Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare™ | TLP:WHITE | Alert ID : 7e560429 | Feb 16, 2024, 03:03 PM

With the Health-ISAC APAC Summit just around the corner (more information below) we thought we would highlight a couple of things happening in that region. We'll start with a quick look at some cloud security related news in South Korea. Then we'll pop down to Australia for a more in depth look at how the Australian government is working to address cyber information sharing protections and how the private sector may be able to help shape their approach through an open consultation.

Welcome back to *Hacking Healthcare*™.

Health-ISAC APAC Summit

Before we jump in, we would like to remind you of the upcoming Health-ISAC APAC Summit that is being hosted in Melbourne, Australia from March 19-21. For those still undecided on attending, we would encourage you to take advantage of this opportunity to meet the Health-ISAC team and your fellow colleagues in what is always a fantastic learning and networking experience. Registration closes February 18th.

https://h-isac.org/summits/2024-apac-summit/

Korean Cybersecurity Requirements

Recently, the Republic of Korea's Ministry of Science and ICT made a decision to partially revise their "Notice on Cloud Computing Service Security Certification", which reflects the high and middle tier evaluation criteria of the cloud security certification rating system. As with the EU Cloud Scheme A, the proposed amendments include language that would require the location of cloud systems and data be limited to the Republic of Korea, making it difficult for US companies to comply.[i] In general, data localization has long been seen as detrimental to mutual cybersecurity and national security goals, particularly between countries that have a long history of cooperation. If you are engaged with any cloud services in the Republic of Korea, you may want to consider submitting comments expressing your concerns. The comment period closes on February 26th, so you don't have much time.

Even if you aren't concerned about the Republic of Korea specifically, this global trend doesn't bode well for us-based tech companies and the many global healthcare entities that rely on them. We'll keep an eye on how this progresses and report back.

Australia Considers Cyber Information Sharing Protections

Information sharing protections have been a popular topic of discussion in policy circles over the past few years as cyber incident reporting has become increasingly pervasive globally. While some countries have found a measure of success in this area, such as the United States' Cyber Security Information Sharing Act of 2015 (CISA 2015), others are in the midst of finding a balance between incentivizing reporting and not undercutting regulators and the general public's expectation that entities be held to account for lax security.

2023-2030 Australian Cyber Security Strategy

The most recent development on this issue can be found in the current national cyber strategy. Released late in November of last year, the 64-page 2023-2030 Australian Cyber Security Strategy is a broad document outlining a layered strategy to protect Australian citizens and infrastructure.[ii] Among the six "shields" that make up the strategy, Shield one "Strong Businesses and Citizens" identified the need to "make it easier for Australian businesses to access advice and support after a cyber incident."[iii] One of the core issues flagged by this section is what is referred to as industry's reluctance "to share detailed and timely cyber incident information," due in part to concerns that information shared with the government could end up being used against them in regulatory actions.[iv] The strategy notes that this reluctance hampers the government's ability to understand the cyber threat environment and to provide aid to victims.

In an effort to improve this information sharing deficiency and quell fears of follow-on regulatory action, the Australian government cited the desire to develop a "limited use obligation" that would "aim to limit how information that industry shares with [the Australian Signals Directorate (ASD) and the Cyber Coordinator][v] can be used by other Australian Government entities, including regulators."[vi]

Put more simply, information shared with ASD or the Cyber Coordinator could not then be used by regulators or others to take action against the entity. Information provided would only be able to be used for proscribed cyber security purposes. However, the strategy explicitly states that the mechanism would not be intended to broadly restrict regulatory or law enforcement action and it would not provide broad immunity from legal liability.

Consultation on Proposed Reforms

The limited use obligation idea proposed in the Australian Cyber Strategy was then expanded upon in a 64-page follow up consultation.[vii] This follow-up provides a summary of private sector feedback on the issue and interim measures being taken by the government, provided clarification on the potential for a "safe harbor" approach, and called for private sector feedback to help better shape the eventual limited use legislative mechanism.

Initial Feedback: According to the consultation, private sector feedback on the idea of limiting the use of, or ability to share, information provided to ASD and the Cyber Coordinator was broadly positive. A number of respondents even referenced the CISA 2015 "as a model to consider."[viii]

Interim Measure: The government does not appear eager to wait for an eventual legislative mechanism to improve matters. The consultation makes clear that the government is already "exploring a non-legislative limited use obligation for ASD ahead of the proposed legislative reform…on an accelerated timeframe."[ix]

Safe Harbor vs Limited Use: Reiterating their reluctance to provide broad protections against legal liability from the initial Australian Cyber Strategy, the consultation stresses that they prefer a limited use obligation.

Seeking Feedback: The Australian government currently has an open consultation that closes on 5pm AEDT, Friday 1 March 2024. A primary topic of interest to the government is "what functions should be included in the definition of 'prescribed cyber security purposes' for the sharing and use of incident information."[x] Additional questions include "What restrictions, if any, should apply to the sharing of cyber incident information?" and "What else can government do to promote and incentivize entities to share information and collaborate with ASD and the Cyber Coordinator in the aftermath of a cyber incident?"[xi]

Action & Analysis
Included with Health-ISAC Membership

Congress
Tuesday, February 13
No relevant hearings

Wednesday, February 14
No relevant meetings

Thursday, February 15
No relevant meetings

International Hearings/Meetings
No relevant meetings
EU

[i] https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme
[ii] https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf
[iii] https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf
[iv] https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf
[v] The Cyber Coordinator has the responsibility to lead the coordination and triaging of government action in response to a major cyber incident and the ASD is the lead government entity that works with government and industry to detect and respond to incidents and threats to critical infrastructure.

[vi] https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf
[vii] https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2023-30-consultation-paper.pdf
[viii] https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2023-30-consultation-paper.pdf
[ix] https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2023-30-consultation-paper.pdf
[x] https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2023-30-consultation-paper.pdf
[xi] https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2023-30-consultation-paper.pdf
[xii] https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2023-30-consultation-paper.pdf

Report Source(s)

Health-ISAC

Release Date

Feb 16, 2024, 11:59 PM

Reference | References

Europa Analytics
Health-ISAC Webinar Playback
homeaffairs
homeaffairs

Tags

Liability, Regulation, Hacking Healthcare, Information Sharing, APAC, cloud, Australia, Korea

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.

Share Threat Intel:

For guidance on sharing indicators with Health-ISAC via CSAP, please visit the Knowledge Base article CSAP "Share Threat Intel" Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base Additionally, this collaborative medium provides opportunities for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

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