September 22, 2021

This week, *Hacking Healthcare* begins by breaking down the relevant elements of the European Union's (EU) annual State of the Union speech, including cybersecurity, healthcare, and semi-conductors. Next, we examine a new Policy Statement delivered by the US Federal Trade Commission (FTC) on the applicability of the Health Breach Notification Rule to health and fitness apps. Finally, we cover another twist to ransomware tactics that looks to undercut the use of ransomware negotiators and contact with law enforcement. Welcome back to *Hacking Healthcare*.

1. EU State of the Union Speech Touches on Cyber and Healthcare

The European Union's (EU) annual *State of the Union* address took place on September 15th, with European Commission President Ursula von der Leyen addressing a wide range of matters that included cybersecurity and digital aspects of healthcare.

Cyber: Cyber issues were specifically called out in a section addressing EU-wide defense. Declaring that "we cannot talk about defence without talking about cyber," von der Leyen stated that the EU "should not just be satisfied to address the cyber threat, but also strive to become a leader in cyber security."[i]

Von der Leyen emphasized that "it should be here in Europe where cyber defence tools are developed," and that a *European Cyber Defense Policy*, "including legislation on common standards under a new *European Cyber Resilience Act*," is needed. She declared that EU member states should start with "a common assessment of the threats we face and a common approach to dealing with them."[ii]

Semi-Conductors: The chip shortage has been keenly felt worldwide, and the EU appears poised to follow the United States in addressing its reliance on state-of-the-art chips manufactured abroad. The President's speech called for a new European Chips Act that will "link together our world-class research, design and testing capacities," and "create a state-of-the-art European chip ecosystem, including production."[iii] Von der Leyen pitched this as not only a means to remain competitive in this market but also as an important step in maintaining "tech sovereignty."[iv]

Digital Health: On health issues, von der Leyen mentioned the start of the European Health Emergency preparedness and Response Authority (HERA) and proposed a new health preparedness and resilience mission for the whole of the EU, which is to be backed by €50 billion by 2027.[v] Among other things, HERA is to "support research and innovation for the development for new medical countermeasures, including through Union-wide clinical trial networks and platforms for the rapid sharing of data."[vi]

Action & Analysis
Included with H-ISAC Membership

2. New FTC Ruling Clarifies Health Apps' Compliance with Breach Notification Rule

Last week, the Federal Trade Commission (FTC) issued a policy statement to clarify how aspects of the American Recovery and Reinvestment Act of 2009 applied to health and fitness apps that collect or use consumer health data. The policy statement is a step toward defining how the ever-expanding health and fitness app marketplace, replete with entities that generally fall outside HIPAA, will be expected to treat the security and privacy of data they collect.

The statement comes as the FTC acknowledges that health apps and connected devices have proliferated widely in the 12 years since the initial legislation and that they are "ripe for scammers and other cyber hacks."[vii]

Published on September 15th, the policy statement was approved on a 3-2 party line vote by the Democratic majority. The policy statement

"affirms that health apps and connected devices that collect or use consumers' health information must comply with the Health Breach Notification Rule, which requires that they notify consumers and others when their health data is breached."[viii]

In the FTC's words, the Health Breach Notification Rule is meant to "ensure that entities who are not covered by the Health Insurance Portability and Accountability Act ("HIPAA") nevertheless face accountability when consumers' sensitive health information is compromised."[ix] Failure to comply may result in civil penalties of $43,792 per violation per day.[x]

Notably, the statement also highlights that the term "breach" extends beyond cybersecurity intrusions to cover unauthorized access and the sharing of covered information without an individual's authorization.

Action & Analysis
Included with H-ISAC Membership

3. Ransomware Gang Warns of Repercussions for Contacting Negotiators or Law Enforcement

Ransomware's rather rapid evolution to include data exfiltration and extortion continues as cybercriminals look to stay one step ahead of processes and policies designed to minimize their chance of a large successful payout. One such ransomware group has determined that third-party assistance is cutting into their success and profits and has a new warning for their victims.

Organizations have been increasingly turning to professional ransomware negotiators, law enforcement, and legal experts for guidance on how best to proceed when victimized by a ransomware attack. Contacting these entities may lower future legal and regulatory risk, help negotiate a lower ransom payment, or even help identify and prosecute the perpetrators. But for the ransomware groups committing the attacks, these third parties can complicate the process by lengthening negotiations, lowering success rates, lessening payouts, and increasing the risk of identification.

One such ransomware group, Ragnar Locker, has since posted an announcement stating that "if you will hire any recovery company for

negotiations or if you send request to the Police/FBI/investigators, we will consider this hostile intent and we will initiate the publication of whole compromised Data immediately," and "we will find out and punish with all our efforts."[xi] While apparently written by a non-native English speaker, the intent is clear.

Ragnar Locker is not an inconsequential cybercriminal, having been linked to attacks against the game company Capcom, chip manufacturer ADATA, and Aviation company Dassault Falcon Jet.[xii] It remains to be seen if this tactic gains widespread adoption by other prominent ransomware groups.

Action & Analysis
Included with H-ISAC Membership

Congress

Tuesday, September 21st:
- Senate – Judiciary Committee: Hearings to examine big data, focusing on implications for competition and consumers.

Wednesday, September 22nd:
- Senate – Aging Committee: Hearings to examine fraud, scams, and COVID-19, focusing on how older Americans have been targeted during the pandemic.

Thursday, September 23rd:
- Senate – Homeland Security and Governmental Affairs Committee: Hearings to examine national cybersecurity strategy, focusing on protection of federal and critical infrastructure systems.

International Hearings/Meetings –

- No relevant meetings

EU –

- No relevant meetings

Conferences, Webinars, and Summits –

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

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

[i] https://ec.europa.eu/commission/presscorner/detail/ov/SPEECH_21_4701

[ii] https://ec.europa.eu/commission/presscorner/detail/ov/SPEECH_21_4701

[iii] https://ec.europa.eu/commission/presscorner/detail/ov/SPEECH_21_4701

[iv] https://ec.europa.eu/commission/presscorner/detail/ov/SPEECH_21_4701

[v] https://ec.europa.eu/commission/presscorner/detail/ov/SPEECH_21_4701

[vi] https://ec.europa.eu/commission/presscorner/detail/en/ip_21_4672

[vii] https://www.ftc.gov/news-events/press-releases/2021/09/ftc-warns-health-apps-connected-device-companies-comply-health

[viii] https://www.ftc.gov/news-events/press-releases/2021/09/ftc-warns-health-apps-connected-device-companies-comply-health

[ix] https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf

[x] https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf

[xi] https://www.bleepingcomputer.com/news/security/ransomware-gang-threatens-to-leak-data-if-victim-contacts-fbi-police/

[xii] https://www.bleepingcomputer.com/news/security/ransomware-gang-threatens-to-leak-data-if-victim-contacts-fbi-police/

##