September 20, 2022

TLP White

This week, Hacking Healthcare begins by examining the draft of the European Commission's *Cyber Resilience Act* (CRA) to understand the practical challenges it aims to address within the current regulatory framework for digital products and services, as well as where gaps may exist. We briefly break down the document's contents and explain the impact it may have on the healthcare industry. Then, we cover the Cybersecurity and Infrastructure Security Agency's (CISA) Request for Information (RFI) soliciting public input on the incident reporting and ransomware reporting aspects of the previously passed *Cyber Incident Reporting for Critical Infrastructure Act of 2022* (CIRCIA).

Welcome back to *Hacking Healthcare*.

1. Overview of the Cyber Resilience Act

On September 15, the European Commission presented a proposal for a new EU-wide cybersecurity regulation, the Cyber Resilience Act (CRA). Described as the "first ever EU-wide legislation of its kind," the proposal "introduces common cybersecurity rules for manufacturers and developers of products with digital elements, covering both hardware and software."[1] While the text is far from finalized, it appears likely that it will have both direct and indirect impacts on the healthcare sector organizations.

Broadly, the CRA aims to improve cybersecurity safeguards for digital products on the market to reduce the number of exploited vulnerabilities and to prevent potential entry points for cyberattacks. Last year alone, the EU estimated that the global annual cost of software and hardware attacks amounted to roughly €5.5 trillion.[2] The commission predicts that if the CRA is implemented, it could reduce the cost of cyber incidents by "roughly €180 - €290 billion annually."[3]

Based on the "security by design" approach, the CRA addresses three areas to promote more secure hardware and software: making cybersecurity mandatory; ensuring that manufacturers will remain responsible for their product's cybersecurity throughout its life cycle; and better informing consumers about these parameters when choosing a product with digital elements.

While the legislation may sometimes be described as primarily affecting manufacturers and vendors of just smart IoT devices, the scope is much larger — covering any software, whether embedded or not, and requiring a mandatory conformance assessment for products that are deemed critical. However, there are notable exceptions that we will cover in the analysis section.

The CRA divides these into two classes of "critical products with digital elements," reflecting the related level of cybersecurity risk:

- Those regarded to be of "higher risk" like firewalls, smartcards, token, IoT devices for use by critical infrastructure providers under NIS 2,[4] robot sensors and controllers, smart meters; and

- Those regarded as "lower risk," such as identity management system software, browsers, password managers, mobile device management software, remote access/sharing software.

Under the proposed EU rules, certain products will have to meet various cybersecurity requirements to be sold throughout member states. For example, when placing a product on the market, manufacturers should have "appropriate policies and procedures, including coordinated vulnerability disclosure policies to remediate potential vulnerabilities in the product."[5] Manufacturers must ensure that vulnerabilities are handled effectively over the expected product lifetime or for five years after being placed on the market, whichever is shorter. Failure to comply with the essential cybersecurity rules can "prohibit or restrict that product being made available on its national market."[6] Offending companies may also face fines of up to €15 million or 2.5% of their global turnover, whichever is higher.

Similar to the incident reporting timeline of NIS 2, the CRA imposes short-term reporting obligations on manufacturers to report any actively exploited vulnerabilities contained in a product with digital elements, as well as any incident that impacts the security of products, to the European Union Agency for Cybersecurity (ENISA)[7] within 24 hours of becoming aware of it. Additionally, the CRA would also require organizations defined as importers or distributors to report cybersecurity vulnerabilities in products with digital elements as they are identified.

Action and Analysis
Membership required

2. CISA's RFI on CIRCIA Incident Reporting

On September 12, the Cybersecurity and Infrastructure Security Agency (CISA) published a long-awaited Request for Information (RFI) regarding the cyber incident reporting provisions of the Critical Infrastructure Act of 2022 (CIRCIA).[8] The RFI is an important

opportunity for the private sector to weigh in on various aspects of the forthcoming incident reporting requirements, and they will help CISA understand the burdens and concerns facing private-sector entities across sectors.

As a reminder of how we got here, cyber incident reporting and ransomware payment reporting were elements of CIRCIA, which was passed earlier in the year. However, while the critical infrastructure provisions were written with baseline requirements by legislators, the details of who and what would be covered, along with other aspects, were left to a lengthy rulemaking process to be overseen by CISA. Part of that rulemaking process is the requirement to seek public input to help ensure that CISA understands the complexities of incident reporting and the burdens and concerns of private-sector entities in order to craft a balanced approach. The RFI and its accompanying listening sessions are the primary drivers for this public input.

CISA is particularly interested in:[9]

- Definitions for and interpretations of the terminology to be used in the proposed regulations;
- The form, manner, content and procedures for submission of reports required under CIRCIA;
- Information regarding other incident reporting requirements, including the requirement to report a description of the vulnerabilities exploited; and
- Other policies and procedures, such as enforcement procedures and information protection policies, that will be required for implementation of the regulations.

To get more specific, some of the aspects this rulemaking is looking to determine include:

- The meaning of “covered entity,” “covered cyber incident,” “substantial cyber incident,” and “supply chain compromise”;
- What constitutes “reasonable belief” that a covered cyber incident has occurred?
- When should the time for the 24-hour deadline for reporting ransom payments begin?
- Guidelines or procedures regarding the use of third-party submitters.

This is not by any means an exhaustive list and is not meant to restrict commentators on the recommendations they would like to provide. Comments must be submitted by November 14, 2022 for consideration.

Action & Analysis
Membership required

Congress

Tuesday, September 20th:
- No relevant hearings

Wednesday, September 21st:
- No relevant hearings

Thursday, September 22nd:
- No relevant hearings

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

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.

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

[1] https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_5375
[2] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
[3] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
[4] https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333 – The Network and Information Security (NIS) Directive is currently undergoing a revision that will expand its scope and security requirements for EU member states.
[5] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
[6] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
[7] https://www.enisa.europa.eu/
[8] https://www.federalregister.gov/documents/2022/09/12/2022-19551/request-for-information-on-the-cyber-incident-reporting-for-critical-infrastructure-act-of-2022
[9] https://www.federalregister.gov/documents/2022/09/12/2022-19551/request-for-information-on-the-cyber-incident-reporting-for-critical-infrastructure-act-of-2022