December 1st, 2020

TLP White

This week, *Hacking Healthcare* looks at proposed legislation from the United Kingdom (U.K.) that appears to signal the country is resolutely moving forward with the banishment of Huawei from its telecommunications infrastructure. We break down what it means for the U.K., other countries in similar positions, and users of the U.K.'s networks. Next, we briefly reiterate how the blurring of the cyber/physical divide is opening up new attack vectors that draw attention to the need for cyber-biosecurity. Lastly, we provide a quick recap of major findings from the Healthcare Information and Management Systems Society (HIMSS) 2020 Cybersecurity Survey.

Welcome back to *Hacking Healthcare*.

1. **U.K. Seeks to Emphasize Importance of Huawei Removal Through Financial Penalties**

   Earlier this year, the U.K. government signaled a policy reversal by determining it was in the national interest to remove Huawei from critical infrastructure and ensure the company's hardware would be excluded from new 5G telecommunications networks. Last week, Prime Minister Boris Johnson's government signaled just how serious they are by proposing security legislation that would impose significant fines organizations who do not comply with new security requirements by the set deadlines.[1]

   The legislation, entitled the *Telecommunications Security Bill*, would essentially codify the government's decision on Huawei's removal. The bill contains 14 clauses meant to introduce a stronger telecommunication security framework and 9 clauses that "introduce new national security powers for the government to manage risks posed by high risk vendors."[2] It is within the latter clauses that the government lays out significant financial penalties for non-compliance, with "continuing contravention" costing upwards of £100,000 per day.[3] The legislation also formalizes a timeline for the removal of Huawei's equipment that is already installed in the U.K.'s telecommunications infrastructure. According to the legislation, Huawei must be removed in its entirety by 2027.

   As for Huawei, the company has continually attacked government policies aimed at restricting the use of its equipment. Huawei's representatives have stated that these policy decisions are politically motivated and are "not based on a fair evaluation of the risks."[4] They have gone so far as to commission economic research to prove that this decision will ultimately hurt the U.K. and have suggested that with Trump on his way

out, the U.K. may wish to rethink its strategy.[5, 6] The Trump administration has been a fierce proponent of banning Huawei and strongly advocated similar approaches to other allies.

Action & Analysis
H-ISAC Membership Required

2. The Need for Cyber-Biosecurity

From our "We Hadn't Really Considered This Before" department, in a November 27th correspondence to the scientific journal *Nature*, academics and researchers from Ben-Gurion University sought to highlight how cyberattacks could negatively impact the biological research sector through manipulation of DNA synthesis.[7] With so much attention being given to the research and development of COVID-19 treatments and vaccines, the authors' correspondence is a timely reminder of how "cyber dangers are spilling over to the physical space, blurring the separation between the digital world and the real world, especially with automation in the biological lab."[8]

In their piece, the authors outline how a malware attack against biologists' computers could lead to the potential manipulation of DNA sequencing which they claim may go unnoticed because current screening protocol systems are outdated.[9] Additionally, the authors cite the potential for man-in-the-browser attacks against "[s]oftware used to design and manage synthetic DNA projects."[10] This type of attack could lead to the unintentional creation of harmful substances.

How likely such an attack may be is debatable, however the authors did carry out a proof of concept to prove their conclusions' validity. They report that their effort to conduct such an attack was not caught by existing screening software, and the order they created was moved to production before the authors notified relevant authorities and the order was canceled. The authors end their piece by outlining mitigation measures that they feel may prevent this type of attack in the future, including implementing cybersecurity protocols for synthesizers, "such as electronic signatures on orders, and adapt[ing] to provide intrusion detection approaches, ranging from heuristic signatures to artificial intelligence behavioral analysis, to identify malicious code."[11]

Action & Analysis
H-ISAC Membership Required

3. HIMSS 2020 Cybersecurity Survey Results

In case you missed it, HIMSS released their *2020 HIMSS Cybersecurity Survey* in mid-November and its findings are a useful data point for healthcare providers looking to assess the current cybersecurity environment. While the full 32-page document is freely available online from HIMSS, below we've picked out some notable takeaways we felt were worth exploring.

1. Despite early suggestions that cybercriminal and state actors would avoid or minimize their intentional targeting of the healthcare sector during the COVID-19 pandemic, the survey research suggests that significant cybersecurity incidents have become the norm in the healthcare space. HIMSS survey results show that ~70 percent of respondents experienced at least one significant event in the past 12 months.[12] HIMSS was quick to point out that the actual percentage of healthcare entities that experienced incidents this year is likely higher as some organizations may not know or may not wish to publicly disclose such an incident.[13]

2. Concerningly, when evaluating the impact of significant cyber incidents, 15% of respondents reported disruption of systems/devices impacting clinical care, and 3% reported damage or destruction of systems and devices impacting clinical care.[14] Furthermore, of the types of patient safety issues caused by significant security incidents, 28% reported a disruption to emergency services and 17% reported issues that could result in serious patient injury or harm.[15] Lastly, only 39% of respondents felt their organization had effective mechanisms in place to detect patient safety issues related to significant security incidents.[16]

3. While the security of patient data is often highlighted as the most significant concern for healthcare organizations, the HIMSS survey suggests that current threat actors consider targeting patient records a distant third priority (targeted 34% of the time) as compared to financial information (51%) and employee information (48%).[17]

4. Legacy systems are a growing rather than shrinking problem. While acknowledging that there are legitimate reasons for legacy systems to exist, HIMSS found 80% of respondents are employing legacy systems. The recent end of life for Windows 7 appears to be a major culprit of this year's increase.

Action & Analysis
H-ISAC Membership Required

Congress –

Tuesday, December 1st:
- No relevant hearings

Wednesday, December 2nd:
- Senate – Committee on Homeland Security and Governmental Affairs – Subcommittee on Federal Spending Oversight and Emergency Management: Hearings to examine state and local cybersecurity, focusing on defending our communities from cyber threats amid COVID-19.

Thursday, December 3rd:
- No relevant hearings

December 1st, 2020

International Hearings/Meetings –

- No relevant hearings

EU –

Tuesday, December 1st:

- European Commission - Committee on Environment, Public Health and Food Safety

Sundries –

It's hard to keep a big botnet down: TrickBot sputters back toward full health

https://www.cyberscoop.com/trickbot-status-microsoft-cyber-command-takedown/

Personal data of 16 million Brazilian COVID-19 patients exposed online

https://www.zdnet.com/article/personal-data-of-16-million-brazilian-covid-19-patients-exposed-online/

Conferences, Webinars, and Summits –

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

Contact us: follow @HealthISAC, and email at contact@h-isac.org

---

[1] https://www.bbc.com/news/technology-55044182
[2] https://www.gov.uk/government/publications/telecommunications-security-bill-factsheets/factsheet-1-overview
[3] https://www.bbc.com/news/technology-55044182
[4] https://www.bbc.com/news/technology-55044182
[5] https://www.cyberscoop.com/huawei-uk-fines-security-bill/
[6] https://www.bbc.com/news/technology-55044182
[7] https://www.nature.com/articles/s41587-020-00761-y.epdf?sharing_token=WrWwDN-FkOdBex9by7Avv9RgN0jAjWel9jnR3ZoTv0NL8O3FZQt7i2a40oTwYLJPFz184wQMd47k4I9vP_m_KxdkwgB8s3TjKL3CWbYnVQOvuMrx9ODaGZMU7jFPAVy78oCfVyrz0df15z716-fLDxeCHnkIcmF6s88n63V4muk%3D
[8] https://www.nature.com/articles/s41587-020-00761-y.epdf?sharing_token=WrWwDN-FkOdBex9by7Avv9RgN0jAjWel9jnR3ZoTv0NL8O3FZQt7i2a40oTwYLJPFz184wQMd47k4I9vP_m_KxdkwgB8s3TjKL3CWbYnVQOvuMrx9ODaGZMU7jFPAVy78oCfVyrz0df15z716-fLDxeCHnkIcmF6s88n63V4muk%3D
[9] https://www.nature.com/articles/s41587-020-00761-y.epdf?sharing_token=WrWwDN-FkOdBex9by7Avv9RgN0jAjWel9jnR3ZoTv0NL8O3FZQt7i2a40oTwYLJPFz184wQMd47k4I9vP_m_KxdkwgB8s3TjKL3CWbYnVQOvuMrx9ODaGZMU7jFPAVy78oCfVyrz0df15z716-fLDxeCHnkIcmF6s88n63V4muk%3D
[10] https://www.zdnet.com/article/this-new-cyberattack-can-dupe-scientists-into-creating-dangerous-viruses-toxins/
[11] https://www.nature.com/articles/s41587-020-00761-y.epdf?sharing_token=WrWwDN-FkOdBex9by7Avv9RgN0jAjWel9jnR3ZoTv0NL8O3FZQt7i2a40oTwYLJPFz184wQMd47k4I9vP_m_KxdkwgB8s3TjKL3CWbYnVQOvuMrx9ODaGZMU7jFPAVy78oCfVyrz0df15z716-fLDxeCHnkIcmF6s88n63V4muk%3D
[12] https://www.himss.org/sites/hde/files/media/file/2020/11/16/2020_himss_cybersecurity_survey_final.pdf
[13] https://www.himss.org/sites/hde/files/media/file/2020/11/16/2020_himss_cybersecurity_survey_final.pdf
[14] https://www.himss.org/sites/hde/files/media/file/2020/11/16/2020_himss_cybersecurity_survey_final.pdf
[15] https://www.himss.org/sites/hde/files/media/file/2020/11/16/2020_himss_cybersecurity_survey_final.pdf
[16] https://www.himss.org/sites/hde/files/media/file/2020/11/16/2020_himss_cybersecurity_survey_final.pdf
[17] https://www.himss.org/sites/hde/files/media/file/2020/11/16/2020_himss_cybersecurity_survey_final.pdf