Health-ISAC Weekly Blog -- Hacking Healthcare®

Hacking Healthcare | TLP:WHITE | Alert ID : 23996ee3 | Aug 26, 2024, 03:31 PM

This edition of Hacking Healthcare® evaluates a new and significant international cybercrime initiative making progress at the United Nations (U.N.). We explore where this initiative came from, who supports it, and why it may not be as beneficial for cracking down on cybercrime as its name might suggest. Next, we briefly outline what might be expected from a reorganization within the United States' Department of Health and Human Services.

Welcome back to Hacking Healthcare®.

What to Make of the New U.N. Convention Against Cybercrime

In May of last year, Hacking Healthcare® provided an update on a multi-year effort to create a United Nations (U.N.) cybercrime convention.[1] [2] Roughly fifteen months later, the controversial convention has cleared a major hurdle and appears to be on its way to be accepted by the U.N. General Assembly later this year. Let's explore the backstory for this convention and examine why it may not be the positive outcome its name might suggest.

Why Create a U.N. Cybercrime Convention?

While calculating the full effect of global cybercrime remains impossible, attempts at contextualizing its impact have suggested that the cost to the global economy may be around $10 trillion.[3] [4] Unsurprisingly, that creates quite an incentive for governments around the world to find common ground toward addressing the issue. What might surprise you is that the international community's interest in building consensus policy approaches for cybercrime goes much further back than the relatively recent rise of ransomware and the mature cybercrime ecosystem we know today.

Back in November of 2001, an effort led by the Council of Europe[5] ended with the creation of the Budapest Convention on Cybercrime.[6] This convention has helped to create a shared international understanding of cybercrime, provided guidance for the harmonization of domestic legal approaches to cybercrime among parties to the convention, and has facilitated international cooperation on transnational cybercrime issues. Since 2001 it has added protocols to expand its scope and currently boasts 76 parties to the convention, including representation from every continent.[7] [8]

While the Budapest Convention has been successful, it has faced criticisms that have limited its global adoption. Most prominently is the feeling that the development of the convention was not a truly global endeavor and that the process was dominated by Europe and the "West's" conception of cybercrime. Many developing economies, and even several major economies like India and Brazil, had limited to no input. These governments have generally been hesitant to accede to a convention that may not adequately reflect their views. Along those lines, Russia and China have also rejected the convention as they generally disagree with certain aspects of its approach, and they have cited concerns that it would violate their state sovereignty.

These criticisms opened the door for Russia to pursue the creation of a convention within the truly global context of the U.N. It has also allowed them to ensure that its approach is far more aligned with their perspective and policy objectives. This process started in 2017 and appears to be heading toward a conclusion with the recent unanimous adoption of the current text by the U.N. Ad Hoc Committee on Cybercrime on August 8.[9] It is now expected to go to the General Assembly for a vote this fall.

Action & Analysis

Included with Health-ISAC Membership

Cybersecurity Likely to Benefit From HHS Reorganization

Toward the end of July, the United States Government's Department of Health and Human Services (HHS) announced an internal reorganization that, in their words, "will streamline and bolster technology, cybersecurity, data, and artificial intelligence (AI) strategy and policy functions."[13] Let's explore these changes in more depth and analyze how they may affect the healthcare sector in the United States.

What is Changing and Why?

The major changes in structure and responsibility are described by HHS as:[14]

- The Office of the National Coordinator for Health Information Technology (ONC) will be renamed the Assistant Secretary for Technology Policy and Office of the National Coordinator for Health Information Technology (ASTP/ONC);

- Oversight over technology, data, and AI policy and strategy will move from the Assistant Secretary for Administration (ASA) to ASTP/ONC, including the HHS-wide roles of Chief Technology Officer, Chief Data Officer, and Chief AI Officer; and

- The public-private effort between the health sector and the federal government on cybersecurity (405(d) Program) will move from ASA to the Administration for Strategic Preparedness and Response (ASPR), joining the other health sector cybersecurity activities already located in ASPR's Office of Critical Infrastructure Protection and advancing the Department's one-stop-shop approach to healthcare cybersecurity.

According to HHS, this reorganization will "clarify and consolidate" the above critical functions with the expectation that centralizing cybersecurity and technology strategy and policy should create better efficiency.

Action & Analysis

Included with Health-ISAC Membership

[1] https://h-isac.org/health-isac-hacking-healthcare-5-4-2023/

[2] It may be referred to as *United Nations convention against cybercrime: Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes*

[3] https://www.economist.com/graphic-detail/2024/05/17/unexpectedly-the-cost-of-big-cyber-attacks-is-falling

[4] https://www.forbes.com/sites/forbestechcouncil/2023/02/22/105-trillion-reasons-why-we-need-a-united-response-to-cyber-risk/

[5] https://www.coe.int/en/web/about-us/who-we-are

[6] https://www.coe.int/en/web/cybercrime/the-budapest-convention

[7] Excluding Antarctica

[8] https://www.coe.int/en/web/cybercrime/parties-observers

[9]https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Documents/AC_291_L15_ADVANCE_UNEDITED.pdf

[10]https://www.euractiv.com/section/law-enforcement/opinion/the-un-cybercrime-convention-is-a-victory-for-digital-authoritarianism/

[11]https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Documents/AC_291_L15_ADVANCE_UNEDITED.pdf

[12] https://www.eff.org/deeplinks/2024/06/if-not-amended-states-must-reject-flawed-draft-un-cybercrime-convention

[13]https://www.hhs.gov/about/news/2024/07/25/hhs-reorganizes-technology-cybersecurity-data-artificial-intelligence-strategy-policy-functions.html

[14]https://www.hhs.gov/about/news/2024/07/25/hhs-reorganizes-technology-cybersecurity-data-artificial-intelligence-strategy-policy-functions.html

[15] https://aspr.hhs.gov/newsroom/Pages/405d-Transition-25July2024.aspx

[16] https://aspr.hhs.gov/newsroom/Pages/405d-Transition-25July2024.aspx

Report Source(s)

Health-ISAC

Release Date

Aug 26, 2024, 11:59 PM

Reference | References

coe
Euractiv
HHS
coe
coe
economist

EFF
Health-ISAC
unodc
HHS

Tags

U.N., Hacking Healthcare, Geopolitics, Cybercrime, FDA, Policy, United Nations, HHS, cybersecurity

---

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 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.

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).