JPIASource

SUMMER 2026 VOLUME 8 ISSUE 3 ACWA JPIA RISK MANAGEMENT FOR THE WATER INDUSTRY

Cybersecurity

Best Management Practices

KnowBe4 KYND

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

ACWA JPIA

According to the Federal Bureau of Investigation (FBI), California ranks first in the United States for internet crime complaints, with victims reporting losses totaling more than $2.5 billion in 2024. Two of the top three cybercrime complaints were extortion and phishing/spoofing. The JPIA provides Cybersecurity Resources and Best Management Practices (BMPs) for prevention, detection, and response to support water agencies participating in the Liability Program.

Public agencies, including California water agencies, conduct some portion of their daily business online, and more agencies are expanding their digital presence, which can heighten vulnerability and increase the risk of cyber threats. Common cyber risks facing water agencies include phishing attempts and vendor impersonation fraud.

Phishing

According to Merriam-Webster, phishing is “the practice of tricking Internet users (as through the use of deceptive email messages or websites) into revealing personal or confidential information which can then be used illicitly.” Employees are the primary target of phishing attacks within water agencies. Some common types of phishing that an agency may experience include:

- Deceptive emails (Email Phishing)
- Targeting specific people (Spear Phishing)
- Phone calls (Vishing)
- Text messages (Smishing)

A successful phishing attack can have lasting consequences for a water agency, including data breaches and security compromises. The JPIA encourages members to prevent and mitigate the effects of phishing attacks by:

- Combining technical defenses such as email filters, Multifactor Authentication (MFA), and anti-virus software.
- Developing strong policies and procedures.
- Continual employee education.
- Strong security habits such as unique passwords and backups.

Vendor Impersonation Fraud

One specific form of phishing affecting water agencies is vendor impersonation fraud. These attempts typically aim to divert payments to existing vendors by falsifying payment routing information. Victims unknowingly pay scammers instead of their vendors. These scams can go undetected until the organization receives a legitimate payment dispute from its vendor.

Tips to avoid vendor impersonation fraud include:

- Check email details by looking closely at the sender's email address and domain.
- Call vendors by using a phone number from your existing records to confirm any changes to payment routing information.
- Ensure all employees use a personnel change request form to formally request a change in payroll, banking, change of address, etc.
- Report all suspected fraud attempts according to agency policies and procedures.
- Ensure all employees are trained to recognize phishing attempts, spoofed emails, and social engineering tactics.

Multifactor Authentication (MFA)

MFA, also known as two-factor authentication, is a security control that combines two or more authenticators to verify a user's identity before granting access to a system. When enabled, MFA makes it harder for unauthorized individuals to gain access to networks and information systems, including Supervisory Control and Data Acquisition (SCADA) systems, billing systems, and email.

Cybersecurity remains a growing and evolving risk for water agencies. The JPIA is committed to supporting our members by providing resources to reduce these risks. **Section 26** of the JPIA's Risk Control Manual offers cybersecurity resources to help agencies recognize future phishing attempts. Resources from agencies such as CISA also provide vital information and tools to manage risks and strengthen national cybersecurity.

Additionally, the JPIA provides third-party cybersecurity resources to members participating in the Cyber Liability Program through our partnerships with KnowBe4 and KYND. KnowBe4 provides simulated email phishing camgaigns and training to help your Agency's staff to mitigate against cyber threats. KYND scans member domains and provides the results in an easy-to-read dashboard intended to monitor and track cyber exposures within your Agency's network. For more information, please contact the JPIA's Cybersecurity Risk Specialist, Hunter Sargent.

Frequently Asked Questions

1) What is the difference between MFA and 2FA?
2FA uses two factors of authentication while MFA may have additional security layers.

2) What should I do if I get an MFA prompt I didn't initiate?
Deny it immediately and report it. Repeated prompts may indicate someone has your passwords.

3) What is spear phishing?
Targeted phishing is directed at a speci ic person or department.

4) Can phishing happen through text or phone calls? **Yes.**
Smishing = SMS phishing
Vishing = Voice phishing

5) What is vendor impersonation fraud?
When a scammer pretends to be a legitimate vendor and requests changes to payment details (such as new banking details).

6) How do attackers impersonate vendors?

- **Spoofed email addresses**
- **Compromised vendor accounts**
- **Slight domain changes (e.g., .co instead of .com)**

7) What is the biggest red lag when dealing with vendor impersonation?
Urgent requests to change payment instructions or to wire funds quickly.

8) How should we verify changes to vendor payments?
Always con irm using a known phone number (not the one in a suspicious email).

Photo credits: JPIA; Envato; Jean-Phillippe Delbergheon-Unsplash; Maulana-ahmad-Akc9RvLoAOw-Unsplash

JPIASource

The *JPIA*Source is not intended to be exhaustive. The discussion and best practices suggested herein should not be regarded as legal advice. Readers should pursue legal counsel or contact their insurance providers to gain more exhaustive advice.

P.O. Box 619082 | Roseville | CA 95661-9082
(800) 231-5742 | www.acwajpia.com