August 10th, 2021

TLP White

This week, *Hacking Healthcare* begins by describing the most recent developments related to the creation of a Bureau of Cyber Statistics and what they might mean for the healthcare sector. Next, we reiterate how important it is to be aware of your cyber-physical systems, especially systems not typically associated with having a cyber component. Finally, we wrap up with a breakdown of Russia's new cybercrime proposal in the United Nations and how it remains at odds with Western approaches. Welcome back to *Hacking Healthcare*.

1. **More Support for Cyber Statistics Bureau**

   In a speech at the beginning of this month, National Cyber Director Chris Inglis made it known that he supports the creation of a Bureau of Cyber Statistics.[1] His high-profile support for this bureau boosts the possibility that one of the key recommendations from the bi-partisan Cyberspace Solarium Commission will get the backing of the White House, which should help drive forward legislation aimed at bringing the idea of the Bureau of Cyber Statistics to fruition.

   Inglis echoed the Solarium Commission report's assertion that "the U.S. government and broader marketplace lack sufficient clarity about the nature and scope of [cyber] attacks to develop nuanced and effective policy responses."[2] He stated that the absence of information, such as "where [cyber risk] is concentrated, where it cascades, [and] what causes it" results in uneven and likely less than optimal responses. While his position on the issue isn't surprising given that he served as a member of the Cyberspace Solarium Commission, his appointment as the United States' first National Cyber Director should give the notion additional clout and may help push the White House to adopt a position of formal support.[3]

   While the Executive Branch continues to consider their official position on the issue of creating a Bureau of Cyber Statistics, some members of Congress have been actively pursuing its creation. At the end of July, Senators Angus King (I-ME), Mike Rounds (R-SD), and Ben Sasse (R-NE) announced the release of their *Defense of United States Infrastructure Act*.[4]

   Among its many items, the bill would establish the Bureau of Cybersecurity Statistics within the Department of Homeland Security to "drive insights into what works and

what doesn't to mitigate critical cybersecurity risk to businesses, government, and the American people."[5] Some of the more notable aspects of that section include:

- A very broad definition of "Cyber Incident"
- An open-ended scope to "collect and analyze information concerning cybersecurity, including…any other area the Director determines appropriate"
- A requirement to work with NIST in recommending national standards, metrics, and measurement criteria for cyber statistics
- A requirement that covered entities submit a report to the Bureau every 180 days "containing such data and information as the Director determines necessary"
- Some legal and regulatory protection for entities disclosing information and entities where incidents initially occurred

Action & Analysis
Included with H-ISAC Membership

2. Pneumatic Tubes Highlight Cyber-Physical Risk

Part of the challenge to properly securing the complex and often sprawling IT environment that exists within a hospital is knowing all the systems that could potentially be compromised by a cyberattack. This challenge can be exacerbated by the amount of physical systems that many people wouldn't ordinarily expect to have cyber/internet enabled aspects. A prominent example of this risk was highlighted last week centering around pneumatic tubing.

In a report published by security vendor Armis, nine critical vulnerabilities were identified in the Translogic Pnuematic Tube System (PTS) by Swisslog Healthcare.[6] For those not familiar, a PTS is commonly used by hospitals to send medications, samples, and other material items safely and quickly throughout a hospital. The compromise of such a system could lead to items being rerouted or damaged.

The criticality of this discovery is heightened by the assertion that "over 80% of hospitals in North America" and "3,000 hospitals worldwide" use Swisslog Healthcare's pneumatic tube system (PTS) solution.[7] The set of vulnerabilities that was identified would allegedly allow "an unauthenticated attacker to take over Translogic PTS stations and essentially gain complete control over the PTS network of a target hospital."[8]

There is no known evidence that any of these vulnerabilities have been exploited, and Swisslog has since reportedly created a patch for all but one of the vulnerabilities and has released mitigations for the remaining one.[9]

For more information, read the H-ISAC bulletin at: https://h-isac.org/armis-discovers-9-vulnerabilities-in-infrastructure-used-by-80-of-major-hospitals-in-north-america/

Action & Analysis
Included with H-ISAC Membership

3. **Russia's Take on Cybercrime**
   Russia's uncooperative attitude toward prosecuting cyber criminality is a generally accepted fact in countries like the United States and its allies. However, Russia has managed to cultivate a slightly different image in some international forums like the United Nations, where it has routinely introduced proposals and draft language that gives the impression that the opposite is true.

   Most recently, Russia introduced a 69-page draft convention to the United Nations entitled *United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*.[10] This document purports to tackle cybercrime by calling for "domestic laws to criminalize changing digital information without permission," while also [directing] member states to formulate domestic laws to disallow unsanctioned malware research, "[forbidding] the creation and use of digital data to mislead the user," and potentially broadening pathways for extradition.[11]

   While some of these proposed items could be acceptable to countries like the United States if worded carefully and aligned with existing international agreements, such as the Budapest Convention on Cybercrime, the positive aspects of the convention draft are wrapped up with numerous contentious issues deeply at odds with existing policy. Critics have noted that included in the draft are calls for "technical backdoors in network systems, network wiretapping capabilities, and potential technical censorship," as well as backdoors that could "potentially curb freedom of speech, expression or press."[12]

   It does not appear likely that this draft will end up garnering significant support, but it does continue to allow Russia to muddy the waters on how seriously they take cybercrime and how cooperative they are being in attempting to find solutions.

   Action & Analysis
   Included with H-ISAC Membership

Congress –

Tuesday, August 10th:
- No relevant hearings

Wednesday, August 11th:
- No relevant hearings

Thursday, August 12th:
- No relevant hearings

International Hearings/Meetings –

- No relevant meetings

EU –

- No relevant meetings

August 10th, 2021

Conferences, Webinars, and Summits –

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

Contact us: follow @HealthISAC, and email at contact@h-isac.org

---

[1] https://www.cyberscoop.com/national-cyber-director-endorses-plan-for-a-bureau-to-collect-analyze-threat-data/

[2] https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view

[3] https://www.cyberscoop.com/national-cyber-director-endorses-plan-for-a-bureau-to-collect-analyze-threat-data/

[4] https://www.king.senate.gov/newsroom/press-releases/king-rounds-sasse-introduce-bipartisan-cybersecurity-legislative-package-to-better-protect-us-critical-infrastructure

[5] https://www.king.senate.gov/newsroom/press-releases/king-rounds-sasse-introduce-bipartisan-cybersecurity-legislative-package-to-better-protect-us-critical-infrastructure

[6] https://www.armis.com/research/pwnedpiper

[7] https://www.armis.com/research/pwnedpiper

[8] https://www.armis.com/research/pwnedpiper

[9] https://www.cyberscoop.com/pneumatic-tubes-ransomware-hospitals-swisslogic-armis/

[10] https://www.kommersant.ru/docs/2021/RF_28_July_2021_-_E.pdf

[11] https://www.theregister.com/2021/08/03/russia_cybercrime_laws/

[12] https://www.theregister.com/2021/08/03/russia_cybercrime_laws/