July 10, 2018

TLP White

We start with a look at some of the big technology companies and their goals for healthcare, particularly with artificial intelligence (AI), and then continue the AI theme with a look at part of what the government is doing, and why it may not be enough. We conclude with a recent court case that is bringing some clarity to the world of cybersecurity insurance. Welcome back to *Hacking Healthcare:*

Hot Links –

1. ***Big Tech Keeps Stepping Up their Healthcare Game.*** It's no secret that big IT companies have been aggressively pursuing the healthcare market in a number of ways. Four of the biggest (Microsoft, Google, Apple, and Amazon) have all been actively looking at how their technologies can help administrators, practitioners, and patients be more efficient, make better use of data, improve security, manage privacy, and empower everyone to manage their personal healthcare. Let's take a quick look at a few examples.

   Microsoft recently hired a couple new executives to oversee its healthcare efforts, including:
   - Microsoft Genomics which provides "…researchers and clinicians with highly accelerated, cloud-powered genomic processing services.";
   - Azure Security and Compliance Blueprint, which is an "end-to-end application development foundation to help health organizations move to the cloud.."; and
   - Project Empower MD, a research collaboration that "will create a system that listens and learn from what doctors say and do".[1]

   Meanwhile, Google has been investing heavily into their DeepMind AI, which is focusing on how to make sense of the massive amount of data produced through healthcare apps, medical devices, and patient records.

[1] https://blogs.microsoft.com/blog/2018/02/28/microsofts-focus-transforming-healthcare-intelligent-health-ai-cloud/

For their part, Apple has been focusing on Apple Health Records[2], which has been putting the management of healthcare records into the hands of patients so they can "aggregate their health care records from multiple institutions alongside their patient-generated data". Most recently, Apple filed 54 patents designed to turn the iPhone into a medical device that "can monitor biometric data such as blood pressure and body fat levels to develop algorithms to predict abnormal heart rates"[3], among other things.

Not to be left out, Amazon established a "secret" lab called Grand Challenge that is focused on cancer research and using their massive Amazon Web Services cloud platform to use "artificial intelligence to organize, parse, and check unstructured medical record data for errors."[4]

These are just a few examples of what these and many others companies are doing to bring advanced technology that has been successfully serving other markets to bear on healthcare. The common elements include the use of AI to address big data problems, and leveraging the nearly ubiquitous deployment of advanced mobile phones to create even more of that data.

2. ***Speaking of Artificial Intelligence and Privacy....*** On May 10th of this year, the Trump Administration held a closed door summit on Artificial Intelligence for American Industry. The summit "brought together more than 100 senior government officials, technical experts from top academic institutions, heads of industrial research labs, and U.S. business leaders in the agriculture, energy and manufacturing, financial services, healthcare and transportation sectors to discuss the policies that will be needed to harness the promise of AI-powered technologies."[5]

   That sounds great, but not everyone was happy with the way it was conducted. The Electronic Privacy Information Center (EPIC), brought together several scientific organizations and nearly 100 of their own experts to petition the White House Office of Science and Technology Policy (OSTP). In their petition they say "The reach of AI is so vast, so important, and encompasses so many issues, it is imperative that the Administration provide the American public the opportunity to comment on proposed policy initiatives impacting the American Public."[6]

   In particular, the petition notes that "the words 'accountability,' 'transparency', 'ethics', and 'fairness' do not appear in the report of the White House AI Summit."[7] Those seem

[2] https://www.apple.com/healthcare/health-records/
[3] https://www.healthcareitnews.com/news/patents-hold-clues-about-apple-amazon-google-and-microsoft-plans-healthcare#gs.40pEjRs
[4] https://www.theverge.com/2018/6/5/17431012/amazon-grand-challenge-moonshot-lab-google-glass-creator-babak-parviz
[5] https://www.law360.com/aerospace/articles/1060355/artificial-intelligence-policy-needs-public-input-gov-t-told
[6] https://epic.org/privacy/ai/OSTP-AI-Petition.pdf
[7] https://epic.org/privacy/ai/OSTP-AI-Petition.pdf

like some rather important ideas that probably should be considered when developing policies that will likely involve the personal information of American citizens.

Unfortunately, government has a habit of sometimes soliciting input from the private sector and then running off to do whatever it is they are going to do in a way that isn't always transparent. In some cases, this is justified by national security concerns, and to be fair, AI is being leveraged by the military and intelligence communities in ways that might warrant some amount of secrecy. But as we have discussed before, government policies, even those that are for managing their own internal processes and projects, often find their way into the private sector by virtue of agency purchasing power.

3. ***Insurer Must Cover Loss.*** Cybersecurity insurance has been getting a lot of attention in recent years as the insurance industry looks to evolve its products, and organizations look to find ways to protect themselves from loss. However, the relative newness of the business has meant that what policies ultimately cover or don't cover isn't always clear. A recent ruling in the Second Circuit U.S. Court of Appeals may have brought at least a little clarity.

   In September of 2014, an employee of Medidata Solutions Inc. was tricked into transferring nearly $4.8 million dollars to a bank account in China. Known as "business email compromise (BEC)"[8], this type of social engineering attack remains common today, but the FBI didn't start tracking it until 2013 and in 2014 many organizations simply weren't aware of it as serious threat. Whether or not this particular employee should have been more careful or if the proper processes were in place to avoid this type of mistake is a topic for another time.

   What matters here is that Medidata believed their cybersecurity insurance covered them for the loss, but their insurer, Federal Insurance Co. (a unit of Chubb Ltd.), thought otherwise, so Medidata filed suit in 2015. Fast forward 3 years through the speedy court system, and we have a resolution.

   The Second Circuit judge ruled that Federal Insurance must cover the $4.8 million loss. Basically, Federal had argued that the policy required a direct hack of Medidata's computer systems and that the fraudulent email didn't meet that criteria. However, the Court determined that because the email "made a change to a data element, as the email system's appearance was altered by the spoofing code to misleadingly indicate the sender", it was in fact a hack as defined in the policy.

Congress –

Tuesday, July 10:
--No relevant hearings

[8] https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise

Wednesday, July 11:
--Hearing to discuss election security preparations from both federal and vendor perspectives. (Senate Committee on Rules & Administration)[9]

Thursday, July 12:
--No relevant hearings

Conferences, Webinars, and Summits –

--Health IT Summit – Denver, CO (7/12) <https://vendome.swoogo.com/2018-Denver-HITSummit>
--Health IT Summit – St. Petersburg, FL (7/24) <https://vendome.swoogo.com/StPetersburg-HITSummit-2018>
--NH-ISAC & Boston Scientific Medical Device Security Workshop – Maple Grove, MN (7/24) <https://nhisac.org/events/nhisac-events/medical-device-security-workshop-at-maplegrove-mn/>
--NH-ISAC Blended Threats Exercise Series – MN (7/25) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--CSS - Healthcare System Management of Medical Devices (7/26) <https://nhisac.org/events/nhisac-events/css-2/>
--Basic Best Practices in Cybersecurity – Abilene, TX (7/31) <https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-texas-2/>
--Health IT Summit – Boston, MA (8/7) <https://vendome.swoogo.com/2018-Boston-Health-IT-Summit>
--NH-ISAC Blended Threats Exercise Series – CA (8/28) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--Biotech/Pharma Security Workshop at Gilead Sciences – Foster City, CA (8/29) <https://nhisac.org/events/nhisac-events/biopharma-workshop-at-gilead-sciences-foster-city-ca/>
--Biotech/Pharma Security Workshop at Amgen – Tokyo, Japan (8/29) <https://nhisac.org/events/nhisac-events/biotech-pharma-security-workshop-at-amgen-tokyo/>
--Basic Best Practices in Cybersecurity – Abilene, KS (8/29) <https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-kansas-3/>
--NH-ISAC Blended Threats Exercise Series – DE (9/10) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--Basic Best Practices in Cybersecurity – Nashville, TN (9/21) <https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-nashville/>
--NH-ISAC Blended Threats Exercise Series – GA (10/2) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>

[9] https://www.rules.senate.gov/hearings/election-security-preparations-federal-and-vendor-perspectives

--NH-ISAC Blended Threats Exercise Series – MD (10/4) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--NH-ISAC & Cleveland Clinic Medical Device Security Workshop – Breachwood, OH (10/17-18) <https://nhisac.org/events/nhisac-events/medical-device-security-workshop-at-cleveland-clinic-beachwood-oh/>
--Health IT Summit – Seattle, WA (10/22) <https://vendome.swoogo.com/2018-Seattle-HITSummit>
--CSS - "Table Stakes" in the Development and Demployment of Secure Medical Devices – Minneapolis, MN (10/22) <https://nhisac.org/events/nhisac-events/css-3/>
--NIST Cybersecurity Risk Management Conference – Baltimore, MD (11/4-6) <https://www.nist.gov/cyberframework>
--Health IT Summit – Beverly Hills, CA (11/8-9) <https://vendome.swoogo.com/2018-BeverlyHills>
--2018 NH-ISAC Fall Summit – San Antonio, TX (11/26-29) <https://www.destinationhotels.com/la-cantera-resort-and-spa>

Sundries –
-- **The Worst Cybersecurity Breaches of 2018 So Far**
<https://www.wired.com/story/2018-worst-hacks-so-far>
-- **All the Ways iOS 12 Will Make Your iPhone More Secure**
<https://www.wired.com/story/apple-ios-12-iphone-security>
-- **New York jury convicts two men for trading on hacked press releases**
<https://www.reuters.com/article/us-usa-crime-insidertrading-cyber/new-york-jury-convicts-two-men-for-trading-on-hacked-press-releases-idUSKBN1JW313?feedType=RSS&feedName=domesticNews>
-- **Subpoenas of Google, Twitter In Reporter's Assault Suit OK'd**
https://www.law360.com/whitecollar/articles/1060527/subpoenas-of-google-twitter-in-reporter-s-assault-suit-ok-d

Contact us: follow @NHISAC and email at contact@nhisac.org