July 20, 2022

TLP White

This week, Hacking Healthcare begins by examining a court case in Illinois, where an insurance provider has taken a client to court to nullify a cyber insurance policy over the client's misrepresentation of the security controls they claimed to have had in place. Then, we briefly assess the slowly diverging legal and regulatory regimes of the U.K. and the E.U. by looking at what a new data protection reform bill and an A.I. policy paper might mean for the healthcare sector. Welcome back to *Hacking Healthcare*.

Cyber Insurance Policy Dispute Over Security Control Misrepresentation

Cyber insurance has been in turmoil over the past few years as insurers have struggled to assess dynamic cyber risks with limited visibility into the threat landscape. This has caused the prices of policies to rise, strict pre-conditions on coverage to be placed on the insured, and some insurers have backed out of the market entirely. A new court filing in the U.S. District Court for the Central District of Illinois now illustrates just how seriously insurers are about limiting their losses and why healthcare organizations should be wary in how they go about acquiring an insurance policy.

In the seven-page filing made on July 6th, Travelers Property Casualty Company of America (Travelers) is seeking the court to declare a cyber insurance policy with International Control Services (ICS) null and void, as well as rescinding the policy and "declaring that Travelers has no duty to indemnify or defend ICS for any losses, costs or claims under the Policy, including without limitation, any losses, costs or claims resulting from the 2022 Ransomware Event."[1]

Travelers' reasoning for their position is that ICS misrepresented the degree to which they employed multi-factor authentication (MFA) on their systems, and that Travelers would not have offered them a policy had the true extent of MFA implementation been known.

According to the court filing, Travelers alleges that in both an MFA attestation and a CyberRisk Tech Application signed by ICS's CEO, ICS affirmed the usage of MFA for a multitude of cases, such as remote access to email and remote and internal access to administrative accounts.[2] Travelers' filing states that ICS was victimized in May of 2022 by a ransomware attack in which the attackers gained access to an ICS server. During the investigation of the incident Travelers became aware that MFA was not being utilized to protect the server or any other digital asset other than to protect its firewall.[3]

Nothing has been settled at the time of this writing, but Travelers would appear to have a strong case.

Action & Analysis
Included with H-ISAC Membership

U.K and E.U. Diverge on A.I. and Tech Issues

Despite Brexit, the U.K. has been slow to make significant legal and regulatory changes in areas like cybersecurity and emerging technology. They have generally remained aligned with the existing rules and regulations that they were under as a member of the European Union. However, it seems that the inevitable divergence between the U.K. and E.U. on these issues may start to widen judging by the release of two new documents on Monday. The implications for healthcare sector members may be significant depending on how unaligned these regimes become.

Signs of change began to emerge on Monday as the U.K. government released both a *Data Protection and Digital Information Bill*, and a set of proposals on how A.I. would be regulated within the U.K. that appears explicitly at odds with the E.U. approach.

The first document represents a reform of data protections that will stray from what exists within the E.U., but U.K. government officials have stressed that it fully expects the E.U. to find the U.K.'s revisions adequate and up to the E.U.s standards.[4] The Bill is 192 pages in length and is split into six parts related to data protection, digital verification services, customer and business data, other provisions about digital data, regulation and oversight, and final provisions.[5]

In terms of A.I., the U.K. appears to be pursuing a separate set of rules and regulations that would sit alongside and augment sections of the Data Protection and Digital Information Bill. The U.K.'s approach here is outlined in a policy paper that was also released on Monday.[6] The *Establishing a pro-innovation approach to regulating AI* document outlines how the U.K. is looking to establish innovation-friendly and flexible approaches to regulating A.I., one that differs in its approach to the E.U.

The policy paper proposes that the U.K. will pursue an approach in which they "set out the core characteristics of A.I. to inform the scope of the A.I. regulatory framework but allow regulators to set out and evolve more detailed definitions of AI according to their specific domains or sectors." While the paper does not lay out an exhaustive list of core principles, it suggests the following:[7]

- Ensure that A.I. is used safely
- Ensure that A.I. is technically secure and functions as designed

- Make sure that A.I. is appropriately transparent and explainable
- Embed considerations of fairness into A.I.
- Define legal person's responsibility for A.I. governance
- Clarify routes to redress or contestability

Action & Analysis
Included with H-ISAC Membership

Congress -

Tuesday, July 19th:
- No relevant hearings

Wednesday, July 20th:
- No relevant hearings

Thursday, July 21st:
- 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, 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] Travelers Property Casualty Co. of America v. International Control Services Inc., *No. 22-cv-2145*

---

[2] Travelers Property Casualty Co. of America v. International Control Services Inc.*, No. 22-cv-2145*

[3] Travelers Property Casualty Co. of America v. International Control Services Inc., No. 22-cv-2145

[4] https://iapp.org/news/a/uk-unveils-data-reform-bill-proposes-ai-regulation/

[5] https://publications.parliament.uk/pa/bills/cbill/58-03/0143/220143.pdf

[6] https://www.gov.uk/government/publications/establishing-a-pro-innovation-approach-to-regulating-ai/establishing-a-pro-innovation-approach-to-regulating-ai-policy-statement#executive-summary

[7] https://www.gov.uk/government/publications/establishing-a-pro-innovation-approach-to-regulating-ai/establishing-a-pro-innovation-approach-to-regulating-ai-policy-statement#executive-summary