Digital Risk: Remote-Monitoring, IoT Sensors and Data Integrity Picture This





This image shows the control room of a small municipal water treatment facility during a routine morning shift. A single plant operator is seated at a workstation with two monitors displaying the facility's SCADA dashboard — chemical levels, flow rates, and system status all reading normal in green. The operator is filling out paperwork and glancing occasionally at the screen. Without warning, the cursor on the right monitor begins to move on its own. A dropdown menu opens. A chemical dosing value begins to change — sodium hydroxide climbing rapidly from 100 parts per million toward a number the operator has never seen entered before. He leans forward, staring at the screen.

What is happening in this image is not a equipment malfunction or a sensor error — it is a person somewhere else in the world, right now, adjusting the chemical levels of a water supply for 15,000 people from a keyboard the operator cannot see or stop. The remote monitoring system that was installed to make this facility easier to manage has become the access point through which a lethal chemical change is being made in real time. No alarm has sounded. No authentication request has appeared. The system accepted the connection because it had no way to tell the difference between an authorized employee and an attacker. Digital systems that control physical safety outcomes must be treated with the same rigor as any other safety-critical control — because when they fail, the consequences are not data losses. They are chemical burns, injuries, and deaths.