October 2, 2018

TLP White

We start with a look at the FDA's plans to advance innovation in digital health. We also discuss a recently resolved bug on the Twitter platform, and DHS's effort to understand and mitigate supply chain risks. We conclude by shedding some light on how the Middle East is integrating technology to solve healthcare challenges. Welcome back to *Hacking Healthcare:*

Hot Links –

1. ***FDA Plans for Advancing Innovation in Digital Health.*** The Food and Drug Administration ("FDA") published a blog post describing the agency's approach to advancing innovation in digital health.[1] The post, written by FDA Commissioner Scott Gottlieb, emphasizes the FDA's belief that a modern, flexible, risk-based approach to regulation is the best way to limit time and cost of market entry, ensure patient safety, and encourage continued development innovation in digital health. The post details the FDA's plans for implementing this approach to how the agency regulates as well as to the FDA's internal operations.

   The blog post also reviews the FDA's recent developments with respect to digital health innovation, including the launch of the Digital Health Innovation Action Plan and subsequent launch of the digital health software precertification pilot program and commitment to issue new guidance in this space. Through the discussion, the FDA recognized the need for a flexible regulatory approach that allows product developers, patients, and regulators to keep up with frequent software updates, and that enables a rapid cycle of product improvement.

   As part of the FDA's digital health agenda, the agency is pushing for additional resources as part of the FDA's FY2019 budget. This budget includes a proposal to create a Center of Excellence for Digital Health ("CoE"), and within that a cybersecurity unit. One of the cybersecurity unit's missions is to establish a public-private multi-disciplinary effort convening a broad range of stakeholders and expertise to serve as a resource for

[1] https://www.fda.gov/NewsEvents/Newsroom/FDAVoices/ucm621675.htm

industry and the FDA in assessing cybersecurity vulnerabilities and incidents as well as to identify solutions.

2. ***Twitter Bug.*** Twitter recently resolved a bug discovered in its account activity API ("AAAPI") that affected the direct message function and interactions with companies that use Twitter for customer service activities. In order for the bug to compromise interactions between customers and businesses, the user must have chatted with a company on Twitter, and the company must have relied on a developer that used AAAPI to permit the chat function. When this occurred, the DMs between the customer and business or protected tweets could have gone to a different developer. The bug ran from May 2017 until September 10, 2018, and fortunately had a relatively limited impact affecting less than 1% of users. Upon discovery of the bug, Twitter immediately released a fix so that data would not continue to go to incorrect developers.

   Some bugs, including the Twitter bug, aren't always the result of proactive hackers, which are more often a topic of conversation. Moreover, bugs and other misconfigurations may run on a system for extended periods of time in ways that are difficult to detect. In this case, the bug exposed sensitive information for over a year before detection.

3. ***DHS Studying Supply Chain Risks.*** Last week the MITRE Corporation hosted a meeting to discuss the Department of Homeland Security ("DHS") Cyber Supply Chain Risk Management Program.[2] The purpose of the meeting was to introduce the program and provide an update on the Supply Chain Task Force. The meeting follows a Request for Information issued by DHS in August announcing the department's deep dive into information and communications technology ("ICT") supply chain risk management.

   According to a DHS notice, "DHS seeks information about capabilities that address risk as a function of threat, vulnerability, likelihood, and consequences, and aggregate multiple data sets into structured archives suitable for analysis and visualization of the relationships of businesses, individuals, addresses, supply chains, and related information."[3] The government is in search of a better understanding of capabilities that permit identification and mitigation of supply chain risks presented by ICT-based services and service providers that use ICT for specific support functions.

   DHS intends to use information gathered through the due diligence capability among organizations and in combination with other information to broadly address supply chain risks to federal, state, local, tribal, and territorial governments as well as critical

[2] https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/ssca/2018-fall/Fall%202018%20SSCA%20Forum%20Agenda.pdf

[3] https://www.fbo.gov/index?s=opportunity&mode=form&id=cc0129f78d35c150620ac884f1493fdd&tab=core&_cview=1

infrastructure owners and operators. Comments in response to the RFI are due on October 10, 2018.

4. ***Digital Health in the Middle East.*** With new technology spawning at a rapid clip, governments, health providers and companies are all devoting a significant amount of effort understanding how to adopt new technology to solve healthcare challenges. With so many technologies available, the challenge resides in finding viable models to bring technological innovations to healthcare and to patients. The Economist Intelligence Unit ("EIU") launched a report analyzing how digital technologies are shaping the Middle East's healthcare ecosystems, activities and stakeholders. [4]

   The EIU report found that: (1) government-led digital transformation efforts in several parts of the Middle East are reshaping how individuals and organizations in the healthcare ecosystem are interacting with each other, with a stronger need for collaboration and new terms of engagement; (2) the value of technology in different markets and geographies can be expanded by growing telehealth use and by implementing data-driven solutions to create smarter, more efficient and more precise healthcare outcomes; and (3) digital technology is enabling new care experiences by reconfiguring medical service delivery, bringing opportunities in decentralized and near-patient products and services.

Congress –

Tuesday, October 2:
--No relevant hearings.

Wednesday, October 3:
--Hearing to examine rare diseases, focusing on expediting treatments for patients (Senate Subcommittee on Children and Families).[5]

Thursday, October 4:
--No relevant hearings.

International Hearings/Meetings –

EU –

--No relevant hearings.

[4] http://www.eiu.com/Handlers/WhitepaperHandler.ashx?fi=Digital-Health-Middle-East-EIU-2018.pdf&mode=wp&campaignid=DigitalHealthME
[5] https://www.senate.gov/committees/hearings_meetings.htm

October 2, 2018

Conferences, Webinars, and Summits –

--NH-ISAC Blended Threats Exercise Series – GA (10/2) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--NH-ISAC Blended Threats Exercise Series – MD (10/4) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--Information Sharing Turns 20: Learn more at Borderless Cyber USA – Washington, DC (10/4) <https://nhisac.org/events/nhisac-events/information-sharing-turns-20-learn-more-at-borderless-cyber-usa/>
--HSCC Joint Cyber Working Group Meeting – Nashville, TN (10/9-11) <https://nhisac.org/events/nhisac-events/hscc-joint-cyber-working-group-meeting/>
--Biotech/Pharma Security Workshop – Tokyo, Japan (10/17) <https://nhisac.org/events/nhisac-events/biotech-pharma-security-workshop-tokyo/>
--Health IT Summit – Seattle, WA (10/22) <https://vendome.swoogo.com/2018-Seattle-HITSummit>
--CSS - "Table Stakes" in the Development and Deployment of Secure Medical Devices – Minneapolis, MN (10/22) <https://nhisac.org/events/nhisac-events/css-3/>
--Summit on Third-Party Risk – Leesburg, VA (10/24-26) <https://nhisac.org/events/nhisac-events/summit-on-third-party-risk/>
--2018 Heathcare CyberGard Conference – Charlotte, NC (10/25-26) <https://nhisac.org/events/nhisac-events/2018-heathcare-cybergard-conference/>
--NIST Cybersecurity Risk Management Conference – Baltimore, MD (11/7-9) <https://www.nist.gov/news-events/events/2018/11/nist-cybersecurity-risk-management-conference>
--Health IT Summit – Beverly Hills, CA (11/8-9) <https://vendome.swoogo.com/2018-BeverlyHills>
--NH-ISAC Blended Threats Exercise Series – So. CA (11/19) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--2018 NH-ISAC Fall Summit – San Antonio, TX (11/26-29) <https://www.destinationhotels.com/la-cantera-resort-and-spa>
--FIRST Symposium 2019 – London, UK (3/18/19) <https://nhisac.org/events/nhisac-events/first-symposium-2019/>

Sundries –

-- **DEF CON report finds decade-old flaw in widely used ballot-counting machine** <https://www.cyberscoop.com/def-con-voting-village-report/>
-- **Uber to pay $148 million to states for 2016 data breach** <https://www.cyberscoop.com/uber-data-breach-settlement-148-million/>
-- **Cisco Releases Alerts for 14 High Severity Bugs** <https://www.bleepingcomputer.com/news/security/cisco-releases-alerts-for-14-high-severity-bugs/>
-- **Election security bill won't pass ahead of midterms, says key Republican**

October 2, 2018

<https://thehill.com/policy/cybersecurity/408368-lankford-election-security-bill-wont-pass-ahead-of-midterms>
--**Wyden: Senators need protection from ongoing Russian hacking campaign**
<https://www.politico.com/story/2018/09/19/russians-hacking-senators-emails-fancy-bear-830642>

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