March 25 2023 ByLaws, Policy & Procedures Committee

Rob Heaney sought guidance for the security of CVPCSD water and billing systems, finding a great local advisor in Deborah Curtis

Placer Co Chief Information Security Officer
1-530-889-4232
dcurtis@placer.ca.gov

Talking with Deborah, it's clear that our customer's banking info is only a part of the security concern; in fact our water treatment and delivery system is considered part of the National Critical Infrastructure.

She proved to be an invaluable resource, and with her CVPCSD has the opportunity to create a local partnership with a large and mature security structure. She is also professionally connected to the National and International security community. This connection vastly leverages our access to security knowledge and best practices.

The following is a list of observations and suggestions Deborah had for a start, which should ensure we're well along to a hardened organization. There is much more to the matter but here's a good start.

- Ransomware is a big concern. The measures on this page help foil attacks.
- There is a "Nationwide Cyber Security Review" self test (conducted by DHS, CISA Cyber and Infrastructure Security Agency) in the Fall that we are encouraged to take part in. It costs nothing and gives us an opportunity to get a deeper, personalized understanding of our system. The Placer Co IT office will be part of this.
- Remote access points are potential security weaknesses. This includes cell phones, computers, the web site, etc.
- Make sure to keep firmware and software patched (for example MicroSoft Tues patches) on all devices in the system. This is a biggie.
- Set all passworded access to two factor authentication. Also a biggie.
- Make sure all passwords are complex. Think "s&e92$nGS2q5#" instead of our dog's name or 'Password123'. Yet another biggie.
- Look for ALL internet connected components throughout the system (cameras, remotely accessible pumps or valves, gates, etc) and change passwords from factory default to complex new ones.
- Another self test, "Requesting Cyber Hygiene Services", conducted by CISA, is available. Procedure consists of a questionnaire, then a test around a week after completion. Questionnaire should be arriving at Rob's email address and will be forwarded to appropriate personnel when it arrives. This is cost free and anonymous, and there is no obligation to participate, but it looks like another valuable self assessment tool for us. Web address: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services
- Another valuable ransomware security website: https://www.cisa.gov/stopransomware