August 14, 2018

TLP White

We start with an announcement from the Department of Homeland Security about the formation of a National Risk Management Center. We also address some amendments to Ohio law which have implications for Blockchain and data breaches. We conclude with discussing a recent data breach and the role that employees play in those statistics. Welcome back to *Hacking Healthcare:*

Hot Links –

1. ***DHS Announces National Risk Management Center.*** From our "Where were you when…?" department, we look at the recent Department of Homeland Security ("DHS") National Cybersecurity Summit. The summit brought together a few hundred people from government and industry to listen to leaders discuss the importance of cybersecurity to the nation and to their world.

   The words "collaborate", "coordinate", "public/private", and "partnership" were in full force during the day long summit. If you have spent any time working for or with the government, you may be forgiven for thinking that these words are code for "we don't really know what we want to do, but working together is better than not. Right?" And in truth, while lots of smart people are committed to making a difference, details were a bit light. DHS did announce a new federal risk management initiative, created to help coordinate risk management efforts among government and industry.[1] The fact sheet published by DHS explains that as part of the initiative, there will be a new National Risk Management Center ("Center") housed within DHS.[2]

   According to DHS, the Center "will create a cross-cutting risk management approach between the private sector and government to improve the defense of our nation's critical infrastructure." DHS has identified three mission areas for the Center: (1) identify, assess, and prioritize risks to national critical functions; (2) collaborate on the development of risk management strategies and approaches to manage risks to national critical functions; and (3) coordinate integrated cross-sector risk management activities.

[1] https://www.dhs.gov/news/2018/08/01/dhs-hosts-successful-first-ever-national-cybersecurity-summit
[2] https://www.dhs.gov/sites/default/files/publications/18_0731_cyber-summit-national-risk-management-fact-sheet.pdf

It is encouraging that there is activity in this space, and we are supportive of DHS and its mission to coordinate and facilitate risk management approaches between the public and private sector.

2. ***Ohio Legislation Has Implications for Blockchain and Data Breaches.*** This month Ohio enacted legislation bringing its existing Uniform Electronic Transaction Act more in step with modern technology.[3] Senate Bill 220 legitimizes Blockchain technology by recognizing records or contracts that have been secured through Blockchain technology as falling within the definition of "electronic record," and a signature secured through Blockchain technology as an "electronic signature" for the purposes of the statute. Ohio is part of a small but growing number of states implementing similar changes. Amendments like this one that give Blockchain legal effect and enforceability are particularly interesting given the promise that the technology holds in the healthcare sector. States are signaling to the private sector that they recognize the legitimacy of Blockchain and that they are willing to give companies in this space the support of legal enforcement for those that seek to take advantage of it.

   Senate Bill 220 also creates a legal safe harbor for companies that have implemented reasonable security measures prior to experiencing a data breach. The bill provides that in the event of a data breach, covered entities that have created, maintained, and complied with a written cybersecurity program that meets statutory requirements are entitled to an affirmative defense to any tort claims arising out of the incident. The statute states that a company may satisfy the cybersecurity program requirements if the covered entity's cybersecurity program reasonably confirms to any one of several federal frameworks, including the NIST Cybersecurity Framework.

3. ***Role of Employees in Breach Barometer.*** The Protenus Breach Barometer ("Breach Barometer" or "report") revealed that 3.15 million patient records were compromised in 142 healthcare data breaches between April and June of this year.[4] This was among several findings contained in the Protenus Breach Barometer, the output of a collaboration between Protenus and Databreaches.com with data collected from the Department of Health and Human Services, press reports, and proprietary nonpublic data from the Protenus AI platform. The report notes that in Q2 2018, around 30 percent of privacy violations were repeat offenders, explaining that "[o]n average if an individual healthcare employee breaches patient privacy once, there is a greater than 30% chance that they will do so again in three months' time, and a greater than 66% chance they will do so again in a years' time."[5]

---

[3] http://search-prod.lis.state.oh.us/solarapi/v1/general_assembly_132/bills/sb220/EN/05?format=pdf

[4] https://healthitsecurity.com/news/3.15m-records-exposed-by-142-healthcare-data-breaches-in-q2-2018

[5] https://cdn2.hubspot.net/hubfs/2331613/Breach_Barometer/2018/Q2%202018/Q2%202018%20Protenus%20Breach%20Barometer.pdf?t=1533584664360&utm_campaign=Breach%20Barometer&utm_source=hs_email&utm_medium=email&utm_content=65005819&_hsenc=p2ANqtz-_XWPWF6gooDWVgMw93hVzIL0XD4J8h-p8XIP9FXFgY-XvuUrfDQ9W7LMkISkhSDI7dzYvi80RP-yER-QFM5ibXx0f8cOh06YWJYc0OUaV2j32XZmU&_hsmi=65005819

We found this to be one of the report's most interesting findings because it suggests a clear opportunity for improvement. While it is difficult to predict the next big hacking trend, or what the next wave of malware will do, getting your workforce trained up to recognize an incident early on, and providing them with the infrastructure to effectively communicate any unusual activity to the right team is invaluable. It would also help to reduce some of the repeat offender statistics revealed in the report.

To read more on this and other findings, take a look at the complete report which can be found here.

Congress –

Tuesday, August 14:
--No relevant hearings

Wednesday, August 15:
--No relevant hearings

Thursday, August 16:
-- An oversight hearing to examine the Federal Communications Commission (Senate Committee on Commerce, Science, and Transportation)[6]

Conferences, Webinars, and Summits –

--NH-ISAC Blended Threats Exercise Series – No. 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/>
--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/>
--NH-ISAC Blended Threats Exercise Series – MD (10/4) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>

[6] https://www.senate.gov/committees/hearings_meetings.htm

--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/>
--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/>
--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>
--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>

Sundries –

--**Ready-to-use bitcoin ATM malware found for sale online**
<https://www.cyberscoop.com/bitcoin-atm-malware-trend-micro/>
--**Windows 10 Enterprise Getting "InPrivate Desktop" Sandboxed Execution Feature**
<https://www.bleepingcomputer.com/news/microsoft/windows-10-enterprise-getting-inprivate-desktop-sandboxed-execution-feature/>
--**Pentagon Bans Soldiers from Using GPS Apps and Devices**
<https://threatpost.com/pentagon-bans-soldiers-from-using-gps-apps-and-devices/134757/>
--**Facebook looks to advance data privacy conversation**
<https://www.politico.com/newsletters/morning-tech/2018/08/06/facebook-looks-to-advance-data-privacy-conversation-306614>
--**WhatsApp for Windows 10 Updated With Forwarding Restriction to Reduce Fake news**
<https://www.bleepingcomputer.com/news/microsoft/whatsapp-for-windows-10-updated-with-forwarding-restriction-to-reduce-fake-news/>

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