MINNESOTA STATE BAR ASSOCIATION

APRIL 2023

BENCH + BAR of Minnesota

MINNESOTA'S RACIALLY BIASED JURY POOLS AND HOW TO FIX THEM

The shifting emphasis of U.S. CYBERSECURITY

BY MARK LANTERMAN ✉ *mlanterman@compforensics.com*

MARK LANTERMAN is CTO of Computer Forensic Services. A former member of the U.S. Secret Service Electronic Crimes Taskforce, Mark has 28 years of security/forensic experience and has testified in over 2,000 matters. He is a member of the MN Lawyers Professional Responsibility Board.

On March 2, the Biden-Harris administration released its National Cybersecurity Strategy.[1] The strategy outlines key steps needed to create a more secure, resilient cyberspace, acknowledging that "cybersecurity is essential to the basic functioning of our economy, the operation of our critical infrastructure, the strength of our democracy and democratic institutions, the privacy of our data and communications, and our national defense."

Two shifts are described as necessary in reshaping and strengthening cyberspace. The first requires a rebalancing of responsibility—specifically, that those organizations in the best position to effect change in our digital landscape are called upon to do so, rather than individuals or small businesses. The strategy lays out the role of regulation in balancing innovation with liability and articulates a movement away from placing the brunt on consumers.

Cybersecurity and Infrastructure Security Agency Director Jen Easterly recently urged businesses to prioritize consumer security, suggesting legislation be created to "prevent technology manufacturers from disclaiming liability by contract, establishing higher standards of care for software in specific critical infrastructure entities, and driving the development of a safe harbor framework to shield from liability companies that securely develop and maintain their software products and services."[2] Our digital age could be generally described as a kind of Wild West, with heavy reliance upon technology with relatively few safeguards. There seems always to be a temptation to view the dangers associated with our digital world as hypothetical and somehow separate from our "real lives." As we are now seeing, this characterization is becoming increasingly unacceptable; businesses are being held accountable for their products and consumers are no longer expected to accept the same degree of risk. Jen Easterly pointed to Apple's security policies as a strong example for other technology companies to follow, including its widescale use of multi-factor authentication. These sorts of measures are moving from "preferred" to "mandatory," much as the installation of seat belts did in the years after their introduction.

> "CYBERSECURITY IS ESSENTIAL TO THE BASIC FUNCTIONING OF OUR ECONOMY, THE OPERATION OF OUR CRITICAL INFRASTRUCTURE, THE STRENGTH OF OUR DEMOCRACY AND DEMOCRATIC INSTITUTIONS, THE PRIVACY OF OUR DATA AND COMMUNICATIONS, AND OUR NATIONAL DEFENSE."

In addition to building cybersecurity into products and software, "The Administration supports legislative efforts to impose robust, clear limits on the ability to collect, use, transfer, and maintain personal data and provide strong protections for sensitive data."[3] Unlike previous approaches, this strategy points to mandatory standards as a way to establish consistent improvement, especially in upholding consumer protections. Underscoring these efforts is a need for private and public sector cooperation, information sharing, and shared responsibility.

Similarly, the second shift highlights the need to incentivize and balance long-term cyber goals with short-term, necessary improvements to existing technology. Proactive cybersecurity systems and policies, education, research programs, and the establishment of a diverse cyber workforce are all components of how the U.S. government plans to make itself an example of cybersecurity investment and modernization. This will be especially evident as it works to better secure critical sectors; consider, for instance, the government's proactive investment in a new energy infrastructure. In addition to adopting a zero-trust architecture (involving the implementation of multi-factor authentication, encryption, and more stringent access controls, among other advancements), the strategy also describes the federal government's need to "replace or update IT and OT systems that are not defensible against sophisticated cyber threats."

One such threat described in the report is ransomware. It would have been discussed in the report in any case, but as it happened, this strategy was released in the wake of a ransomware attack on the U.S. Marshals Service. In February the Service revealed that it had been the victim of "a ransomware and data exfiltration event"[4] in which sensitive data had been compromised. A huge concern was that this hack would have breached information related to the Federal

Witness Security Program, but thankfully, it seems that this information has been kept secure.[5] While many details have not been reported, it might be that the attackers were not financially motivated. As noted in an NPR report, "If no ransom was demanded, that could speak to the potential hidden motivation. Nation-state adversaries including Iran and Russia have launched destructive attacks designed to look like ransomware in an effort to cover up efforts to steal intelligence or cause disruption in the past."[6] Though much about the attack remains unclear (or undisclosed), the elements laid out in the National Cyber Strategy to combat ransomware should be considered in preventing or mitigating future attacks:

1. leveraging international cooperation to disrupt the ransomware ecosystem and isolate those countries that provide safe havens for criminals;
2. investigating ransomware crimes and using law enforcement and other authorities to disrupt ransomware infrastructure and actors;
3. bolstering critical infrastructure resilience to withstand ransomware attacks; and
4. addressing the abuse of virtual currency to launder ransom payments.

These components work together in making ransomware a less profitable venture for cybercriminals, combined with a general prohibition against paying ransoms when they are requested.

The next steps for the strategy will be published in a subsequent implementation plan. The effectiveness of the action items and national progress toward long-term improvement will be assessed, and lessons learned from cyber incidents will continue to be incorporated. It is encouraged that big-picture security reviews—for example, those created by the Cyber Safety Review Board[1]—are also utilized by private companies. ▲

NOTES

[1] *https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf*

[2] *https://www.cnbc.com/2023/02/27/cisa-director-praises-apple-security-suggests-microsoft-twitter-need-to-improve.html*

[3] *https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf*

[4] *https://www.nbcnews.com/politics/politics-news/major-us-marshals-service-hack-compromises-sensitive-info-rcna72581*

[5] *https://www.npr.org/2023/02/28/1160112051/hackers-steal-sensitive-law-enforcement-data-in-a-breach-of-the-u-s-marshals-ser*

[6] *https://www.npr.org/2023/02/28/1160112051/hackers-steal-sensitive-law-enforcement-data-in-a-breach-of-the-u-s-marshals-ser*