August 25th, 2020

TLP White

This week, Hacking Healthcare is devoted to exploring the physical aspects of data security that, while sometimes easy to overlook, are no less important. This issue will examine the types of incidents members should consider, various legal and regulatory elements, the applicability of insurance, and what practical steps you can take to mitigate threats to physical data security.

Welcome back to *Hacking Healthcare*.

The physical aspects of data security. When we think of data breaches, most of us think of digital threats. Our minds immediately focus on exploited vulnerabilities and malicious cyber criminals based somewhere overseas. However, when it comes to securing data from unauthorized access and improper use, there are other considerations. From well-established threats such as natural disasters, to break-ins and lootings, there are numerous physical incidents that organizations should consider when assessing their responsibility to reasonably protect sensitive data.

Aren't these events uncommon?
While not as common as the everyday threat from malicious cyber actors, physical incidents have the potential to bring legal and regulatory burdens, and they happen more often than you might realize.

Below are just a few examples worth examining:

- **Walgreens**: In late July, it was reported that roughly 180 Walgreens locations suffered break-ins during May and June.[1] Theft of prescription drugs may not be surprising, but Walgreens also reported the theft of hard drives and paper records potentially containing "customers' health insurance and vaccination information," as well as photo ID numbers, contact information, and address information.[2, 3]

- **Cub Pharmacies**: Like Walgreens, Cub Pharmacies reported that six of its locations were looted during May. In a public notice, Cub Pharmacies acknowledged the "removal of locked safes, binders containing past prescription records, and prescription orders that were in the process of being completed."[4] In total, they estimated that "customer

names, addresses, prescription numbers, drug names, drug quantities, ordering physician names and addresses, number of refills remaining, prescription dates, and date of birth" information was compromised.[5]

- **Lifespan ACE**: At a time when so many individuals are working remotely, it is also important to consider the risk associated with the theft of employee devices. In February 2017, an employee of Lifespan ACE, a not-for-profit health system based in Providence, RI, had their laptop stolen from a parked car. According to HHS, the laptop, which was used for work purposes, "was never recovered… and [the] employee's work emails may have been cached in a file on the device's hard drive." Ultimately it was assessed that whoever had stolen the laptop would potentially have access to "patient names, medical record numbers, demographic information, including partial address information, and the name of one or more medications that were prescribed or administered to patients."[6] Resolving this issue with HHS ultimately cost Lifespan ACE over a million dollars.[7]

- **Natural Disasters**: Natural disasters are an unchanging reality that present a risk to the integrity of facilities while also creating opportunities for devices to be stolen or lost. This risk can come from a variety of situations, such as the required evacuation of personnel due to an encroaching wildfire or hurricane or a tornado that sweeps through a facility and leaves devices with PHI unaccounted for.

Regardless of the cause, accounting for physical risks to digital information is an essential aspect of overall cybersecurity risk management.

Action & Analysis

----SURVEY LINK HERE----

Congress –

Tuesday, August 25th:
- No relevant hearings

Wednesday, August 26th:
- No relevant hearings

Thursday, August 27th:
- No relevant hearings

August 25th, 2020

International Hearings/Meetings –

- No relevant hearings

EU –

Sundries –

New P2P botnet infects SSH servers all over the world
https://arstechnica.com/information-technology/2020/08/new-p2p-botnet-infects-ssh-servers-all-over-the-world/

FBI, CISA Echo Warnings on 'Vishing' Threat
https://krebsonsecurity.com/2020/08/fbi-cisa-echo-warnings-on-vishing-threat/

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

Conferences, Webinars, and Summits –
-- H-ISAC Monthly Member Threat Briefing – Webinar (8/25/2020)
https://h-isac.org/hisacevents/h-isac-monthly-member-threat-briefing-11/
-- STOP HEMORRHAGING DATA: MINIMIZE THIRD-PARTY RISK IN HEALTHCARE BY RISKRECON – Webinar (9/1/2020)
https://h-isac.org/hisacevents/stop-hemorrhaging-data-minimize-third-party-risk-in-healthcare-by-riskrecon/
--Healthcare Cybersecurity Forum – Southeast – Nashville, TN (9/9/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426517
-- ENISA Trust Services Forum - CA Day 2020 - Schloßplatz Berlin, Germany (9/22/2020)
https://h-isac.org/hisacevents/enisa-trust-services-forum-ca-day-2020/
--Healthcare Cybersecurity Forum – Northeast – Boston, MA (9/22/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/427126
--H-ISAC Cyber Threat Intel Training - Titusville, FL (9/22/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-titusville-fl/
--H-ISAC Security Workshop - Virtual (9/23/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-forchheim-germany/
--Summit on Security & Third Party Risk – National Harbor, MD (9/28/2020-9/30/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428840
--H-ISAC Monthly Member Threat Briefing – Webinar (9/29/2020)
https://h-isac.org/hisacevents/h-isac-monthly-member-threat-briefing-12/

August 25th, 2020

-- The MedTech Conference – Virtual (10/5/2020)
https://h-isac.org/hisacevents/the-medtech-conference-toronto/
-- Healthcare Cybersecurity Forum – Houston, TX (10/8/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428840
-- NCHICA AMC Security & Privacy Conference - Durham, North Carolina (10/21/2020-
10/22/2020)
https://h-isac.org/hisacevents/nchica-amc-security-privacy-conference/
-- 2020 H-ISAC European Summit - Santpoort-Noord, Netherlands (10/20/2020-10/22/2020)
https://h-isac.org/summits/european-2020-summit/
--CYSEC 2020 – Dubrovnik, Croatia (10/27/2020 – 10/28/2020)
https://h-isac.org/hisacevents/cysec-2020-croatia/
--Healthcare Cybersecurity Forum - Pacific Northwest – Seattle, WA (10/28/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428886
--H-ISAC Security Workshop - Seattle, WA – (10/29/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-seattle-wa-2/
--Healthcare Cybersecurity Forum – California – Los Angeles, CA (11/12/2020)
https://h-isac.org/hisacevents/healthcare-cybersecurity-forum-california-2/
--H-ISAC Security Workshop - Paris, France (11/18/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-paris-france/
--H-ISAC Fall Summit - Phoenix, AZ (11/30/2020-12/4/2020)
https://h-isac.org/summits/fall-summit-2020/
-- H-ISAC Security Workshop - Prague, Czech Republic (12/8/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-prague/
-- 2021 APAC Summit – Singapore (3/23/2021-3/25/2021)

[1] https://www.calhipaa.com/phi-exposed-due-to-break-ins-at-cvs-pharmacy-and-walgreens/
[2] https://www.cyberscoop.com/walgreens-robbery-health-data/
[3] https://oag.ca.gov/system/files/E_DL_L03.pdf
[4] https://www.cub.com/pharmacy/notice-of-data-incident.html
[5] https://www.cub.com/pharmacy/notice-of-data-incident.html
[6] https://www.hhs.gov/sites/default/files/lifespan-ra-cap-signed.pdf
[7] https://www.hhs.gov/sites/default/files/lifespan-ra-cap-signed.pdf