in protecting critical infrastructure.[5]

   The report found that most of the SSAs "had not developed methods to determine the level and type of adoption of the NIST CSF," which is something that GAO has historically recommended.[6] GAO commented that SSAs' evaluation of their sectors' adoption and implementation of the NIST CSF within critical infrastructure is "essential to protection efforts."[7] As such, the study concluded with recommendations to the SSAs to commit

themselves to "[collecting] and [reporting] sector-wide improvements from use of the framework across its critical infrastructure sectors using existing initiatives."[8]

Congress –

Tuesday, March 10th:
- Senate – Committee on the Judiciary - Hearings to examine copyright law in foreign jurisdictions, focusing on how other countries are handling digital piracy.

- Senate – Committee on Small Business and Entrepreneurship - Hearings to examine the coronavirus and America's small business supply chain.

- House – Committee on Small Business - The Impact of Coronavirus on America's Small Businesses

- House – Committee on Homeland Security - Community Perspectives on Coronavirus Preparedness and Response

Wednesday, March 11th:
- No relevant hearings

Thursday, March 12th:
- No relevant hearings

International Hearings/Meetings –

Wednesday, March 11th:
- NHS Webinar: Bringing together the NHS App and online consultations

EU – No relevant hearings/meetings

Conferences, Webinars, and Summits –

--H-ISAC Monthly Member Threat Briefing – Webinar (3/31/2020)
https://h-isac.org/hisacevents/h-isac-monthly-member-threat-briefing-6/
--H-ISAC Security Workshop - Cambridge, MA (4/7/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-cambridge-ma/
--H-ISAC Security Workshop - Atlanta, GA (4/13/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-atlanta/
--Healthcare Cybersecurity Forum - Mid-Atlantic – Philadelphia, PA (4/20/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426497
--CYSEC 2020 – Dubrovnik, Croatia (4/29/2020 – 4/30/2020)
https://h-isac.org/hisacevents/cysec-2020-croatia/
--H-ISAC 2020 Spring Summit – Tampa, FL (5/11/2020 – 5/15/2020)
https://h-isac.org/summits/strike-back-summit/
--H-ISAC Security Workshop - Frederick, MD (6/9/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-frederick-md/
--AAMI Exchange – New Orleans, LA (6/12/2020-6/15/2020)
https://h-isac.org/hisacevents/aami-exchange/
--H-ISAC Security Workshop - Lisbon, Portugal (6/17/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-lisbon-portugal/

--H-ISAC Security Workshop - Buffalo, NY (6/23/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-buffalo-ny-2/
--H-ISAC Inaugural APAC Summit – Singapore (6/23/2020-6/25/2020)
https://h-isac.org/summits/apac-summit-2020/
--Healthcare Cybersecurity Forum - Rocky Mountain – Denver, CO (7/20/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426499
--Healthcare Cybersecurity Forum – Southeast – Nashville, TN (9/9/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426517
--H-ISAC Security Workshop - Greenwood Village, CO (9/16/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-greenwood-villiage-co/
--Healthcare Cybersecurity Forum – Northeast – Boston, MA (9/22/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/427126
--Summit on Security & Third Party Risk – National Harbor, MD (9/28/2020-9/30/2020)
https://h-isac.org/hisacevents/summit-on-security-third-party-risk/
--Healthcare Cybersecurity Forum – Texas – Houston, TX (10/8/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428840
--H-ISAC Security Workshop - Mounds View, MN (10/27/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-buffalo-ny/
--Healthcare Cybersecurity Forum - Pacific Northwest – Seattle, WA (10/28/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428886
--Healthcare Cybersecurity Forum – California – Los Angeles, CA (11/12/2020)
https://h-isac.org/hisacevents/healthcare-cybersecurity-forum-california-2/

Sundries –

--Hackers seize on coronavirus fears for fodder in spearphishing, misinformation schemes
https://www.cyberscoop.com/coronavirus-spearphishing-misinformation-italy-russia/
--Younger generation of professionals expect more from today's healthcare, Philips study shows
https://www.healthcareitnews.com/news/europe/younger-generation-professionals-expect-more-today-s-healthcare-philips-study-shows
--UAE to set up first virtual hospital in the Middle East
https://www.healthcareitnews.com/news/europe/uae-set-first-virtual-hospital-middle-east
--How to track the coronavirus: Dashboard delivers real-time view of the deadly virus
https://www.zdnet.com/article/how-to-track-the-coronavirus-dashboard-delivers-real-time-view-of-the-deadly-virus/

Contact us: follow @HealthISAC, and email at contact@h-isac.org

[1] https://www.justice.gov/criminal-ccips/page/file/1252341/download
[2] https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services
[3] https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services
[4] https://www.gao.gov/assets/710/704808.pdf
[5] https://www.govinfo.gov/content/pkg/PLAW-113publ274/pdf/PLAW-113publ274.pdf
[6] https://www.gao.gov/assets/710/704808.pdf
[7] https://www.gao.gov/assets/710/704808.pdf
[8] https://www.gao.gov/assets/710/704808.pdf