HACKING HEALTHCARE

Hacking Healthcare- Weekly Blog

TLP:WHITE

Mar 03, 2025

This week, Health-ISAC®'s Hacking Healthcare® examines new draft proposal from the European Commission meant to ensure an effective EU-wide response to a large-scale cyber crisis. Join us as we examine what it is, why it's been developed, and how Health-ISAC members might get use out of it.

Welcome back to Hacking Healthcare®.

European Commission Proposes Cyber Crisis Coordination Blueprint

On February 24, the European Commission published a new proposal designed to ensure an effective and efficient response to large-scale cyber incidents, the Cyber Blueprint — Proposal Council Recommendation.

What is it and why is it being proposed?

There is a clear understanding in the EU that digital technologies and global connectivity are vital to economic growth, are transformative to critical infrastructure, and are increasingly ubiquitous and irreplaceable. However, these technologies and connectivity have also opened the door for large-scale cybersecurity incidents that “can cause a level of disruption that exceeds a Member State’s capacity to respond to it,” or which may have “a significant impact on more than one Member State.”[i]

Within that context, the Commission has published this new proposal, which follows on from a recommendation made by the Council of the European Union last May,[ii] that called for "a revised Cybersecurity Blueprint in the form of a Council recommendation that will address the current challenges and complex cyber threat landscape, strengthen existing networks, enhance cooperation, and break silos between organisations…."[iii] The revision it references is the existing Blueprint for coordinated response to large-scale cross-border cybersecurity incidents and crises from 2017.[iv]

In particular, while it acknowledges that "Member States have a primary responsibility in the management of national cyber crises," the potential for cross-border effects necessitates a clear plan of how and when the various union-level entities should coordinate with each other to maximize their ability to effectively respond to a large-scale cybersecurity incident from beginning to end.[v] Importantly, the blueprint is non-binding and was developed to be complementary to, and consistent with, existing EU policies.

What is in it?

The proposal is split into several parts. The opening provides background on the proposal, outlines the existing environment of policy frameworks, mechanisms, and actors, highlights particular policy goals and various considerations that went into the planning process, and provides rationale for the approaches taken.

- Following that are several numerated sections:

- Section (I) provides the aim, scope, and principles of the EU cyber crisis framework.

- Section (II) addresses preparing for a union-level cyber crisis, with an emphasis on trusted information sharing processes, cybersecurity exercises, and Domain Name System (DNS) security and resiliency.

- Section (III) addresses detection strategies and crisis escalation.

- Section (IV) provides an outline of what various EU-level entities should be doing to respond once a union-level cyber crisis has been established.

- Section (V) addresses recovery from a cyber crisis.

- Section (VI) addresses secure communications.

- Section (VII) outlines coordination with military actors.

- Section (VIII) addresses cooperation with strategic partners.

In addition, there is a separate annex document that outlines the blueprint for responding to a cybersecurity crisis in diagram form, the relevant union-level actors across the cyber crisis management lifecycle and the crisis management mechanisms, and the blueprint's guiding principles.

Action and Analysis

Included with Health-ISAC Membership

[i] https://digital-strategy.ec.europa.eu/en/library/cyber-blueprint-draft-council-recommendation
[ii] https://data.consilium.europa.eu/doc/document/ST-10133-2024-INIT/en/pdf
[iii] https://data.consilium.europa.eu/doc/document/ST-10133-2024-INIT/en/pdf
[iv] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017H1584#:~:text=This%20Blueprint%20applies%20to%20cybersecurity,that%20they%20require%20timely%20policy
[v] As defined in NIS 2: "a large-scale cybersecurity incident is an incident which causes a level of disruption that exceeds a Member State's capacity to respond to it or has a significant impact on at least two Member States."
[vi] https://digital-strategy.ec.europa.eu/en/library/cyber-blueprint-draft-council-recommendation

[vii] https://digital-strategy.ec.europa.eu/en/library/cyber-blueprint-draft-council-recommendation
[vii] https://digital-strategy.ec.europa.eu/en/library/cyber-blueprint-draft-council-recommendation

Reference(s)	Europa Analytics, Europa Analytics, Europa Analytics
Report Source(s)	Health-ISAC

Alert ID 93397c42

View Alert

Share Feedback
was this helpful? |

Tags Hacking Healthcare, Information Sharing, Incident Response, Europe, European Union, European Commission

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

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).

For Questions or Comments
Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**