Incident Action Checklist – Cybersecurity

For on-the-go convenience, the actions in this checklist are divided up into three "rip & run" sections and provide a list of activities that water and wastewater utilities can take to prepare for, respond to and recover from a cyber incident. You can also populate the "My Contacts" section with critical information that your utility may need during an incident.

Cyber Incidents and Water Utilities

Cyberspace and its underlying infrastructure are vulnerable to a wide range of hazards from both physical attacks as well as cyberthreats. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy or threaten the delivery of essential services such as drinking water and wastewater.

As with any critical enterprise or corporation, drinking water and wastewater utilities must evaluate and mitigate their vulnerability to a cyber incident and minimize impacts in the event of a successful attack. Impacts to a utility may include, but are not limited to:

- Interruption of treatment, distribution or conveyance processes from opening and closing valves, overriding alarms or disabling pumps or other equipment
- Theft of customers' personal data such as credit card information and social security numbers stored in on-line billing systems
- Defacement of the utility's website or compromise of the email system
- Damage to system components
- Loss of use of industrial control systems (e.g., SCADA system) for remote monitoring of automated treatment and distribution processes

Cyber incidents can compromise the ability of water and wastewater utilities to provide clean and safe water to customers, erode customer confidence and result in financial and legal liabilities. The following sections outline actions drinking water and wastewater utilities can take to prepare for, respond to and recover from cyber incidents.

Actions to Prepare for a Cyber Incident

Utility

- [ ] Identify all mission critical information technology (IT) systems, considering business enterprise, process control and communications. Document the key functions of the mission critical objectives, and identify the personnel or entity responsible for operating and maintaining each IT system.

- [ ] Identify an overall IT security lead to coordinate with each IT system manager and oversee all cyber-related duties.

- [ ] Ensure that IT system managers enforce cybersecurity practices on all business enterprise, process control and communications systems. For example, verify adherence to user authentication, current anti-virus software and installation of security patches.

- [ ] Identify priority points of contact for reporting a cyber incident and requesting assistance with response and recovery. Include any state resources that may be available such as State Police, National Guard Cyber Division or mutual aid programs, as well as the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) at https://www.cisa.gov/reporting-cyber-incidents.

- [ ] Review and update the utility's emergency response plan (ERP) to address a cyber incident impacting business enterprise, process control and communications systems. Account for all potential impacts on operations, and ensure emergency contacts are current.

- [ ] Prevent unauthorized physical access to IT systems through security measures such as locks, sensors and alarms. Include workstations and process control systems (e.g., programmable logic controllers or PLCs).

- [ ] Train all essential personnel to perform mission critical functions during a cyber incident that disables business enterprise, process control and communications systems. Include the manual operation of water collection, storage, treatment and conveyance systems.

- [ ] Conduct drills and exercises for responding to a cyber incident that disables critical business enterprise, process control and communications systems.

Actions to Prepare for a Cyber Incident *(continued)*

IT Staff or Vendor

- ☐ Establish a program for maintaining updated anti-virus software on all critical IT systems, along with rapid installation of all security patches.
- ☐ Set up an automatic back-up on critical systems and ensure the process is producing a readable, uncorrupted restore file on a routine basis.
- ☐ Implement rigorous user authentication, including multi-factor authentication where possible. Use individual accounts and unique passwords for each employee, and restrict IT system access privileges to the level needed for a user's duties.
- ☐ Restrict internet access to process control systems unless absolutely necessary.
- ☐ Where possible, separate process control system traffic from business traffic through the use of a firewall. If this is not possible, logically filter traffic through the use of a firewall.
- ☐ Identify all routes of remote access to IT systems. Eliminate remote access where possible, and restrict remaining access (e.g., do not allow persistent remote access to control networks).
- ☐ Assess the use of additional strategies to protect IT systems, such as application whitelisting, network segmentation with restricted communication paths and active monitoring for adversarial system penetration.
- ☐ Conduct a detailed assessment of vulnerabilities in all mission critical IT systems. Consider use of the tools and subject matter experts provided by the DHS Cybersecurity and Infrastructure Security Agency (https://www.cisa.gov/cybersecurity). Develop an action plan to mitigate all significant vulnerabilities identified in the assessment.

Notes:

Actions to Respond to a Cyber Incident

Utility

- [ ] If possible, disconnect compromised computers from the network to isolate breached components and prevent further damage, such as the spreading of malware. Do not turn off or reboot systems – this preserves evidence and allows for an assessment to be performed.
- [ ] Notify IT personnel and/or IT vendor of the incident and the need for emergency response assistance. In addition, DHS CISA can assist with IT system response and recovery (https://www.cisa.gov/reporting-cyber-incidents).
- [ ] Assess any damage to utility systems and equipment, along with disruptions to utility operations.
- [ ] Execute the utility ERP as needed, including notification of utility personnel, actions to restore operations of mission critical processes (e.g., switch to manual operation if necessary), and public notification (if required).
- [ ] Report the cyber incident as required to law enforcement and regulatory agencies.
- [ ] Notify any external entities (e.g., vendors, other government offices) that may have remote connections to the affected network(s).
- [ ] Document key information on the incident, including any suspicious calls, emails, or messages before or during the incident, damage to utility systems, and steps taken in response to the incident (including dates and times).

IT Staff or Vendor

- [ ] Review system and network logs, and use virus and malware scans to identify affected equipment, systems, accounts and networks.
- [ ] Document which user accounts were or are logged on, which programs and processes were or are running, any remote connections to the affected IT systems or network(s) and all open ports and their associated applications.
- [ ] If possible, take a "forensic image" of the affected IT systems to preserve evidence. Tools to take forensic images include Forensic Tool Kit (FTK) and EnCase.
- [ ] If possible, identify any malware used in the incident, any remote servers to which data may have been sent during the incident, and the origin of the incident. DHS CISA can assist with the forensic analysis (www.cisa.gov/reporting-cyber-incidents).
- [ ] Research and identify if any employee or customer personally identifiable information (PII) was compromised.
- [ ] Check the system back-up time stamp to determine if the back-up was compromised during the incident.
- [ ] Document all findings, and avoid modifying or deleting any data that might be attributable to the incident.

Notes:

Actions to Recover from a Cyber Incident

Utility

- [ ] Continue to work with IT staff, vendors and integrators, government partners and others to obtain needed resources and assistance for recovery.
- [ ] Notify affected employees and customers if any PII was compromised.
- [ ] Submit an incident report through WaterISAC (866-H2O-ISAC). Membership is not required to submit a report.
- [ ] Develop a lessons learned document and/or an after action report (AAR) to document utility response activities, successes, and areas for improvement. Create an improvement plan (IP) based on your AAR and use the IP to update your vulnerability assessment, ERP and contingency plans.
- [ ] Register for cybersecurity alerts and advisories from water sector and government partners to be aware of new vulnerabilities and threats. Two sources of cybersecurity alerts are WaterISAC, which has a basic membership that is free, and ICS-CERT (https://ics-cert.us-cert.gov/alerts).

IT Staff or Vendor

- [ ] Remove any malware, corrupted files and other changes made to IT systems by the incident.
- [ ] Restore IT systems as required (e.g., re-image hard drives, reload software). DHS CISA can assist with the IT system recovery (https://www.cisa.gov/reporting-cyber-incidents).
- [ ] Restore compromised files from a system back-up that has not been compromised.
- [ ] Install patches and updates, disable unused services and perform other countermeasures to harden the system against known vulnerabilities that may have been exploited.

Notes:

My Contacts and Resources

CONTACT NAME	UTILITY/ORGANIZATION NAME	PHONE NUMBER
	Law Enforcement	
	IT Staff/Vendor	
	SCADA Staff/Vendor	
	DHS Cybersecurity and Infrastructure Security Agency (CISA)	
	Local Laboratory	
	State Primacy Agency	
	Local Emergency Management Agency	
	Local Health Department	
	WARN Chair	
	State Emergency Management Agency	

Resources

- Best Cybersecurity Practices (Water ISAC)
- Cyber Security Evaluation Tool (DHS ICS-CERT)
- Advisories (DHS ICS-CERT)
- Cybersecurity Advisors (DHS)
- DHS Cybersecurity and Infrastructure Agency (CISA)
- Cybersecurity Guidance and Tool (AWWA)

Notes: