November 5th, 2019

TLP White

In this edition of Hacking Healthcare, we lead off by providing you with a few important announcements from the National Institute of Standards and Technology ("NIST"). We then discuss the use of a critical hospital technology and how it has led to public web-streaming of sensitive healthcare information. Next, we fill you in on the rise of attacks against managed service providers, and we explore what that means for small businesses and government entities. We then explore how a group of 15 technology companies are challenging a key assumption of the talent shortage in the cybersecurity workforce. Finally, we give you a brief update on how Norsk Hydro's cyber insurance payout is fueling skepticism in the cyber insurance market. Welcome back to *Hacking Healthcare*.

NIST Announcements:

- The comment period for **NIST Special Publication (SP) 1800-24, Securing Picture Archiving and Communications System ("PACS")**, will close on November 18, 2019. NIST encourages all impacted parties to review and comment. (link)
- NIST is still reviewing and accepting Letters of Interest ("LOI") for the **Securing Telehealth Remote Patient Monitoring Ecosystem**. If you would like to participate in the project, please email hit_nccoe@nist.gov and request an LOI template. As a reminder, NIST's "technology collaborators are selected on a first-come, first-serve basis, if their product or services align with the project needs." (link)

1. **Unsecured National Health Service Data Streamed Live.** Legacy hardware and software remain a significant vulnerability to organizations attempting to defend against current threats. Patients and healthcare providers inside the United Kingdom ("U.K.") were reminded of this last week, when Techcrunch reported that a hobbyist with an inexpensive amateur radio set up was picking up real-time medical and healthcare information and streaming it for the world to see. The culprit? Pagers.

   While pagers are often seen as an anachronism these days, many who work in hospitals continue to find invaluable use for them. As recently as 2017, nearly 80% of hospitals within the United States still provided pagers, and within the U.K., the National Health

Service ("NHS") still operates around 130,000 of them.[1,2] The reason for pagers' continued relevance is that their low operating frequency allows them to receive data through significantly more interference than many alternative communication technologies. This characteristic makes pagers vital for individuals like doctors who are often operating deep in hospital corridors or within reinforced rooms built to minimize x-ray exposure. However, pager technology predates the security and privacy era, and most common pager protocols do not make use of encryption. This allows for their data to be picked up by anyone with even a rudimentary radio set up.

It was from the NHS pagers that medical and healthcare data was being picked up and streamed online. The information being streamed, which included descriptions of "accidents, incidents and medical emergencies, often including patients' home addresses," was thankfully taken offline once the household the information was streaming from was contacted, but it is unknown for how long the stream was up, or who happened to come across it while it was up. When pressed about their knowledge of the insecurity of NHS pagers, several of the NHS trusts that operate them responded that they knew or were aware of the possibility this could happen.[3]

2. **Threats to Managed Service Providers Increase.** The ever-increasing complexity of modern technology, combined with the cost of running a fully resourced IT department, has been partially responsible for the growth of managed service providers ("MSPs"). Within the IT space, MSPs sell themselves as an efficient way to outsource the pain of configuring and managing networks, applications, and other critical functions. However, their success has made them a target for an increasing number of ransomware attacks, and there is some concern that many MSPs are not as proficient in cybersecurity as many of their clients may believe.[4]

   The growth of IT MSPs has made them more visible to malicious actors, and the knowledge that compromising an MSP can mean compromising dozens of clients has increased the incentive to target them. Cloud security provider Armor has been keeping track of publicly known attacks against MSPs and cloud-based service providers. Their most recent report puts the incident count at 13, with many coming in the last few months.[5] Notable MSP attacks include attacks against TSM Consulting, whose

[1] https://www.journalofhospitalmedicine.com/jhospmed/article/141692/hospital-medicine/hospital-based-clinicians-use-technology-patient-care?
[2] https://techcrunch.com/2019/10/30/nhs-pagers-medical-health-data

[3] https://techcrunch.com/2019/10/30/nhs-pagers-medical-health-data
[4] https://www.armor.com/blog/top-mistakes-managed-service-providers-msps-make-in-cyber-security/
[5] https://arstechnica.com/information-technology/2019/10/the-count-of-managed-service-providers-getting-hit-with-ransomware-mounts/

compromise affected 22 Texas municipalities in August, and PerCSoft, an MSP whose compromise "infected as many as 400 dental practices."[6]

3. **Are You Looking in the Wrong Places for Cyber Personnel?** Both the public and private sector have long lamented the shortage of cyber talent, but a new initiative from fifteen major technology companies looks to assess just how self-inflicted that shortage may be. The fifteen companies, including Google, Facebook, and Apple, have announced that they are altering their cybersecurity job descriptions and requirements. The changes represent an acknowledgement that requirements like a four-year bachelor's degree and gender-biased job descriptions may be inadvertently filtering out talented individuals.

   The thinking is summed up by the Aspen Institute's John Carlin in an interview with CyberScoop, "A bachelors degree is actually not a good proxy for whether you have the talent."[7] Essentially, these companies are looking to assess if the talent gap is more of a skills gap. They are betting that there are a significant number of individuals who have the talent but lack the skills or credentials to meet the job descriptions for many cybersecurity roles, or that feel put off by the way those jobs are described. Furthermore, beyond just refining the requirements and descriptions, many of these companies are investing in mentorship and internal development programs.[8]

   How successful this pivot in strategy may be is not yet certain, but few organizations can claim they have all the cybersecurity personnel they need to ensure secure operation, and at time when burnout among cybersecurity professionals from overwork is rampant, organizations should be open to exploring this model to find cybersecurity talent. Furthermore, this type of strategy can easily be adopted by organizations of all sizes, as it is not resource intensive. If you're struggling to find cybersecurity talent or lack the resources to acquire it using traditional methods, adopting innovative approaches may be necessary.

4. **Norsk Hydro Update.** The LockerGoga attack that crippled Norsk Hydro earlier this year has continued to make headlines as a test case for the evolving cyber insurance market. The most recent update came from the company's third quarter earnings report, and it appears that only $3.6 million of the total $60-70 million in damages has been paid out. While Norsk Hydro has never revealed how much it expected to receive from their policy, this is likely far less than they would have anticipated. Just after the attack Norsk

[6] https://www.armor.com/reports/new-msps-compromised-reports-armor/
[7] https://www.cyberscoop.com/cybersecurity-workforce-aspen-cybersecurity-group-apple-facebook-google/
[8] https://www.cyberscoop.com/cybersecurity-workforce-aspen-cybersecurity-group-apple-facebook-google/

Hydro publicly stated they had "a solid cyber risk insurance policy with recognized insurers, with global insurer AIG as lead."[9]

We have discussed his before, and you will recall that this is not the only high-profile cyber insurance case that has garnered a lot of attention as of late. Mondelez is currently in the process of suing its insurer for $100 million after they determined that Mondelez's losses were an act of war and therefore not covered by the policy.[10] While general consensus is that it better to have cyber insurance than to go without it, just remember to carefully inspect your policies to ensure you know what is covered. And be prepared to find that maybe you can't really be sure just yet.

Congress –

Tuesday, November 5th:
- No relevant hearings

Wednesday, November 6th:
- No relevant hearings

Thursday, November 7th:
- No relevant hearings

International Hearings/Meetings –

EU –

Wednesday, November 6th:
-European Parliament – Committee on Environment, Public Health and Food Safety

- Draft Agenda - Enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society

Friday, November 8th:
-European Commission - Expert Panel on Effective Ways of Investing in Health End of Mandate Conference: "Evidence-Based Expertise for Better Policy-Making"

Conferences, Webinars, and Summits –

--Maximize your Threat Sharing by Anomali – Webcast (11/6/2019)
https://h-isac.org/hisacevents/maximize-your-threat-sharing/
--CHIME Healthcare CIO Boot Camp – Phoenix, AZ (11/6/2019-11/9/2019)
https://h-isac.org/hisacevents/chime-healthcare-cio-boot-camp/
--Health IT Summit (Southwest) – Houston, TX (11/14/2019-11/15/2019)
https://endeavor.swoogo.com/2019-Dallas-Health-IT-Summit
--Southwest Healthcare Cybersecurity Forum – Dallas, TX(11/15/2019)
https://endeavor.swoogo.com/2019_Southwest_Cybersecurity_Forum
--Health IT Summit (Northwest) – Seattle, WA (11/19/2019-11/20/2019)

[9] https://www.reuters.com/article/norway-cyber/norsk-hydro-details-loss-from-cyber-attack-says-aig-lead-insurer-idUSL8N21D3WX
[10] https://www.theregister.co.uk/2019/01/11/notpetya_insurance_claim/

November 5th, 2019

https://endeavor.swoogo.com/2019-PacificNorthwest-HITSummit
--Pacific Northwest Healthcare Cybersecurity Forum – Seattle, WA (11/20/2019)
https://endeavor.swoogo.com/2019_Pacific_Northwest_Cybersecurity_Forum
Cyber Security & Data Protection Summit 2019 – London, UK (11/20/2019)
https://cybersecuritysummit.co.uk/
--2019 H-ISAC Fall Summit – San Diego, CA (12/2/19-12/6/2019)
https://h-isac.org/summits/fall-summit-2019/
--H-ISAC Security Workshop – London, UK (2/5/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-2/
-- H-ISAC Security Workshop - Cambridge, MA (4/7/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-cambridge-ma/

Sundries –

--A Chinese hacking group breached a telecom to monitor targets' texts, phone metadata
https://www.cyberscoop.com/chinese-hacking-group-breached-telecom-monitor-targets-texts-phone-metadata/
--A health care algorithm offered less care to black patients
https://arstechnica.com/science/2019/10/a-health-care-algorithm-offered-less-care-to-black-patients/
--Defense Innovation Board Lays Out 5 Key Principles for Ethical AI
https://www.nextgov.com/emerging-tech/2019/10/defense-innovation-board-lays-out-5-key-principles-ethical-ai/161008/
--Utah renewables company was hit by rare cyberattack in March
https://www.cyberscoop.com/spower-power-grid-cyberattack-foia/

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