COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 30, Number 21. June 07, 2021
Tactics Get Uglier As Ransomware Attacks Rise; Forensic Reviews Help Get Hackers Out

By Nina Youngstrom

The dollar amounts demanded in ransomware attacks and the viciousness of some tactics used to persuade organizations to part with the ransom are escalating, experts say, highlighting the magnitude of the cyber challenges they face. That raises the stakes for layered security, which has become more affordable, and for forensic investigations to help eject hackers from your computer systems if they manage to get a foothold.

"The problem is, it's really difficult to stop," said Scott Wrobel, managing member of N1 Discovery, a digital forensics and cybersecurity firm. "They make so much money on a daily or weekly basis, it's hard for any company or country to stop this from happening. The only way is to have all companies understand what their obligations are and take the time and effort to perform information technology properly and make sure they're not vulnerable. It's a cultural shift." In a June 2 memo to corporate executives and business leaders,[1] the Biden administration urged them to drive down risk of ransomware attacks and outlined best practices. "Strengthening our nation's resilience from cyberattacks—both private and public sector—is a top priority of the President's," the memo stated.

One of Wrobel's clients was recently hacked by DarkSide, the same ransomware group that shut down Colonial Pipeline, which supplies almost half the gas and fuel to the East Coast. DarkSide demanded $15 million from Wrobel's client in exchange for the decryption key to unlock its data. "We didn't pay the ransom because we were able to recover without the decryption key, but the tactics they used were very intrusive," he said April 21 at the Health Care Compliance Association's Compliance Institute.[2] The hackers sent employees "grotesque" pictures, including decapitated bodies, to scare them and pressure the company to pay the ransom. As miserable as this was, the company didn't cave, and ultimately its data was released on the dark web. "We are seeing this trend now because they are not getting paid the ransom," he explained. Another ransomware group, Carbon Spider, has been calling employees to threaten them with bodily harm when their bosses won't pony up and then texting violent pictures. "The first decision on whether to pay the ransom is whether you can recover without paying, knowing you will be hit with some other issues," Wrobel said. "It should all be discussed."