Hacking Heathcare - Weekly Blog

Hacking Healthcare | TLP:WHITE | Alert ID : fae0390a | Oct 15, 2024, 08:38 AM

This week, Health-ISAC®'s Hacking Healthcare® examines a healthcare data breach that highlights how exfiltrated data like medical imagery can create serious complications for entities working through incident response and ransom demands. In addition, we raise awareness around the cybersecurity risks associated with the mergers and acquisition process in the healthcare sector.

Welcome back to Hacking Healthcare®.

Healthcare Data Breach Reiterates Complexity of Incident Response

A United States-based healthcare entity has made progress toward settling a lawsuit related to a data breach from last year that led to the exposure of a large quantity of sensitive patient images. The fallout from the incident highlights the incredibly difficult legal and regulatory position that healthcare entities continue to find themselves in.

What happened?

In early 2023, a United States-based healthcare organization recognized unauthorized activity in its IT systems. An investigation revealed that a Russian-aligned malicious cyber actor had accessed a system containing sensitive patient information that included a large quantity of patient images. The malicious cyber actor was able to exfiltrate a sizeable amount of data, including the images, and then attempted to extort the healthcare organization. It appears that in an attempt to pressure the victim organization to pay, the malicious cyber actor began publicly leaking data that included these sensitive images.

The victim organization determined it would not pay the ransom demand, and as part of its incident response, law enforcement was notified, cyber incident response firms were brought in, and the organization notified affected individuals.

In the wake of these actions, a class action lawsuit was brought against the healthcare organization by patients affected by the incident. The lawsuit claimed that there were insufficient security protections in place to protect such sensitive information, that the healthcare organization should have known it was a likely target, and that not paying the ransom and allowing the images to be leaked publicly was harmful to the patients.

Lawsuit

The most recent update suggests that a settlement is likely between both parties. While the proposed terms have yet to be accepted by the court, it would appear likely, given the reported settlement amount. If reported figures are accurate, the settlement would cost many times more than the initial ransom demand.

Action & Analysis

****Included with Health-ISAC Membership****

While the above recommendations are mostly applicable to the larger entity making an acquisition or the one leading a merger, it is important to highlight the position of the target of an acquisition, or lesser partner in a merger. While legal and business considerations can create limitations or disincentives to be aggressively forthright regarding your organization's cybersecurity, we would urge you to remember that the clarity you provide on these matters impacts patient health and safety. We would urge you to consider sharing relevant cybersecurity information to the greatest extent practical under these conditions.

[i] https://www.theguardian.com/technology/2017/may/31/hackers-publish-private-photos-cosmetic-surgery-clinic-bitcoin-ransom-payments

[ii] https://www.8newsnow.com/investigators/hackers-target-las-vegas-plastic-surgeons-post-patient-information-naked-photos-online/

[iii] https://www.thedailybeast.com/hackers-steal-photos-from-plastic-surgeon-to-the-stars-claim-they-include-royals

[iv] https://www.wired.com/story/vastaamo-psychotherapy-patients-hack-data-breach/

[v] https://www.darkreading.com/cyber-risk/hackers-weaponize-sec-disclosure-rules-against-corporate-targets

Report Source(s)

Health-ISAC

Release Date

Oct 15, 2024, 11:59 PM

Reference | References

8newsnow
thedailybeast
The Guardian
Wired
Dark Reading

Tags

M&A, Mergers & Acquisitions, Hacking Healthcare, Incident Response, Ransomware

Conferences, Webinars, and Summits:

https://h-isac.org/events/

Hacking Healthcare:

Hacking Healthcare is co-written by John Banghart and Tim McGiff.

John Banghart has served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Councils 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 Councils 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.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISACs annual Hobby Exercise and provides legal and regulatory updates for the Health-ISACs monthly Threat Briefing.

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

Share Threat Intel:

For guidance on sharing indicators with Health-ISAC via HTIP, please visit the Knowledge Base article "HTIP - Share Threat Intel" here.

The "Share Threat Intel" feature allows for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Access the Health-ISAC Threat 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 Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments:

Please email us at toc@h-isac.org