October 8th, 2019

Hacking Healthcare

TLP White

In this edition of Hacking Healthcare, we begin by reviewing the troubling news that 10 hospitals were impacted by ransomware last week. Next, we briefly explore why ransomware, despite constant presence in news headlines, is not as well understood as might be hoped. Finally, we examine a survey that strongly ties an organization's cybersecurity maturity to favorable valuations in mergers and acquisitions. Welcome back to *Hacking Healthcare*.

1. **Ransomware Hits Hospitals Again.** Ransomware hit the healthcare sector again last week, affecting hospitals in both the United States and Australia. Multiple hospitals in Alabama were forced to turn patients away a day after numerous Australian hospitals were impacted by ransomware that wreaked havoc on a regional computer network. In total, seven hospitals in Australia and three in Alabama had services severely limited. There has been no reported link between the attacks at this time.

   The three hospitals hit in Alabama were forced to turn away new patients with non-critical conditions after their computer systems were effectively paralyzed by the attack.[1] While operations were shifted to manual and paper based methods, efficiency was impacted, and the disruption forced the re-routing of non-critical patients to other nearby hospitals.[2] It is important to note that patients in this instance were lucky to be in an area with access to other healthcare providers. Individuals in more rural areas may not have had access to alternative healthcare options. Consequently, those populations may be at greater risk when it comes to cyberattacks on healthcare systems.[3]

   Recent reports on the incidents in Alabama have stated that Ryuk Ransomware, which has seen prolific usage in attacks this past year, is the malware behind the disruptions.[4] Furthermore, it was reported on October 5th that the Alabama hospitals paid the currently undisclosed ransomware demands to unlock their systems, but they expected to continue re-routing new patients throughout the weekend as they attempted to recover. There appears to be little sign of abatement in the ransomware epidemic hitting the United States. News of the Alabama hospital incidents came on the same day that anti-malware and anti-virus software provider EMSISOFT released their *State of Ransomware in the U.S.* report, which indicated that in the first nine months of this year at least 621 U.S. entities have been impacted by ransomware.[5]

The news was equally grim in Australia. Seven hospitals in Gippsland and southwest Victoria were impacted by ransomware that "blocked access to several systems by the infiltration of ransomware, including financial management" and forced them to "[isolate] and [disconnect] a number of systems… to quarantine the infection."[6] The incident led to delays for non-critical operations, but authorities from the country's Department of Premier and Cabinet were quick to allay fears that patient data had been compromised.[7] No new updates were available at the time of writing.

While there have not yet been any reports of loss of life resulting from the attack, the seriousness of cyberattacks impacting hospital operations cannot be overstated. While many hospitals are able to continue essential operations through such disruptions, efficiency and capacity are significantly reduced. The unfortunate side effect of being part of a critical industry sector like healthcare is the incentive for malicious actors to target you, expecting a quick pay day. Ten hospitals hit in quick succession, even if proven unrelated, is a disturbing confluence of incidents that at best represents a single actor knowingly targeting the vulnerable, and at worst, represents a trend of malicious actors openly normalizing such actions.

2. **Who wants to Report Ransomware?** One key to solving any problem is to have as close to a complete understanding of that problem as possible. Unfortunately, such a level of understanding is proving to be incredibly difficult when it comes to collecting data on how ransomware impacts the healthcare industry. Without a reliable data set to track ransomware trends, both generally and in healthcare specifically, formulating effective policies and ensuring proper resource allocation often becomes guesswork.

   Allan Liska from the cybersecurity company Recorded Future is making one of the first attempts to fill this void.[8] Liska dissected the Unites States' Health and Human Services (HHS) public database on breach notifications to find healthcare ransomware incidents between January 2015 and September 2019. In total, he found 117 incidents, averaging around 30 per year.[9] This finding is significantly less than was expected. Additionally, "69 of the incident reports (61%) confirmed the victim did not pay a ransom, 17 of the tracked incidents (15%) confirmed payment, and the rest were unknown."[10] This is noteworthy because it illustrates that, even when an incident is reported, basic information such as whether a payment was made is often lacking. This insight is noted in Liska's conclusion that healthcare ransomware incidents are likely underreported and official records are often incomplete.[11]

   Liska's efforts, which are available in a downloadable appendix on Recorded Future's website, are a useful first step in quantifying the issue, but the underlying causes of underreporting remain. The healthcare industry is well aware of the scrutiny regulators place on them and the financial and reputational costs associated with cybersecurity incidents. These realities provide hefty incentives to only disclose what is required by law, which often discounts ransomware incidents where patient data is not compromised. This paradoxical situation makes it difficult to measure if ransomware attacks on healthcare are on the rise, if payments are increasing, or if investment in tackling this issue is effective.

3. **Organizational Cybersecurity Maturity Impacts Monetary Value.** A new survey conducted by (ISC)2, the International Information System Security Certification Consortium, concludes that cybersecurity readiness is a key factor that is assessed during merger and acquisition (M&A) negotiations.[12] According to the ISC(2) survey, increased attention is being paid to all aspects of an organization's cybersecurity posture and history, and organizations need to be wary of overlooking warning signs that could lead to a devaluation after being purchased or merged.[13] A few key takeaways are listed below.

   Cybersecurity audits appear to be standard practice at this point, with 100% of survey respondents claiming that they expect to see them during an M&A process.[14] Additionally, failing to be forthright with a potential buyer when it comes to cybersecurity can lead to negotiations breaking down completely, with 49% of participants indicating they had seen such a lack of openness derail negotiations.[15] A further 77% of respondents claimed that they had "made recommendations on whether to proceed with an M&A deal based on the strength of the target company's cybersecurity program." And finally, a resounding 95% of survey participants consider cybersecurity programs to be tangible assets, with 82% asserting that robust cybersecurity infrastructure and policies raised the value of an organization.[16]

   This survey represents yet another example of why cybersecurity programs must receive adequate resources and attention. By calling out the importance of cybersecurity in the M&A process, and by outlining how a strong cybersecurity posture can increase the valuation of an organization, the ISC(2) survey shows that cybersecurity must be thought of as an important component of the whole business. Organizations should already be in the habit of conducting internal cybersecurity audits, but if you need another reason to budget for one, the potential to raise your organization's value may be a compelling one.

Congress –

Tuesday, October 8th:
-No relevant hearings

Wednesday, October 9th:
-No relevant hearings

Thursday, October 10th:
-No relevant hearings

October 8th, 2019

International Hearings/Meetings –

EU – None This Week

Conferences, Webinars, and Summits –

--H-ISAC Grand Rounds Webinar Series #1: Cost Effective Threat Intel – Webinar (10/9/2019)
https://h-isac.org/hisacevents/h-isac-grand-rounds-webinar-series-1-cost-effective-threat-intel/
--2019 H-ISAC European Summit – Zurich, Switzerland (10/16/2019-10/17/2019)
https://h-isac.org/summits/european_summit/
--Health IT Summit (Midwest) – Minneapolis, MN (10/17/2019-10/18/2019)
https://endeavor.swoogo.com/2019-Minneapolis-Health-IT-Summit
--Healthcare Cybersecurity Forum (Midwest) – Minneapolis, MN (10/18/2019)
https://endeavor.swoogo.com/2019_Midwest_Cybersecurity_Forum
--H-ISAC / MITSF Healthcare Cybersecurity Workshop – Tokyo, Japan (10/24/2019)
http://www.cvent.com/events/h-isac-mitsf-healthcare-cybersecurity-workshop/event-summary-21a9794745bf41c4bb55ba9dd29dc256.aspx
H-ISAC Security Workshop – Titusville, FL (11/4/2019)
https://h-isac.org/hisacevents/h-isac-security-workshop/
--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)
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
--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
https://h-isac.org/hisacevents/h-isac-security-workshop-2/

Sundries –

--Microsoft: U.S. presidential campaign, government officials targeted by recent hacking effort
https://www.cyberscoop.com/iran-microsoft-2020-elections/
--NHSX will not develop new standards, says senior tech advisor
https://www.healthcareitnews.com/news/europe/nhsx-will-not-develop-new-standards-says-senior-tech-advisor
--Egypt used Google Play in spy campaign targeting its own citizens, researchers say
https://arstechnica.com/information-technology/2019/10/egypt-used-google-play-in-spy-campaign-targeting-its-own-citizens-researchers-say/
--Chinese-linked hacking group gets crafty to avoid detection
https://www.cyberscoop.com/rancor-group-check-point-phishing-emails/

October 8th, 2019

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

[1] https://arstechnica.com/information-technology/2019/10/hamstrung-by-ransomware-10-hospitals-are-turning-away-some-patients/

[2] https://www.foxnews.com/tech/alabama-hospitals-ransomware-attack

[3] https://arstechnica.com/information-technology/2019/10/hamstrung-by-ransomware-10-hospitals-are-turning-away-some-patients/

[4] https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/ryuk-attacks-3-hospitals/

[5] https://blog.emsisoft.com/en/34193/state-of-ransomware-in-the-u-s-2019-report-for-q1-to-q3/

[6] https://www.vic.gov.au/cyber-health-incident

[7] https://www.theguardian.com/australia-news/2019/oct/01/systems-shut-down-in-victorian-hospitals-after-suspected-cyber-attack

[8] https://www.cyberscoop.com/ransomware-healthcare-recorded-future/

[9] https://www.recordedfuture.com/healthcare-ransomware-attacks/

[10] https://www.recordedfuture.com/healthcare-ransomware-attacks/

[11] https://www.cyberscoop.com/ransomware-healthcare-recorded-future/

[12] https://www.isc2.org//-/media/ISC2/Research/The-ROI-of-Sound-Cybersecurit-Programs/MAcybersecuritySurveyReportvF92019.ashx

[13] https://www.isc2.org//-/media/ISC2/Research/The-ROI-of-Sound-Cybersecurit-Programs/MAcybersecuritySurveyReportvF92019.ashx

[14] https://www.isc2.org//-/media/ISC2/Research/The-ROI-of-Sound-Cybersecurit-Programs/MAcybersecuritySurveyReportvF92019.ashx

[15] https://www.isc2.org//-/media/ISC2/Research/The-ROI-of-Sound-Cybersecurit-Programs/MAcybersecuritySurveyReportvF92019.ashx

[16] https://www.isc2.org//-/media/ISC2/Research/The-ROI-of-Sound-Cybersecurit-Programs/MAcybersecuritySurveyReportvF92019.ashx