Greg and Dan Show April 24, 2023

Can a Judge Force a Hospital to Pay the Ransom for a Cyber Attack?

- Lehigh Valley Health Network, based in Allentown, Pennsylvania, was hacked in February by the ransomware gang known as BlackCat, which has been associated with Russia.
    - BlackCat is demanding over $5M in ransom.
    - Lehigh Valley Health Network refuses to pay the ransom.
- Naked photos of patients taken during cancer treatment appeared in early March on an online forum used by BlackCat.
    - This is a common practice used by ransomware groups to prove they did breach the target company.
    - It puts additional pressure on the victim company to pay the ransom before more data is released to the public.
- One of the patients, whose photos were exposed, filed a lawsuit on March 13th to force Lehigh Valley Health Network to pay the ransom to get the photos taken off the internet.
- The patient is going by the name Jane Doe to protect her own identity.
- It's not uncommon for victims of ransomware to sue the company that had the breach, but this is the first case I have heard of where the lawsuit is trying to force the company to pay the ransom.
- Other photos posted online also showed patients naked and are now searchable by patient name.
- In a court filing submitted on April 5, Mary Ann La Rock, Lehigh Valley's chief compliance officer, said the healthcare network has identified around 2,760 people whose "***clinically appropriate photographs***" were stolen during the cyberattack.
- Jane Doe, who underwent treatment for breast cancer, said she did not even know the hospital took the pictures, much less that they were released on the internet.
- The lawsuit accuses Lehigh Valley of violating cybersecurity and privacy rules including requirements under the Health Insurance Portability and Accountability Act, or HIPAA, to protect patient data.

- Companies that pay ransoms to Russia-based hackers could be violating U.S. sanctions against Russia-based cybercrime groups.