Water Utility Attacks Reinforce Need for Continuous Cyber Risk Management Secure Halo Says

August 28, 2026

SILVER SPRING, MD - August 28, 2026 -
Secure Halo said the recent attacks reinforce the need for organizations to continuously identify and manage cyber risk across operational technology, third-party access, and other interconnected systems following a joint advisory issued by the Cybersecurity and Infrastructure Security Agency, the FBI, and the Environmental Protection Agency on July 30, 2026, describing a significant escalation in attacks against internet-exposed water utility control systems. The firm said the incident illustrates the type of exposure it has focused on for clients across regulated and critical infrastructure sectors.

The advisory followed a coordinated attack over the weekend of July 26 to 27, 2026 that disrupted operational technology at more than 30 municipal water and wastewater utilities in Minnesota, with confirmed incidents reaching utilities in at least seven states including Michigan. According to officials, attackers changed device passwords to lock operators out of programmable logic controllers and altered equipment settings, forcing several utilities to switch to manual operation and, in some cases, issue boil water notices. No incidents of water contamination have been reported as a result of the activity.

CISA had updated a related advisory, AA26-097A, on July 22, 2026, days before the Minnesota incidents

began, expanding the scope of documented exploitation beyond one manufacturer's controllers to include additional devices from Schneider Electric and Siemens, and noting for the first time that attackers had exfiltrated controller project files. Investigators have also pointed to undocumented cellular modems installed by operators, vendors, or system integrators as an overlooked entry point into control networks that utilities did not know existed. Formal attribution has not been announced, though researchers have noted similarities to previously documented campaigns linked to Iranian-affiliated actors.

CISA's guidance to affected organizations has centered on removing publicly exposed control devices from the internet and auditing third-party and vendor-installed remote access points that may not appear in a utility's own network documentation. Secure Halo said the underlying problem extends well beyond water utilities. Unmanaged assets, vendor connections, remote access pathways, and other undocumented dependencies can create risk across education, healthcare, financial services, manufacturing, government, and other sectors. The firm said these exposures reinforce the importance of treating cyber risk as something that must be continuously identified, prioritized, and managed rather than periodically assessed. The attacks reinforce an approach Secure Halo has increasingly emphasized across its client base: maintaining visibility as technologies, vendors, vulnerabilities, and access pathways change over time.

"Organizations can't manage cyber risk they can't see. These incidents demonstrate why cybersecurity has to extend beyond periodic assessments of known systems. Assets change, vendors change, access changes, and vulnerabilities change. Effective risk management requires continuous visibility into those changes and a process for acting on them," said Richard Osborne, Director of Commercial Services at Secure Halo.

Secure Halo is an enterprise cyber risk and cybersecurity services firm operating as a Mission Critical Partners company. The firm helps organizations identify, prioritize, reduce, and continuously manage cyber risk, through services spanning vCISO leadership, cybersecurity assessment, vulnerability management, managed detection and response, penetration testing, compliance management, insider threat, and third-party risk management. The firm works with organizations across education, financial services, government, healthcare, insurance, manufacturing, public safety, and utilities, with a client roster that has included Fortune 500 companies, state government agencies, and federal contractors. The firm's approach centers on moving organizations beyond point-in-time assessments and checkbox compliance toward continuous visibility, prioritized risk reduction, and measurable improvement in cybersecurity maturity.

More information is available at securehalo.com.

###

For more information about Secure Halo, contact the company here:Secure HaloErin Webb202-629-1960info@securehalo.com962 Wayne Ave, Suite 310, Silver Spring, MD 20910

```
{
  "@context": "https://schema.org",
  "@type": "Organization",
  "name": "Secure Halo",
  "url": "https://securehalo.com/",
  "logo": "https://securehalo.com/wp-content/uploads/2025/01/securehalo-logo.png",
  "contactPoint": [
    {
      "@type": "ContactPoint",
      "telephone": "+1-202-629-1960",
      "contactType": "Customer Service",
      "email": "info@securehalo.com",
      "areaServed": "US"
    },
    {
      "@type": "ContactPoint",
      "telephone": "+1-301-304-1700",
      "contactType": "Sales",
      "email": "info@securehalo.com",
      "areaServed": "US"
    }
  ],
  "address": {
    "@type": "PostalAddress",
    "streetAddress": "962 Wayne Ave, Suite 310",
    "addressLocality": "Silver Spring",
    "addressRegion": "MD",
    "postalCode": "20910",
    "addressCountry": "US"
  },
  "sameAs": [
    "https://www.linkedin.com/company/secure-halo/",
    "https://twitter.com/SecureHalo",
    "https://www.facebook.com/SecureHalo",
    "https://www.youtube.com/@SecureHalo"
  ],
  "foundingDate": "2002-01-01",
  "founder": {
```

"@type": "Person",
"name": "Secure Halo Leadership Team"
},
"parentOrganization": {
"@type": "Organization",
"name": "Mission Critical Partners"
},
"description": "Secure Halo provides trusted, proactive cybersecurity solutions to protect organizations? data, infrastructure, and business continuity. With expertise across industries including government, healthcare, finance, manufacturing, and utilities, Secure Halo offers services such as vCISO, cybersecurity assessments, managed detection and response, compliance support, penetration testing, insider threat management, and third-party risk management."
}

Secure Halo

Secure Halo delivers trusted, proactive cybersecurity solutions?protecting data, infrastructure, and business continuity through services like vCISO, assessments, MDR, compliance, penetration testing, insider threat, and third-party risk management.

Website: https://www.securehalo.com/

Email: info@securehalo.com

Phone: 202-629-1960

SECURE HALO

SECURING THE ENTERPRISE

A **Mission Critical Partners** Company