HACKING HEALTHCARE

Hacking Healthcare - Weekly Blog

TLP:WHITE

Nov 20, 2025

This week, Health-ISAC®'s Hacking Healthcare® examines the recent introduction of a United Kingdom (UK) legislative bill that would update its Network and Information Security (NIS) regulations. Join us as we break down what the UK government hopes to achieve with the new legislation and how it may impact the health sector.

Welcome back to Hacking Healthcare®.

U.K. Network and Information Security (NIS) Regulation Reform Introduced to Parliament

Overview

Prior to the UK's withdrawal from the European Union (EU), like all EU members, the UK adopted EU regulations and directives, such as the General Data Protection Regulation (GDPR) by transcribing them into national law. However, since leaving the EU in 2020, it is no longer bound by EU policy approaches and has had to chart its own course on issues like cybersecurity and privacy. The result of this split has led the UK down a path of slowly updating its EU-era laws and regulations, often taking inspiration from, and lagging a bit behind, the EU's own regulatory updates.

Among the more critical cybersecurity-related EU-era regulations in the UK is the Network and Information Systems Regulations 2018

(NIS). As you would expect, the UK's adoption of NIS was very similar to the rest of the EU member states. The regulations served to "[provide] legal measures to boost the overall level of security (both cyber and physical resilience) of network and information systems that are critical for the provision of digital services (online marketplaces, online search engines, cloud computing services) and essential services (transport, energy, water, health, and digital infrastructure services)."[i]

While the EU pushed ahead on an NIS update years ago, with full implementation ongoing and lagging behind schedule, the UK is only now addressing an NIS update, with the most recent development being the introduction of the Cyber Security and Resilience Bill (CSRB) into Parliament.[ii] This bill would reshape the original NIS to better address technological developments, an evolving threat environment, and to shore up some of the first iteration's shortcomings.

Why the Update?

As mentioned above, a lot has changed since 2018, and technological developments, the evolving threat environment, shortcomings of the first iteration of NIS, and a free hand to draft UK-specific policy has incentivized this update. More specifically, the update will address:

- Technological Developments: Technological developments like the increasing criticality of data centers, managed service providers, and large load controllers have incentivized revising the scope of the NIS regulations to cover newer technologies.[iii]
- Evolving Threat Environment: In its summary of the bill, the Department for Science, Innovation & Technology (DSIT) explained that "[l]ast year, the UK was the most targeted country in Europe," and cited statistics that found "95% of UK's critical national infrastructure organisations experienced a data breach in 2024."[iv] Additionally, DSIT stated that "as the threat has grown more intense, frequent, and sophisticated, our defences have become comparatively weaker."[v]
- Shortcomings of NIS: Two Post-Implementation Reviews (PIR) of the NIS regulations were conducted in 2020[vi] and 2022,[vii] by the UK government. These reviews found several shortcomings with the NIS regulations, including the findings that "although organisations were taking measures to ensure

the security of their network and information systems, the rate of improvement needed to be accelerated," and that the NIS was "not working as intended in several key areas, such as the scope of the regulations and the small number of incident reports being submitted."[viii]

How Will the CSRB Address These Issues?

We won't tackle all the proposed revisions within the CSRB's 100-pages, especially as many will not necessarily apply to the health sector. Still, at a higher level, DSIT describes the CSRB as being built around three pillars:

- Expanded Scope: The CSRB would expand the scope of NIS to better encompass "services which are so essential, that their disruption would affect our daily lives." Aside from data centers, managed service providers, and large load controllers, the most interesting addition is for "designated critical suppliers," which we will address below.
- Effective Regulators: The CSRB would provide regulators with a stronger toolkit to ensure adoption and enforcement of the new NIS regulations. Included would be a new incident reporting regime, new information sharing mechanisms and protections, and new penalties for non-compliance.
- Enable Resilience: The CSRB would include tools to allow the UK government to adapt more dynamically to evolving threats and emerging shortcomings. In particular, the CSRB would enable secondary legislation that could bring "more sectors into scope, or updat[e] and introduc[e] new security and resilience requirements," and provide new powers to the government that would allow them to "direct regulators or regulated entities to take targeted and proportionate action in response to imminent threats that risk UK national security."[ix]

Path Forward

The CSRB has only just been introduced in the House of Commons and has a ways to go before it's signed into law.

Action and Analysis

Included with Health-ISAC Membership*

[i] https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018
[ii] https://bills.parliament.uk/bills/4035/publications
[iii] Large Load Controllers are defined as “organisations that control 300MW of electrical load or more to remotely control consumer appliances”
[iv] https://www.gov.uk/government/publications/deleted-cyber-security-and-resilience-network-and-information-systems-bill-factsheets/summary-of-the-bill
[v] https://www.gov.uk/government/publications/deleted-cyber-security-and-resilience-network-and-information-systems-bill-factsheets/summary-of-the-bill
[vi] https://www.gov.uk/government/publications/review-of-the-network-and-information-systems-regulations
[vii] https://www.gov.uk/government/publications/second-post-implementation-review-of-the-network-and-information-systems-regulations-2018
[viii] https://publications.parliament.uk/pa/bills/cbill/59-01/0329/en/240329en.pdf
[ix] https://www.gov.uk/government/publications/deleted-cyber-security-and-resilience-network-and-information-systems-bill-factsheets/summary-of-the-bill
[x] https://www.gov.uk/government/publications/deleted-cyber-security-and-resilience-network-and-information-systems-bill-factsheets/designating-critical-suppliers
[xi] https://www.gov.uk/government/publications/deleted-cyber-security-and-resilience-network-and-information-systems-bill-factsheets/designating-critical-suppliers
[xii] https://www.gov.uk/government/publications/deleted-cyber-security-and-resilience-network-and-information-systems-bill-factsheets/designating-critical-suppliers
[xiii] Regulated Entities in this context would include designated critical suppliers according to DSIT.
[xiv] https://publications.parliament.uk/pa/bills/cbill/59-01/0329/en/240329en.pdf
[xv] https://www.gov.uk/government/publications/deleted-cyber-security-and-resilience-network-and-information-systems-bill-factsheets/power-to-direct-regulated-entities
[xvi] https://www.gov.uk/government/publications/deleted-cyber-security-and-resilience-network-and-information-systems-bill-factsheets/power-to-direct-regulated-entities

[xvii] https://www.gov.uk/government/publications/deleted-cyber-security-and-resilience-network-and-information-systems-bill-factsheets/information-sharing
[xviii] https://www.gov.uk/government/publications/deleted-cyber-security-and-resilience-network-and-information-systems-bill-factsheets/information-sharing
[xix] https://publications.parliament.uk/pa/bills/cbill/59-01/0329/en/240329en.pdf
[xx] The Explanatory Notes for the CSRB provide examples of pre-positioning and ransomware incidents.
[xxi] https://www.gov.uk/government/publications/deleted-cyber-security-and-resilience-network-and-information-systems-bill-factsheets/incident-reporting

Reference(s)	www, www 1, parliament, parliament 1, www 2, www 3, www 4, www 5, www 6, www 7, www 8
Report Source(s)	Health-ISAC

Alert ID df278576

View Alert

Share Feedback

was this helpful? |

Tags NIS, NIS2, Incident Reporting, Information Sharing, United Kingdom, Security

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/**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.