Health-ISAC™
SHARING SINCE 2010
Collaborating for Resilience in Healthcare

# Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare ○ TLP:WHITE Alert ID : 39ef9454 Jan 26, 2024, 06:45 PM

This week, *Hacking Healthcare*$^{\text{TM}}$ examines a trilateral sanction action against one of the alleged perpetrators of the cyberattack against Australian healthcare insurer Medibank. We provide some background on the recent government sanctions response and then delve into some takeaways and potential ramifications.

Welcome back to *Hacking Healthcare*$^{\text{TM}}$.

**U.S. and U.K. Stand in Sanction Solidarity with Australia for Medibank Cyberattack**

The 2022 ransomware attack against Australian healthcare insurer Medibank was a shock for many. Current estimates of the attack suggest upwards of 9.7 million records stolen, including names, dates of birth, and sensitive medical information, such as "records on mental health, sexual health and drug use."[i] The Australian government has confirmed that at least some of these records ended up on the dark web.[ii]

Since the attack came to light, the Australian government and various international partners have been working to assess the attack and determine attribution. This 18-month investigation culminated this week with the Australian government placing sanctions on a Russian national Aleksandr Ermakov for his role in the cyberattack.[iii]

The sanction includes "a targeted financial sanction and a travel ban" and "makes it a criminal offence, punishable by up to 10 years' imprisonment and heavy fines, to provide assets to Aleksandr Ermakov, or to use or deal with his assets, including through cryptocurrency wallets or ransomware payments."[iv] Australian Minister for Foreign Affairs, Penny Wong, has stated that "[t]he use of these powers sends a clear message—there are costs and consequences for targeting Australia and Australians" and that "[Australia's] Albanese Government will continue to hold cybercriminals to account."[v]

U.S. & U.K. Stand in Sanction Solidarity

Strikingly, despite the victim organization and individuals of the Medibank attack being largely Australian, both the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) and the U.K.'s Foreign, Commonwealth & Development Office immediately placed similar sanctions on Ermakov.

According to U.S. Under Secretary of the Treasury, Brian E. Nelson, this trilateral sanction action is the first of its kind and “underscores our collective resolve to hold these criminals to account.”[vi] The sanction action was justified on the grounds that Ermakov presents a similar risk to both the U.S. and the U.K. The sanction actions by the U.K. and U.S. introduce similar restrictions and asset freezes, as Australia and representatives of both governments were quick to suggest that these types of efforts are likely to continue.[vii]

***Action & Analysis***

**Available with Health-ISAC Membership**

***Congress***

Tuesday, January 23

No relevant hearings

Wednesday, January 24

No relevant meetings

Thursday, January 25

No relevant meetings

***International Hearings/Meetings***

No relevant meetings

***EU***

[i] https://www.gov.uk/government/news/uk-and-allies-sanctions-russian-cyber-hacker
[ii] https://www.foreignminister.gov.au/minister/penny-wong/media-release/cyber-sanctions-response-medibank-private-cyber-attack
[iii] https://www.foreignminister.gov.au/minister/penny-wong/media-release/cyber-sanctions-response-medibank-private-cyber-attack
[iv] https://www.foreignminister.gov.au/minister/penny-wong/media-release/cyber-sanctions-response-medibank-private-cyber-attack
[v] https://www.foreignminister.gov.au/minister/penny-wong/media-release/cyber-sanctions-response-medibank-private-cyber-attack
[vi] https://home.treasury.gov/news/press-releases/jy2041
[vii] https://www.gov.uk/government/news/uk-and-allies-sanctions-russian-cyber-hacker
[viii] https://www.foreignminister.gov.au/minister/penny-wong/media-release/cyber-sanctions-response-medibank-private-cyber-attack
[ix] https://ofac.treasury.gov/media/912981/download?inline

**Report Source(s)**

Health-ISAC

**Reference | References**

Gov.UK
foreignminister
treasury
treasury

**Tags**

Medibank, OFAC, Hacking Healthcare, Sanctions Policy, International Collaboration, Sanctions, Information Sharing, law

**TLP:WHITE:** Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

**For Questions and/or Comments:**
Please email us at contact@h-isac.org

**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 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.

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

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

**For Questions or Comments:**

Please email us at toc@h-isac.org