COVID-19 Requires New Emphasis on Cybersecurity in Healthcare

By Elaina M. Maragakis, JD

The spread of COVID-19 has required us to reexamine and adjust nearly every aspect of our lives. Healthcare cybersecurity is no exception. With the uptick in the spread of COVID-19, experts have seen a corresponding uptick in cybersecurity compromises. This is due to a number of factors, including the increase in remote access arising from work from home arrangements, and opportunities that arise from diverted resources. Given this landscape, it is more critical than ever to shore up your cybersecurity defenses.

Adding Increased Remote Work to the Already Complex Cybersecurity Landscape

Pre-COVID-19, remote work was already increasing at a steady rate, with the healthcare industry leading other industries in the percentage of people working remotely, according to one analysis. A 2019 study by Owl Labs found that "[r]elative to their share of the total workforce," the healthcare industry had the highest percentage (15%) of people who work remotely, as compared with industries such as Technology/Internet (10%), and Financial Services (9%).[1] The top reason for wanting to work remotely was to achieve a "better work-life balance."[2]

Although remote working arrangements were increasing pre-COVID-19, few workers were being trained on *how* to safely work from home. One study reported that in 2019, 38% of remote workers and 19% of remote managers received no training regarding working remotely.[3]

Fast-forward to 2020, and the increase in remote work has grown exponentially, with an estimated 70% increase in remote work in just over two months, from February 4, 2020 to April 7, 2020.[4] The trend does not show signs of waning any time soon. In fact, Global Workplace Analytics estimates that 25-30% of the workforce will be working from home multiple days per week by the end of 2021.[5]

Why the Environment is Ripe for Cyberattacks

The rapid transition to alternative work arrangements has created increased vulnerabilities across all sectors, including health care, particularly given that healthcare information is 50 times more valuable on the underground market than financial information, according to Cybersecurity Ventures.[6] Not only does the healthcare sector have personal information that is *valuable*—names, addresses, birthdates, insurance information, health records—but it also has intellectual property and research, especially relating to COVID-19 that is *priceless*.

On July 16, 2020, Reuters reported on a statement from Britain's National Cyber Security Center which claimed that "[h]ackers backed by the Russian state are trying to steal COVID-19 vaccine and treatment research from academic and pharmaceutical institutions around the world."[7] The obvious value of COVID treatment and vaccine research makes it a vulnerable target. Along the same lines, the World Health Organization has reported a fivefold increase in cyberattacks since the beginning of the pandemic.[8]

It's not just high-profile organizations that are targets. One report noted that more than 93% of healthcare organizations have experienced a data breach in the past three years.[9] Not only can patient data be compromised, but the functionality of wireless medical devices, such as pacemakers and insulin pumps, can also be maliciously manipulated.

How to Help Protect Yourself and Your Workplace

Although organizations should be ever-mindful of keeping pace with entity-wide security and new technology, there are a few immediate, common sense steps that can be easily implemented.

- **Create Policies and Procedures.** Uniform, entity-wide policies establish expectations, and help lend credibility to enforcement efforts. Policies and Procedures also create clear lines of reporting and designate specific individuals to perform specific tasks.
- **Make Sure You Have Cyberinsurance.** Data compromises can be very costly, and those costs can add up quickly. Ensuring adequate insurance and support in the event of a breach can help quickly mitigate damage.
- **Train and Educate Your Employees.** Cyberthreats are ever evolving, so annual training and periodic "refreshers" are helpful in keeping employees up-to-date on emerging threats. Training should include topics such as recognizing phishing emails and best practices (company policy on use of public Wi-Fi, locking screens, etc.). Policies are only effective if they are actually implemented, and training is an effective way to communicate those policies. Specifically focusing on ransomware is critical at this juncture, given that ransomware attacks on healthcare organizations are predicted to grow five-fold by 2021.[10]
- **Provide Real-Time Threat Updates.** Oftentimes, malicious emails are sent to multiple people within an organization. Encourage reporting of suspicious emails and create a system where IT can either delete the email system-wide or send out a cautionary email to prevent other people in the organization from clicking on a malicious link.
- **Understand the Possibility of Insider Threats.** Don't overlook the threats inside your organization, whether intentional or accidental. Ensure that passwords are not shared, and that access is restricted to only those who have a legitimate business need to access information. Lax practices and familiarity can lead to compromises.
- **Ensure Your IT Team Stays Current.** Review protocols with your IT team to ensure that it is current on updates and patches, as well as the latest technology.
- **Manage Passwords Effectively.** Require password changes on a regular basis. This will help mitigate the problematic practice of employees using the same password for multiple accounts, and will also help guard against password breaches. Also consider using two factor authentication (2FA), which requires a second step for credentials after a user enters a username and password.

Heightened vigilance is of paramount importance during this pandemic to ensure that your organization can continue to focus on the healthcare issues, rather than the distractions that necessarily accompany a data breach.

Elaina Maragakis is a litigation attorney at Ray Quinney & Nebeker. Her practice focuses on complex commercial litigation, including contract and business disputes and class actions. She also represents health care entities, including nursing homes and hospitals, in HIPAA analysis litigation and medical staffing issues. Ms. Maragakis chairs RQN's Cybersecurity and Privacy practice group and is CIPP/US certified by the International Association of Privacy Professionals. She assists clients in all aspects of legal compliance with data security laws, including helping companies minimize their risks by preparing Information Security Policies, including Data Breach Response Plans and Employee Data Security Policies. In the event of a breach, she assists with managing a company's compliance with breach notification laws.

1 *State of Remote Work 2019* at 3, published by OWL Labs, available at https://www.owllabs.com/hubfs/Owl%20Labs%202019%20State%20of%20Remote%20Work%20Report%20PDF.pdf.

2 *Id.*

3 *Id.* at 37.

4 Patrick Upatham and Jim Treinen, *Amid COVID-19, Global Orgs See a 148% Spike in Ransomware Attacks; Finance Industry Heavily Targeted*, 4/15/20, VMware Carbon Black Blog, available at https://www.carbonblack.com/blog/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted/.

5 *Work-at-Home After COVID-19-Our Forecast*, Global Workplace Analytics, available at https://globalworkplaceanalytics.com/work-at-home-after-covid-19-our-forecast.

6 *2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics*, available at https://cybersecurityventures.com/cybersecurity-almanac-2019/.

7 William James, Steve Scherer, *Russia trying to steal COVID-19 vaccine data, say UK, U.S. and Canada*, available at https://www.reuters.com/article/us-health-coronavirus-cyber/russia-trying-to-hack-and-steal-covid-19-vaccine-data-says-britain-idUSKCN24H236.

8 *WHO reports fivefold increase in cyber attacks, urges vigilance*, 4/23/20, available at https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance.

9 *2020 Healthcare Cybersecurity Report* at 3, Herjavec Group, available at HerjavicGroup.com.

10 Cybersecurity Ventures, Steve Morgan (Editor in Chief), 4/10/2020, *15 Cybersecurity Statistics To Diagnose The Ailing Healthcare Industry*, available at https://cybersecurityventures.com/15-cybersecurity-statistics-to-diagnose-the-ailing-healthcare-industry/

Advertorial from Ray, Quinney & Nebeker