June 14, 2022

TLP White

This week, *Hacking Healthcare* begins by examining some recent statements made at RSA related to the incoming cyber incident reporting for critical infrastructure sectors in the United States. We break down what Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly said at the conference and what that might translate into for the upcoming rulemaking process. We then pull out some of the more impactful numbers from security firm Sophos' new report on ransomware in healthcare and assess what members should take away from it.

Welcome back to *Hacking Healthcare*.

1. **Director Easterly Questioned on Cyber Incident Reporting – Hints at Consultative Process**

   One of the more impactful pieces of cybersecurity legislation to be passed in recent months is the *Cyber Incident Reporting for Critical Infrastructure Act of 2022* (CIRCIA) that was part of the *Consolidated Appropriations Act of 2022*. Since then, details have been sparse on what might be expected from the eventual rulemaking process that will finalize what the reporting will cover and require, as well as what kind of impact this may have on the industries affected. Some hints to those unknowns were dropped at last week's RSA conference by the Cybersecurity and Infrastructure Security Agency's (CISA) Director, Jen Easterly.

   In a panel focused on Zero Trust, Director Easterly touched on the plans to publish a public Request For Information (RFI) in order to solicit feedback from industry on their perspectives and concerns for the cyber incident reporting rulemaking process.[1] Director Easterly made it clear that she wished to avoid placing undue burden on private sector entities during the stressful period of incident response.[2] She also reiterated the need for CISA to continue to build trust, add value, and increase collaboration with the private sector. To that end, Director Easterly also stated how she believes that critical infrastructure companies are already recognizing that cyber incident reporting is "collectively good for the ecosystem."[3]

Action & Analysis

2. Ransomware in Healthcare

It has been a while since we have taken a look at ransomware more broadly, but it continues to be a serious concern for organizations of every sector. As such, it's beneficial to check in from time to time on its broader trends and developments for the healthcare sector specifically. A good place to start is with some highlights from Sophos' recent healthcare ransomware report for 2022.

Security firm Sophos recently released their *State of Ransomware in Healthcare 2022* report that tracks some of the larger trends as it relates to the healthcare sector. This most recent report includes 5,600 respondents from 31 countries.[4] Some of the key takeaways from the freely available 22-page document include:[5]

- 66% of healthcare organizations were hit by ransomware in 2021 up from 34% in 2020
- 61% of attacks led to encryption
- Backups were used as a means to restore data by 72% of those organizations where data was encrypted
- It is becoming less of a sure thing that data will be recovered by paying a ransom
    - On average, healthcare organizations paying a ransom received 65% of stolen data – down 4% from 2020
    - Only 2% that paid a ransom in 2021 received all their data back – down from 8% in 2020
- The healthcare sector remains the most likely sector to pay a ransom at 61% - up from 34% from 2020 and considerably higher than the 46% cross sector average
- The healthcare sector leads in volume of payments but ranks low in amount paid per ransom
- 94% of ransomware attacks impacted operational ability of an organization

One of the more interesting impacts ransomware is having on the healthcare sector relates to cyber insurance. According to the report:

- 78% of healthcare organizations say they have cyber insurance
- 46% of those who have cyber insurance say there are exclusions or exceptions in their coverage
- 93% noted that cyber insurance was getting harder to secure due to a variety of factors:
    - 51% reported that the level of cybersecurity they need to qualify is now higher
    - 45% said policies are now more complex
    - 48% said fewer companies offer cyber insurance
    - 46% stated that the process takes longer

    - 34% said it is more expensive
- 97% of organizations with cyber insurance made improvements to their cyber defenses to improve their cyber insurance positions
- Cyber insurance had a 97% payout rate for the healthcare sector

Action & Analysis

Congress

Tuesday, June 14th:
- House of Representatives - Committee on Energy and Commerce - Subcommittee on Consumer Protection and Commerce: Hearing: "Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security"

Wednesday, June 15th:
- No relevant hearings

Thursday, June 16th:
- No relevant hearings

International Hearings/Meetings

- No relevant meetings

EU –

Conferences, Webinars, and Summits

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

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

About the Author

Hacking Healthcare is written by John Banghart, who 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, and 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.

June 14, 2022

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

---

[1] https://insidecybersecurity.com/daily-news/cisa-plans-release-request-stakeholder-feedback-incident-reporting-regime

[2] https://insidecybersecurity.com/daily-news/cisa-plans-release-request-stakeholder-feedback-incident-reporting-regime

[3] https://subscriber.politicopro.com/article/2022/06/companies-warming-to-cyber-incident-reporting-mandate-cisa-chief-says-00037950

[4] https://www.sophos.com/en-us/whitepaper/state-of-ransomware-in-healthcare

[5] https://www.sophos.com/en-us/whitepaper/state-of-ransomware-in-healthcare