Dr. Stephen Leffler
President and Chief Operating Officer
The University of Vermont Medical Center

Written testimony for the joint hearing before:
The Subcommittee on Cybersecurity, Information Technology, and Government Innovation; and
The Subcommittee on Economic Growth, Energy Policy, and Regulatory Affairs.
September 27, 2023 at 1:00 pm in room 2154 of the Rayburn House Office Building

Written testimony:

On October 28, 2020, the UVM Medical Center was the victim of a cyberattack. The UVM Medical Center had strong security defense in place and had protected itself against many other attack attempts before, but unfortunately this one got through.

Ransomware was discovered after we experienced operability issues on computers and network systems at the hospital. As soon as we realized UVM Medical Center was experiencing a system-wide outage, we took several steps:

- First, we cut off all internet and other access both to and from UVM Medical Center.
    - To prevent any further access from supposed attackers
    - To prevent spread of the malware to other hospitals within the UVM Health Network (UVM Medical Center is part of a six hospital health system) and to our many partners and vendors. We successfully prevented any spread of the malware and outage from UVM Medical Center to any other partner hospitals within the Network.
- Second, we took Epic, our electronic health record, offline. Epic was not impacted by the cyberattack, but we wanted to make sure the malware did not spread to Epic.
- The third thing we did we was to engage Cisco Talos, a third party expert on cyberattacks that we had on retainer, to assist us with the analysis and recovery.
- Finally, we reached out to local and national law enforcement agencies. In particular, the FBI was extremely helpful and supportive throughout the attack and recovery. Our entire team was also deeply grateful to Governor Phil Scott and the Vermont National Guard for their support during the cyberattack response and recovery.

There were two major impacts of the cyberattack on UVM Medical Center:

- First, the malware encrypted the files and data for virtually our entire infrastructure and for most of our application servers.
    - We had good backups for essentially all of these 1,300+ servers, but we had to completely wipe them clean to remove the malware, and then rebuild our entire infrastructure.

    - For an organization of our size, that was a huge undertaking. It was quite literally a 24 hours a day, 7 days a week effort, and it took us, along with our partners, the first entire month to complete that work.
- The second major impact was that the attack deposited malware on over 5,000 end user devices – computers and laptops.
    - We had to completely wipe all of those devices and reimage them in order to eliminate the malware from our environment, which was also a huge undertaking.

Our team's collective response:

The UVM Medical Center learned and adapted with each curve of the cyberattack, much like we learned with each curve of the COVID-19 pandemic. Our collective teamwork approach is what got us through, day by day. Our team was already more than seven months into Vermont's statewide pandemic response when the cyberattack occurred, and our colleagues were already stressed and exhausted. But what I saw in the halls of our hospital as soon as we knew something was amiss, was nothing short of extraordinary. Tenured physicians and nurses were teaching new health care providers and new graduates how to chart and make orders on paper. Our administrative leaders donned comfortable sneakers and staffed clinical floors to, quite literally, run test results from labs to providers. We purchased walkie talkies for leaders to be able to communicate, and we spread information to staff and board members via telephone chains and text threads. Our approach was to share what we knew, when we knew it – even when there were few additional details we could share. I will always be extremely proud of UVM Medical Center's response to the cyberattack – which from the very first moment was collaborative and showed our care and respect for each other, while prioritizing the best possible care for our patients.

Resolution:

- To restore our infrastructure, we had to ensure we had a clean environment to bring our applications back up, including Epic.
- We have over 600 applications across UVM Medical Center. We worked with our clinical and operational leaders to prioritize the order to restore those applications based on clinical impact.
    - All of those applications were back in full production by early January 2021.
- We are confident that none of our patient or employee data was accessed or extracted. We looked at this very carefully, and we retained experts to conduct a forensic analysis. This is thanks to the quick steps our IT experts took to contain the invasive software and prevent a malignant spread across our systems
- We have learned a lot of lessons from this experience – lessons that we have been sharing with the rest of our health care industry. We had strong security processes in place and had deployed a variety of tools to block malware attacks, yet we were still the victim of a cyberattack. This really is an arms race. As we have all seen in the news over the past few

years, the cyber criminals and actors are getting increasingly sophisticated, and so this important work to protect our systems will never be fully finished. We all are going to have to stay vigilant and continually update our tools and approaches to stay ahead of cyberattacks, and that will continue to be a high priority for the UVM Medical Center and the UVM Health Network going forward.