Table 1

Details of Ransomware Events in Healthcare Following the Hollywood Presbyterian Medical Center Incident

Date and Hospital	Data Affected	Action Taken	Source
February 10, 2016, Lukas Hospital, Neuss, Germany	Shutdown of all systems due to email attachment	No ransom paid; systems restored via backups and a few hours of data lost	Network Security Journal (2016)
February 12, 2016, Klinikum Arnsberg, North Rhine-Westphalia, Germany	Detected on one of 200 servers; network shut down to prevent infection	No ransom paid; systems restored via backups and a few hours of data lost	Network Security Journal (2016)
May 18, 2016, Kansas Heart Hospital, Wichita, KS	Files locked	Ransom paid (small undisclosed amount) but full access not restored; second ransom demanded but not paid	Jayanthi (2016)
March 14, 2016, Ottawa Hospital, Canada	Four computers encrypted	No ransom paid; data restored from backups	Pilieci, (2016)
March 18, 2016, Prime Health Care: Chino Valley Medical Center and Desert Valley Hospital, Victorville, CA	A number of computers and some hospital servers had locked data	No ransom paid; backups restored	Winton (2016)
March 21, 2016, Methodist Hospital, Henderson, KY	Critical files encrypted	No ransom paid; systems restored via backups	Landi (2016)
March 28, 2016, MedStar Health, Baltimore, MD (a 10-hospital system)	No breach of patient data, but email and clinical support systems were unavailable	45 bitcoin ransoms demanded ($19,000), but no ransom paid	Reed (2016)

Sources:

Jayanthi, Akanksha. "Kansas Heart Hospital Pays Ransom, Then Hackers Came Back for More." *Becker's Health IT and CIO Review*, May 23, 2016. Available at http://www.beckershospitalreview.com/healthcare-information-technology/kansas-heart-hospital-pays-ransom-then-hackers-came-back-for-more.html (accessed May 6, 2017).

Landi, Heather. "Kentucky-based Methodist Hospital's System Restored Following Ransomware Attack Last Week." *Healthcare Informatics*, March 21, 2016. Available at https://www.healthcare-informatics.com/news-item/kentucky-based-methodist-hospital-s-system-restored-following-ransomware-attack-last-week (accessed May 11, 2017).

Network Security Journal. "Ransomware Expands, Attacks Hospitals and Local Authorities, and Moves to New Platforms." *Network Security*, no. 3 (2016): 1–2.

Pilieci, Vito. "Ottawa Hospital Hit with Ransomware, Information on Four Computers Locked Down." *National Post*, March 13, 2016. Available at http://news.nationalpost.com/news/canada/ottawa-hospital-hit-with-ransomware-information-on-four-computers-locked-down (accessed May 11, 2017).

Reed, Tina. "MedStar Took 'Extreme' Measures to Block Cyber Threat." *Washington Business Journal*, March 29, 2016. Available at http://www.bizjournals.com/washington/news/2016/03/29/medstar-took-extreme-approach-to-block-security.html (accessed May 11, 2017).

Winton, Richard. "2 More Southland Hospitals Attacked by Hackers Using Ransomware." *Los Angeles Times*, March 22, 2016. Available at http://www.latimes.com/local/lanow/la-me-ln-two-more-so-cal-hospitals-ransomware-20160322-story.html (accessed May 11, 2017).