Health-ISAC Weekly Blog -- Hacking Healthcare

| Hacking Healthcare | ◯ TLP:WHITE | Alert ID : 7c869c16 | May 25, 2023, 10:35 AM |

This week, *Hacking Healthcare* takes a look at a study recently published in the Journal of the American Medical Association (JAMA) that sought to understand the wider impact that cyberattacks have on regional healthcare facilities adjacent to the actual victim. The study appears to confirm what many Health-ISAC members already know: The impacts of cyberattacks radiate outward, and the harm they cause is likely not fully understood.

Welcome back to *Hacking Healthcare*.

The Community-Wide Impact of Ransomware Attacks on Healthcare Delivery Organizations

While we know that cyberattacks affecting healthcare delivery organizations (HDOs) result in tangible negative effects on services and patient outcomes, the body of evidence is still relatively small, and most studies are relatively new. Even less well documented is how cyberattacks at one healthcare facility reverberate outward and impact the wider community. A recent study published in JAMA has taken a stab at illustrating the wider harm that cyberattacks can cause, and its authors have some suggestions for what their findings mean.

Published on May 8, *Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US* assessed two "academic urban emergency departments (EDs) adjacent to a health care delivery organization under a month-long ransomware attack."[i] The authors of the study assessed a variety of metrics based on nearly 20,000 ED visits that occurred prior to the ransomware attack, during the attack, and in the aftermath of the attack at these two locations.

Ultimately, the authors found that "[d]uring the attack and postattack phases, significant increases in patient census, ambulance arrivals, waiting room times, patients left without being seen, total patient length of stay, county-wide emergency medical services diversion, and acute stroke care metrics were seen in the unaffected ED."[ii] In addition, the authors noted an "[increase] in stroke code alerts, stroke diagnoses, and acute treatments with tPA and endovascular treatments during the cyberattack and recovery." some of the more notable numbers included a:[iii]

- 127.8% increase in visits where patients left without being seen
- 50.4% increase in visits where patients left against medical advice

- 47.6% increase in median waiting room times

The authors conclude that these findings "support the need for coordinated regional cyber disaster planning, further study on the potential patient care effects of cyberattacks, and continued work to build technical health care systems resilient to cyberattacks such as ransomware."[iv]

Action & Analysis
Included with Health-ISAC Membership

Congress

Tuesday, May 23
No relevant hearings

Wednesday, May 24
No relevant meetings

Thursday, May 25
No relevant hearings

International Hearings/Meetings
No relevant meetings

John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.

[i]https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2804585?
utm_source=For_The_Media&utm_medium=referral&utm_campaign=ftm_links&utm_term=050823
[ii]https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2804585?
utm_source=For_The_Media&utm_medium=referral&utm_campaign=ftm_links&utm_term=050823
[iii]https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2804585?
utm_source=For_The_Media&utm_medium=referral&utm_campaign=ftm_links&utm_term=050823
[iv]https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2804585?
utm_source=For_The_Media&utm_medium=referral&utm_campaign=ftm_links&utm_term=050823
[v]https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2804585?
utm_source=For_The_Media&utm_medium=referral&utm_campaign=ftm_links&utm_term=050823
[vi] [i] https://www.censinet.com/ponemon-report-covid-impact-ransomware

---

Reference | References

jamanetwork
censinet
Health-ISAC

Hacking Healthcare:

Written by John Banghart, who served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.

Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.