Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare™ | TLP:WHITE | Alert ID : fcdc80e9 | Sep 01, 2023, 02:11 PM

This week, *Hacking Healthcare*™ examines the cybersecurity workforce issue. With the recent release of the United States' *National Cyber Workforce and Education Strategy*, we wanted to examine how the United States and the European Union (EU) are attempting to address the growing shortage of skilled cybersecurity personnel. In our analysis section, we then explore what healthcare organizations may be able to do to maximize the talent available in the meantime.

Welcome back to *Hacking Healthcare™*.

Solving the Cyber Workforce Problem

The growing use of technology products to carry out critical functions within all industries, and a general increase in connectivity globally, continues to highlight the need for countries to prioritize building and maintaining a vast, skilled cyber workforce. Unfortunately, thus far the need for this workforce has rapidly outpaced efforts to build it up. With the Biden administration's recent publication of its *National Cyber Workforce and Education Strategy*, we thought it would be a good time to assess how the United States and the European Union are attempting to address this issue and to evaluate what kind of relief the healthcare sector might expect.[i]

United States

The *National Cyber Workforce and Education Strategy* is an expansive 60-page document that clearly indicates that the Biden administration takes the issue seriously.[ii] Much like the *National Cybersecurity Strategy* that came out earlier in the year, the workforce strategy is divided into thematic pillars with associated lines of effort.[iii]

While we won't go into great detail here, the lines of effort encompass much of what you would expect in a whole-of-society approach. Improving cyber education and awareness (especially in K-12 education), reaching out to underserved communities to improve the diversity of the cyber workforce, looking for places to grow public-private partnerships, finding new funding opportunities and expanding existing ones, encouraging skills-based hiring practices, and encouraging "flexible employment models" are some of the approaches raised within the strategy.

While the scope of the strategy is encouraging, there is a distinct lack of specifics when it comes to describing the actual implementation of the various lines of effort. Expected completion dates and resource allocation are largely absent, and in many cases, the wording around these initiatives does not suggest concrete plans or near-term activities.

Furthermore, the National Security Council and the Office of the National Cyber Director are the entities tasked with implementing the strategy, and with a new National Cyber Director yet to be appointed and the potential for an administration change in 2024, it is an open question as to how much of a implementation priority this becomes.

EU

It isn't clear that things are any better in the European Union . *The EU's Cybersecurity Strategy for the Digital Decade*, published in 2020 highlighted an estimated 291,000 unfilled cybersecurity posts and lamented that "hiring and training cybersecurity experts is a slow process leading to greater cybersecurity risks for organisations."[iv] To address this deficiency, the EU highlighted multiple approaches to building out education and awareness while also pursuing upskilling and reskilling EU citizens in digital skill sets like cybersecurity.

More recently, the EU launched its *2023 Year of Skills* initiative, which is designed to "address skills gaps in the European Union" and aid in "reskilling people with the focus on digital and green technology skills."[v] As part of that initiative, the EU launched the *Cybersecurity Skills Academy,* a "European policy initiative aiming to bring together existing initiatives on cyber skills and improve their coordination, in view of closing the cybersecurity talent gap."[vi]

The Academy hopes to address aspects such as:

- Developing frameworks for defining, providing, and assessing cyber skills
- Mapping and citing training opportunities, initiatives, and organizations relating to cyber skills
- Coordinating pledges from stakeholders from the private sector
- Highlighting funding opportunities and projects that support cyber skill development

These types of programs are in addition to the national-level initiatives at the member state level. The maturity of member state efforts varies significantly, from those who only reference it in general digitalization strategies to countries like Latvia, whose *Cyber Security Strategy of Latvia for 2019-2022* "has specific goals to educate public and local administration staff on ICT safety, as well as provide cybersecurity skills for SMEs and citizens."[vii], [viii]

Action & Analysis
Included with Health-ISAC Membership

Conclusion

We know that many of these considerations are more easily said than done, but as the current environment doesn't look to change overnight, we do think they are worth investigating. We certainly hope that cyber strategies like those in the United States and the EU make progress sooner rather than later, and we will be sure to update you on the progress of major initiatives related to them.

Congress

Tuesday, August 29

No relevant hearings

Wednesday, August 30

No relevant meetings

Thursday, August 31

No relevant meetings

International Hearings/Meetings

No relevant meetings

[i] https://www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf
[ii] https://www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf
[iii] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[iv] https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0
[v] https://year-of-skills.europa.eu/about_en
[vi] https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy
[vii] https://digital-skills-jobs.europa.eu/en/actions/national-initiatives
[viii] https://www.mod.gov.lv/en/news/latvia-approves-new-cyber-security-strategy-2019-2022
[ix] https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative
[x] https://commission.europa.eu/system/files/2020-02/communication-shaping-europes-digital-future-feb2020_en_4.pdf
[xi] https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0
[xii] https://www.forbes.com/sites/forbestechcouncil/2023/03/01/why-overcoming-the-cybersecurity-labor-shortage-matters-to-company-success/?sh=8e1c3187766b
[xiii] https://www.euractiv.com/section/cybersecurity/news/eu-seeks-to-bridge-cyber-skills-gap-with-new-academy/
[xiv] https://www.wsj.com/articles/cybersecurity-leaders-suffer-burnout-as-pressures-of-the-job-intensify-b0609ef1
[xv] https://www.securitymagazine.com/articles/98776-one-of-the-biggest-threats-to-a-cybersecurity-team-employee-burnout
[xvi] https://www.stjude.org/education-training/predoctoral-training/internships/information-services-internships/information-services-internships-information-security.html
[xvii] https://jobs.mayoclinic.org/trainingprogramsandinternships

Report Source(s)

Health-ISAC

Reference | References

archives
Forbes
Whitehouse
Whitehouse
mod
Europa Analytics
Euractiv
stjude
Wall Street Journal
Europa Analytics
Europa Analytics
mayoclinic
Security Magazine
Health-ISAC
Forbes
Europa Analytics
Europa Analytics

Tags

Hacking Healthcare, workforce retention, European Union (EU), Workforce

For Questions and/or Comments:

Please email us at contact@h-isac.org

Conferences, Webinars, and Summits:

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

Hacking Healthcare:

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, 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.

Access the Health-ISAC 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 Cyware.

For Questions or Comments:

Please email us at toc@h-isac.org