Health-ISAC™
Collaborating for Resilience in Healthcare

Health-ISAC Weekly Blog -- Hacking Healthcare®

Hacking Healthcare ○ TLP:WHITE Alert ID : e4c228ee Aug 02, 2024, 08:38 AM

This edition of Hacking Healthcare® examines the results of the recent elections in the European Union (EU) and the United Kingdom (U.K.) to assess how they may influence cybersecurity and technology policies that affect the healthcare sector.

Welcome back to Hacking Healthcare®.

European Election Results May Signal Cybersecurity and Technology Policy Changes

A month ago in Hacking Healthcare®, we noted that a series of summer elections had the potential to significantly shift cybersecurity and technology policy in Europe.[i] Now that the dust has settled a bit, we are able to assess with a bit more clarity what the healthcare sector might expect to see in the coming months and years, as well as what the healthcare sector might want to do as a response.

European Parliament

The recent European Parliamentary elections resulted in a rightward-shift in the makeup of Parliament, with the most notable surge for far-right parties coming from France and Germany. However, none of the parties within the European Parliament was able to take an overall majority. This means that coalitions of like-minded parties are set to emerge and form blocs to shore up their political leverage. Despite the gains on the political right, power will reside with the centrists, who are headed by the center-right European People's Party (EPP).

Since the election, leadership positions and committees have been filling out. The EPP has seen its candidates, Ursula von der Leyen and Roberta Metsola, elected to the positions of the President of the European Commission and President of the European Parliament, respectively. These two will have a say in setting the policy agenda, organization, and activities of their institutions. Policy priorities will continue to emerge as this session settles in. Former Prime Minister of Estonia Kaja Kallas will become the Commission's new foreign policy chief.

U.K.

While the far-right surged in many places, the U.K. saw a significant swing in the opposite direction in terms of Parliamentary seats. The left-leaning Labour Party retook sole control of the government for the first time since 2010 in a landslide victory that gives them a healthy majority to govern with. New Prime Minister Sir Keir Starmer will now have the opportunity to reshape the U.K. government's policy approaches on cybersecurity and technology issues. While things are still settling, his recent King's Speech provided some hints as to what we might expect.

The relatively short speech only hinted at Labour's cybersecurity and technology priorities, with a nod toward harnessing A.I. and strengthening safety frameworks. A more comprehensive outline of Labour's policy priorities can be found in the 104-page background briefing for the King's Speech.[ii]

The two most relevant legislative bills for the healthcare sector may be the following:

Digital Information and Smart Data Bill

The Digital Information and Smart Data Bill addresses a broad swath of issues and seeks to "harness the power of data."[iii] While there are mentions of establishing digital verification services, Smart Data schemes, and enabling better data sharing for research, the most relevant aspect for this audience may be data protection.

The background briefing outlines how the bill should strengthen the Information Commissioner's Office (ICO) into a "more modern regulatory structure" with "new, stronger powers."[iv] It may also be "accompanied by targeted reforms to some data laws that will maintain high standards of protection" while also clarifying the "the safe development and deployment of some new technologies." Finally, the bill promises to "promote standards for digital identities around privacy, [and] security."[v]

Cyber Security and Resilience Bill

In response to the numerous damaging cyberattacks against critical infrastructure, especially in healthcare, the bill is meant to "strengthen the UK's cyber defences, [and] ensure that critical infrastructure and the digital services that companies rely on are secure."[vi]

The background briefing does not shy away from the role regulation will play in securing cyberspace, and it lays out the expectation that the bill will expand existing regulation and further empower regulators. Specific areas of focus include protecting digital services and supply chains, ensuring the implementation of "essential cyber safety measures," and mandating increased incident reporting.

Additionally, the background briefing notes the critical need to update existing cross-sector cybersecurity legislation that predates Brexit. While the EU has moved to NIS 2, the U.K. has not yet followed with a similar update.

We explore what these election results may mean in the members-only Action & Analysis section below.

Action & Analysis

Included with Health-ISAC Membership

[i] https://h-isac.org/health-isac-hacking-healthcare-6-17-2024/

[ii] https://assets.publishing.service.gov.uk/media/6697f5c10808eaf43b50d18e/The_King_s_Speech_2024_background_briefing_notes.pd

[iii] https://assets.publishing.service.gov.uk/media/6697f5c10808eaf43b50d18e/The_King_s_Speech_2024_background_briefing_notes.pd

[iv] https://assets.publishing.service.gov.uk/media/6697f5c10808eaf43b50d18e/The_King_s_Speech_2024_background_briefing_notes.pd

[v] https://assets.publishing.service.gov.uk/media/6697f5c10808eaf43b50d18e/The_King_s_Speech_2024_background_briefing_notes.pd

[vi] https://assets.publishing.service.gov.uk/media/6697f5c10808eaf43b50d18e/The_King_s_Speech_2024_background_briefing_notes.pd

Report Source(s)

Health-ISAC

Release Date

Aug 02, 2024, 11:59 PM

Reference | References

Service Gov UK
Health-ISAC

Tags

Regulations, Regulatory, Hacking Healthcare, European Union (EU), European Parliament, Europe, United Kingdom, European Union

For Questions and/or Comments:

Please email us at contact@h-isac.org

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).