Cybersecurity Regulation and the Drastic Need for Improvement

Adava Jefferson

These days, everything revolves around the internet and its impact on our daily lives. Advancements have been made allowing for things like groceries to be delivered at the tap of a button, near instant communication with people located around the world through social media, and the ability to find and obtain virtually any consumer product you want in a matter of days from companies like Walmart and Amazon. Unfortunately, while these advances in technology are more than beneficial, they do not come without any drawbacks or vulnerabilities. Using the internet means opening not only yourself, but others in your home, up to potential attacks, such as online viruses and hackers.[1] Everyday people try their best to protect their online security by using passwords to prevent access to their internet and by steering clear of online scams. Therefore, finding different ways to stay safe and protected on the internet means staying up to date on cybersecurity.

Cybersecurity is defined as "the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information."[2] Current effective methods used in cybersecurity include becoming familiar with potential vulnerabilities, keeping software up to date, using strong passwords, and using multifactor authorization.[3] While these methods are extremely useful for staying safe online, cybersecurity regulation varies depending on the location.[4] In 2019, the European Union ("EU") introduced the Cybersecurity Act, which unified their cybersecurity into a single framework that is meant to assist with the increasing growth of the cybersecurity market and ease trade across the EU.[5] Unlike the EU, the United States has not centralized cybersecurity regulation into a lead agency. Instead, the job is split between entities like the Federal Trade Commission (FTC), the Department of Homeland Security (DHS), and the National Institute of Standards and Technology (NIST).[6] The primary laws concerning cybersecurity are the Federal Trade Commission Act (FTCA), which prohibits deceptive practices in business, and the Gramm-Leach-Biley Act (GLB), which requires protection of personal data collected by companies.[7] While the government is working to protect American citizens through these

---

[1] *What is Cybersecurity*, CISA (Feb. 1, 2021), https://www.cisa.gov/news-events/news/what-cybersecurity.
[2] *Id.*
[3] *Id.*
[4] Frank DePrisco, *Cybersecurity Laws and Legislation (2023)*, CONNECTWISE (Feb. 15, 2023), https://www.connectwise.com/blog/cybersecurity/cybersecurity-laws-and-legislation#:~:text=The%20primary%20law%20governing%20cybersecurity,those%20related%20to%20data%20security.
[5] Kaushik Sen, *List of Cybersecurity Regulations in the European Union*, UPGUARD: COMPLIANCE AND REGULATIONS, https://www.upguard.com/blog/cybersecurity-regulations-in-the-european-union#:~:text=The%20EU%20Cybersecurity%20Act,-Introduced%20in%20June&text=The%20Cybersecurity%20Act%20unifies%20the,build%20trust (last updated Aug. 25, 2023).
[6] Frank DePrisco, *Cybersecurity Laws and Legislation (2023)*, CONNECTWISE (Feb. 15, 2023), https://www.connectwise.com/blog/cybersecurity/cybersecurity-laws-and-legislation#:~:text=The%20primary%20law%20governing%20cybersecurity,those%20related%20to%20data%20security.
[7] *Id.*

agencies and regulations, there are other cybersecurity threats out there. Most of which, most people would never think to consider.

In 2018, two researchers, Billy Rios and Jonathan Butts, attempted to bring awareness to Medtronic's vulnerability in their Medtronic MiniMed and MiniMed Paradigm insulin pumps.[8] This specific vulnerability gave potential attackers the ability to hack these pumps and withhold insulin from patients or trigger a lethal dose remotely.[9] After failing to get Medtronic to present a plan to fix or replace the vulnerable devices, Rios and Butts, along with a few other researchers, created a concept app, which acted as a "universal remote" for all of the Medtronic MiniMed and MiniMed Paradigm insulin pumps.[10] This remote was able to connect to various models of the pump by running through possible serial numbers for connection, and, with the help of a signal-booster, it could cover a radius longer than a few feet.[11] A week after the researchers demonstrated this concept app, Medtronic announced its voluntary recall program.[12] The Medtronic insulin pump story is a scary but real illustration of what lack of cybersecurity measures can do to everyday people at a moment's notice.

In case you or someone you love uses an insulin pump with a wireless feature, there is hope. Beginning in October 2023, the FDA will use its power to reject medical devices that lack the appropriate level of "cybersecurity controls and a post-market patching capability."[13] In December 2022, Congress passed an act which included a section on cybersecurity in medical devices.[14] The powers granted by this act went into effect in March 2023, and the FDA gave makers of medical devices a six month grace period to begin compliance.[15] The FDA has "broad authority" to determine the level of cybersecurity and the penalties if a medical device is not compliant.[16] Although this law regulates new devices, it does not address legacy devices that are still floating around the world.[17] While medical devices are starting to become safer because of federal cybersecurity regulation, there are still other areas which need protection.

The Environmental Protection Agency (EPA) is currently in litigation with the states of Missouri, Arkansas, and Iowa.[18] This litigation concerns the EPA's memorandum, released in March 2023, which includes a procedure requiring states to work on their cybersecurity in their water systems.[19] More specifically, states would be required to assess their security as a part of sanitary surveys, which could be done by self-assessment or third-party assessment, amongst other options.[20] This memorandum was released in an effort to comply with the government's

---

[8] Lily Hay Newman, *These Hackers Made an App That Kills to Prove a Point*, WIRED (July 16, 2019), https://www.wired.com/story/medtronic-insulin-pump-hack-app/.
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] Robert Lemos, *Federal Mandates on Medical-Device Cybersecurity Get Serious*, DARK READING: IOT (Sept. 13, 2023), https://www.darkreading.com/iot/federal-mandates-on-medical-device-cybersecurity-mandate-get-serious.
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] Alexandra Kelley, *EPA Withdraws Cyber Audit Requirement for Water Systems*, NEXTGOV/FCW (Oct. 13, 2023), https://www.nextgov.com/cybersecurity/2023/10/epa-withdraws-cyber-audit-requirement-water-systems/391205/.
[19] Ashden Fein, Micaela McMurrough, Caleb Skeath & Matthew Harden, *EPA Requires States to Address the Cybersecurity of Public Water Systems*, COVINGTON: INSIDE ENERGY & ENVIRONMENT (Mar. 7, 2023), https://www.insideenergyandenvironment.com/2023/03/epa-requires-states-to-address-the-cybersecurity-of-public-water-systems/.
[20] *Id.*

new cybersecurity strategy.[21] The states of Missouri, Arkansas, and Iowa later challenged the EPA's requirement of sanitary surveys.[22] Due to this ongoing litigation, in October 2023, the U.S. Court of Appeals for the Eight Circuit ordered a halt on the enforcement of this memorandum.[23] Although the EPA can no longer, at least temporarily, regulate state cybersecurity in water systems through sanitary surveys, the agency is still working to continue to "support states, drinking water systems, and wastewater systems by providing that technical assistance in the form of cybersecurity risk assessments, subject matter expert consultations, and training."[24]

At the end of the day, using cybersecurity methods is a choice we, as individuals, decide to make every day. Our employers may also decide to use these cybersecurity methods, but what happens when big companies decide they do not want to put in the extra work or money needed to maintain cybersecurity? Do we wait for the government to impose regulations on cybersecurity, or do we wait for the worst case scenario which spurs action? How will we enforce these potential regulations, and more importantly, who will decide where to draw the line? These are all questions that I hope will be discussed and determined in the near future, not only for now, but for the generations to come.

---

[21] *Id.*
[22] Alexandra Kelley, *EPA Withdraws Cyber Audit Requirement for Water Systems*, NEXTGOV/FCW (Oct. 13, 2023), https://www.nextgov.com/cybersecurity/2023/10/epa-withdraws-cyber-audit-requirement-water-systems/391205/.
[23] *Id.*
[24] *Id.*