March 14, 2022

Hacking Healthcare

TLP White

This week, *Hacking Healthcare* begins with a brief overview of a proposed rule from the Securities Exchange Commission (SEC) that would modify their existing guidance on what SEC registrants would have to publicly disclose related to cybersecurity incidents, cybersecurity policies and procedures, and the cybersecurity expertise of an organization's board of directors. Then we take a look at how the conflict in Ukraine has become the focal point of malicious cyber activity, and what healthcare organizations might be able to learn from it. Welcome back to *Hacking Healthcare*.

1. **SEC Proposes New Cyber Reporting Requirements**

   On March 9th, the SEC "proposed amendments to its rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies."[1] The new proposed rule would significantly expand upon what public companies are required to report on regarding cybersecurity.

   SEC Chairman Gensler noted that the SEC's disclosure requirements have routinely evolved to reflect changes to the risk environment, and that the growth of cyber threats has raised the interest and importance of cybersecurity to investors. The SEC believes this rule would "strengthen investors' ability to evaluate public companies' cybersecurity practices and incident reporting."[2]

   According to the SEC's press release the proposed amendments would:[3]

   - Require current reporting about material cybersecurity incidents on Form 8-K
   - Require periodic disclosures regarding, among other things:
     - A registrant's policies and procedures to identify and manage cybersecurity risks
     - Management's role in implementing cybersecurity policies and procedures
     - Board of directors' cybersecurity expertise, if any, and its oversight of cybersecurity risk; and
     - Updates about previously reported material cybersecurity incidents

- Require the cybersecurity disclosures to be presented in Inline eXtensible Business Reporting Language (Inline XBRL)

The proposal is open to a 60-day public comment period.

Action & Analysis
Included with H-ISAC Membership

2. **Ukraine Conflict Becomes Focal Point for Malicious Cyberactivity**

While the all-out cyberwar that some feared may materialize out of Russia's invasion of Ukraine has not appeared in the West (yet), evidence suggests that the cyber domain is certainly not being ignored by the conflict's combatants. The past few weeks of the conflict provide a glimpse of what the cyber threat landscape looks like outside of peacetime for a major cyber power and a region that is central to the cybercrime ecosystem.

As a Russian invasion of Ukraine looked increasingly likely, numerous government organizations across the globe began to issue warnings and advisories to critical infrastructure and others recommending they heighten cyber defenses and prepare for the possibility of attacks should conflict erupt.[4–5] Since then, the West has not yet seen a deluge of devastating cyberattacks on critical infrastructure and other public and private sector organizations. However, evidence suggests that for Russia and Ukraine, cyber operations have skyrocketed, and cyber activity is intensely focused on those two countries.

According to cybersecurity firm Imperva, on March 10th, roughly 80% of the malicious web traffic and application attacks they have visibility over are targeting Russia (~60%) or Ukraine (~20%).[6] That activity appears to be sustained, as the numbers remained similar with Russia at 59% and Ukraine at 26% on March 14th.[7] Further evidence comes from Quad9, a global public recursive Domain Name System (DNS) resolver, whose general manager reportedly stated that their systems blocked 10 times the normal number of phishing and malware related DNS requests in the region on March 9th.[8]

Action & Analysis
Included with H-ISAC Membership

Congress-

<u>Tuesday, March 15th:</u>
- No relevant hearings

<u>Wednesday, March 16th</u>:
- No relevant hearings

March 14, 2022

Thursday, March 17th:

- House of Representatives - Committee on Energy and Commerce – Subcommittee on Health: Hearing: "The Future of Medicine: Legislation to Encourage Innovation and Improve Oversight"

International Hearings/Meetings –

- No relevant meetings

EU –

Thursday, March 17th:

- European Parliament – Public Hearing: General Data Protection Regulation implementation, enforcement and lessons learned

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, and 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] https://www.sec.gov/news/press-release/2022-39

[2] https://www.sec.gov/news/press-release/2022-39

[3] https://www.sec.gov/files/33-11038-fact-sheet.pdf

[4] https://www.cisa.gov/shields-up

[5] https://www.ncsc.govt.nz/newsroom/gsa-2022-2940/

[6] https://www.nextgov.com/cybersecurity/2022/03/more-80-cyberattacks-worldwide-happening-russia-or-ukraine/362964/

[7] https://www.imperva.com/cyber-threat-attack-map/ (accessed 3/14/2022)

[8] https://krebsonsecurity.com/2022/03/report-recent-10x-increase-in-cyberattacks-on-ukraine/