October 7th, 2021


TLP White

October marks Cybersecurity Awareness Month, a collaborative effort between government and industry to raise awareness about the importance of cybersecurity and to ensure that everyone has the resources they need to be safer and more secure online. As a proud cybersecurity awareness champion, we will be weaving in some weekly themes to our articles this month.

This week, *Hacking Healthcare* begins with a nod to multifactor authentication (MFA). We highlight a new threat to one-time password (OTP) solutions that may have implications for organizations employing OTP as part of their MFA solution. We then provide an update on new developments on incident-reporting legislation in the United States. Finally, we wrap up with a discussion on how some recent news stories alleging a link between cyberattacks in healthcare and patient harm may not be as clear-cut as many seem to imply.

But first, if you are an H-ISAC member, please consider participating in the H-ISAC's upcoming Hobby Exercise. See the details below.

Welcome back to *Hacking Healthcare*.

1. **H-ISAC Hobby Exercise Call for Participation**

   The Hobby Exercise is an annual Healthcare and Public Health (HPH) event designed to engage the sector and its partners on significant security and resilience challenges to inform improvements to planning and response. The second iteration of the Hobby Exercise is scheduled for November 2, 2021, at Venable LLP in Washington, DC. We anticipate 30-50 participants, in person, from the public and private sector. This all-day exercise features keynote speakers, large group discussion, breakout room discussions, lunch, and ample breaks to network. The exercise will be held at TLP Amber to facilitate open discussion on these important matters.

*Participant details:* An inclusive, holistic, multidisciplinary approach provides value to this exercise, and we are looking for diverse representation across the sector. This diversity extends to organization type (e.g., MDM, HDO, etc.), role (e.g., IT/Security, HR, Legal, Comms, etc.), and individual experience level.

*Purpose:* The Hobby Exercise educates participants on the issues within healthcare and how H-ISAC and its members can address, and are addressing, them. This exercise builds enduring relationships within and across the public and private sector that help to strengthen understanding, response, and recovery plans and activities.

To participate in the Hobby Exercise or learn more, please email jbanghart@h-isac.org.

## 2. New Challenges for One-Time Password Security and MFA

Keeping out malicious actors has become increasingly difficult as their capabilities continuously improve over time. While many organizations, thankfully, have acknowledged that a singular reliance on static passwords and knowledge-based questions is no longer adequate to defeat determined attackers, some other forms of authentication often used in MFA are also under threat. According to Intel 471, OTP authentication solutions are being targeted by a growing number of bot-based phishing services.[1]

For context, OTP authentication solutions "rely on a one-time password that is generated in a standalone hardware token, or more commonly today, a smartphone app."[2] These passwords change after a set number of seconds and have traditionally been a significant security improvement. However, a recent post by Intel 471 highlighted "an uptick in services on the cybercrime underground that allow attackers to intercept one-time password tokens."[3]

Services of this nature were reported earlier in the year, with a KrebsOnSecurity post from February examining a service called OTP Agency.[4] According to Intel 471, these new services make use of the Telegram messenger to contact victims while appearing "as a legitimate call from a specific bank and deceive victims into typing an OTP or other verification code into a mobile phone in order to capture and deliver the codes."[5] These phishing types of attacks appear to be very successful, which would help explain the increase in the number of services on the market.

*Action & Analysis*
***Membership required***

### 3. Cyber Incident-Reporting Update

Cyber incident reporting remains a topic of conversation in Congress as lawmakers on both sides of the aisle look to respond to the rise of significant cyberattacks impacting U.S. entities. The newest entrant up for consideration, the *Cyber Incident Reporting Act*, was introduced last week by Sen. Peters (D-MI) and Sen. Portman (R-OH).[6] The bill joins the earlier *Cyber Incident Notification Act,* introduced by Sen. Warner (D-VA), as the two major pieces of legislation on the matter currently circulating in the Senate.[7]

As described by its authors, the *Cyber Incident Reporting Act* would "require critical infrastructure owners and operators to report to the Cybersecurity and Infrastructure Security Agency (CISA) if they experience a cyber-attack, and [would require] most entities to report if they make a ransomware payment."[8] Portman and Peters believe the bill will "improve federal agencies' understanding of how to best combat cyber-attacks, help our nation hold hackers accountable for targeting American networks, and bolster the federal government's ability to help prevent these attacks from further compromising national security and disrupting the lives and livelihoods of Americans."

The bill echoes many of the same concerns from the earlier Warner bill, which would "require federal government agencies, federal contractors, and critical infrastructure operators to notify the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) when a breach is detected so that the U.S. government can mobilize to protect critical industries across the country."[9]

Although both the Portman/Peters bill and Warner bill are bipartisan and tackle the same subject matter, the scope and approach of each bill contain important distinctions, at least in their current form. Some of the more notable differences are the timelines for reporting, the entities covered in the reporting, and the enforcement mechanism.

*Action & Analysis*
***Membership required***

### 4. Calmly Assessing the Impact of Cyberattacks on Patient Outcomes

A new report from the Ponemon Institute on the impact of ransomware on healthcare during COVID-19 alleges that ransomware has increased patient mortality rates. [10] Around the same time, a Wall Street Journal article was published describing how ransomware contributed to a newborn baby's fatal health complications.[11]

Both of these articles have put a spotlight back on fears that cyberattacks are negatively impacting patient outcomes. Unfortunately, these articles are often being distorted and sensationalized, muddying the waters on an issue of real importance and making honest

dialogue among healthcare providers, patients, and lawmakers more difficult. Upon closer inspection of the source material, these stories don't appear nearly as clear-cut as some news headlines portray them.

The Ponemon study, *The Impact of Ransomware on Healthcare During COVID-19 and Beyond,* is a 43-page research report sponsored by third-party risk management firm Censinet.[12] Released in September, the report includes a number of concerning figures about the impact of cyberattacks on healthcare. Most notably:[13]

- 22% of respondents in Healthcare Delivery Organizations (HDOs) who experienced a ransomware attack attested to an "increase in mortality rate"
- 36% of respondents in HDOs who experienced a ransomware attack attested to an "Increase in complications from medical procedures"
- 23% of all respondents attested that the "consequences of cyberattacks on patient care" led to "an increase in mortality rate"

The Wall Street Journal article outlines a lawsuit stemming from health complications suffered by a newborn during a ransomware incident at Springhill Medical Center in Alabama. The lawsuit alleges that Springhill Medical Center "failed to inform the plaintiff about the cyberattack and outage," and that "physicians and nurses at Springhill Medical Center failed to conduct multiple tests prior to the birth … and that those tests were not conducted due to the distraction caused by the ransomware attack."[14] While ransomware may well have contributed to the outcome, it has not been settled in court whether it was a decisive factor.

*Action & Analysis*
***Membership required***

***Congress***

Tuesday, October 5th:
- No relevant hearings

Wednesday, October 6th:
- No relevant hearings

Thursday, October 7th:

October 7th, 2021

- Senate – Committee on Commerce, Science, and Transportation: Hearings to examine the state of telehealth, focusing on removing barriers to access and improving patient outcomes.

***International Hearings/Meetings –***

- No relevant meetings

***EU –***

Monday, October 11th
- EU Parliament - Committee on the Environment, Public Health and Food Safety

***Conferences, Webinars, and Summits –***

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

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

---

[1] https://intel471.com/blog/otp-password-bots-telegram

[2] https://h-isac.org/wp-content/uploads/2021/02/H-ISAC_All-About-Authentication-White-Paper.pdf

[3] https://intel471.com/blog/otp-password-bots-telegram

[4] https://krebsonsecurity.com/2021/02/u-k-arrest-in-sms-bandits-phishing-service/

[5] https://intel471.com/blog/otp-password-bots-telegram

[6] https://www.congress.gov/bill/117th-congress/senate-bill/2875

---

[7] https://www.congress.gov/bill/117th-congress/senate-bill/2407/text

[8] https://www.hsgac.senate.gov/media/majority-media/peters-and-portman-introduce-bipartisan-legislation-requiring-critical-infrastructure-entities-to-report-cyber-attacks

[9] https://www.warner.senate.gov/public/index.cfm/2021/7/following-solarwinds-colonial-hacks-leading-national-security-senators-introduce-bipartisan-cyber-reporting-bill

[10] https://www.censinet.com/thank-you-ponemon-covid-ransomware-impact/

[11] https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116

[12] https://www.censinet.com/thank-you-ponemon-covid-ransomware-impact/

[13] https://www.censinet.com/thank-you-ponemon-covid-ransomware-impact/

[14] https://www.hipaajournal.com/lawsuit-alleges-ransomware-attack-resulted-in-hospital-baby-death/