**Public Water Supply Cybersecurity Incident Response Plan Template**

Drinking Water Program

**Purpose and Caution**

This cybersecurity incident response plan template is here to help create a basic cybersecurity incident response plan (**IRP**) or to help think of ways that may improve your current plan. ***Each organization is responsible for its actions during an incident and there is no assurance that the advice and steps presented in this template are appropriate for a given situation.***

**How to Use**

Freely edit this template to match your organization’s needs. Text in blue font is there to highlight content to add and change to black font or as possible suggestions on what to do. The template is organized into two broad sections, the first is for the actual response and the second is a set of appendices with preparation steps, maintenance steps, and references.

**Basic Plan First**

If this is your first version of a written cybersecurity incident response plan, start with the basics of who to contact and when. Then fill out the plan with more substance over time.

**Preparation Steps**

Incident response preparation steps include developing and maintaining this plan, and

* Cataloging assets of your enterprise information technology (**IT**) and operational technology (**OT**) systems (e.g. SCADA, DCS, single loop controller, etc.)
* Identifying internal and external resources to reach out to during an incident
* Keeping backups of software, firmware, and important data files
* Documenting and practicing manual control of your water and wastewater operations
* Holding tabletop exercises to practice and improve your cybersecurity IRP

**More About This Template** **and Acknowledgements**

This Cybersecurity Incident Response Plan Template was created for the Massachusetts Department of Environmental Protection (**MassDEP**) under their Small System Technical Assistance, Training and Outreach for Public Water Systems program by Andrew Hildick-Smith of OT Sec, LLC. The goal is to help water and wastewater utilities with operational resilience and specifically with cybersecurity incident response. While geared towards water and wastewater utilities, this template can be applied and modified for any type of organization. The content and structure of this plan comes from experience with general emergency planning in the water sector, subsequent work in the sector on OT cybersecurity, and talking to utilities that experienced an incident. The layout is loosely modelled after Information Mapping, but with easier editing in mind. The content is also influenced by various publications and classes, which are included in the Reference appendix, and can be used for further insight. Thanks goes to the late Russell J. Murray, Jr. for his early draft of a utility’s cybersecurity IRP. **This template is freely available for anyone’s use**. **Current version: 1.1**.

**(Organization Name) Cybersecurity Incident Response Plan**

of (date), approved by (name of manager/executive)

**Plan Purpose**

The purpose of the (organization) cybersecurity incident response plan (**IRP**) is to assist staff in responding to and recovering from an incident involving the enterprise information technology (**IT**) system and/or the operational technology (**OT**) system.

**Cybersecurity Incident Definition**

A cybersecurity incident is an adverse event or a threat of an adverse event that compromises the confidentiality, integrity, and/or availability of (organization’s) IT or OT systems.

**Contents**

**Incident Response** Page

Incident Response Summary Checklist 2

Incident Identification and Severity 3

Notifications and Contacts 5

Response Team 7

Response Steps 8

Recovery 9

**Appendix**

1. Preparation Steps 10
2. Status and Incident Action Plan 14
3. Draft Communications Language 15
4. Chain of Custody Form 16
5. Data Logging 17
6. Forensic Imaging 18
7. Incident After Action Report 19
8. Incident Command System Overview 20
9. Cybersecurity Incident Response Plan Template – Introduction 21
10. Acronyms and Common Cybersecurity Terms 22
11. Incident Response References 24
12. Incident Response Resources and Miscellaneous Resources 25

**Paper Copies of the Plan**

In case a cybersecurity incident makes our computer systems unusable, we keep paper copies of this plan in the following locations:

* X, Y and Z

Because of the sensitive nature of the information in this IRP, all electronic and paper copies are securely stored, and distribution of the plan is carefully restricted.

**Incident Response Summary Checklist**

**Summary Checklist**

This checklist provides a summary of basic response steps. A minor incident may only involve the first four. The order of, or number of steps may be different than this depending on the situation.

**Identification and Severity**

\_\_\_\_\_ Incident identified by internal staff or external source

\_\_\_\_\_ All participants should begin to take notes on their actions and observations

\_\_\_\_\_ Initial assessment

\_\_\_\_\_ Categorize severity of incident

\_\_\_\_\_ Report initial findings to internal staff and external resources as appropriate

**Incident Response**

\_\_\_\_\_ Assemble the incident response team

\_\_\_\_\_ Isolate known contaminated/breached computers by disconnecting from network

\_\_\_\_\_ Retrieve asset inventory and network diagrams

\_\_\_\_\_ Identify extent and nature of the breach

\_\_\_\_\_ Provide updates to appropriate parties as more is learned and at determined intervals

\_\_\_\_\_ Seek additional external assistance as needed for threat hunting

\_\_\_\_\_ Identify the source of the breach and the mechanism, to prevent a repeat incident

\_\_\_\_\_ Continue to provide updates as more is learned

**Recovery**

\_\_\_\_\_ Determine the priority order for rebuilding systems

\_\_\_\_\_ Check spares inventory

\_\_\_\_\_ Purchase required hardware and software

\_\_\_\_\_ Bring out backups and configuration documentation

\_\_\_\_\_ Rebuild systems from scratch or decontaminate as appropriate

\_\_\_\_\_ Harden, patch and/or remediate the identified vulnerability

\_\_\_\_\_ Reintroduce restored system components and services

\_\_\_\_\_ Regularly communicate restoration status and anticipated timeline to stakeholders

\_\_\_\_\_ Monitor system status during restoration for reinfection or return intrusions

\_\_\_\_\_ Notifying all contacted parties on closure and resolution of the incident

**Lessons Learned**

\_\_\_\_\_ At the end of the incident, pull everyone together for a lessons-learned session

\_\_\_\_\_ Document the incident, the lessons learned and collect copies of everyone notes

\_\_\_\_\_ Update the Cybersecurity Incident Response Plan.

**Incident Identification and Severity**

**Incident Awareness**

Awareness of a potential incident may come from a variety of sources including:

* Declaration by the threat actor
* Unusual system behavior recognized by end users of the IT system, operators of the OT system, and any internal cybersecurity protective software.
* Warnings can also come from outside organizations such as CISA, the local fusion center, other water utilities, vendors, the FBI, etc.

**Problem Indications**

Possible indications of an incident include:

* Active alerts from antivirus/anti-malware software, anomaly detection software, etc.
* Unusual client, server, or network log activity
* Log modifications or other abnormalities
* Slow network response
* System crashes
* Unusual network traffic
* Odd behavior by the OT system
* Ransomware note from a threat actor

**Initial Analysis**

Distinguishing non-threatening events from cybersecurity incidents can take time. Declaring whether there is a real cybersecurity incident, and its extent is difficult and may take several hours involving some of the following activities:

* Studying firewall logs, PC operating system logs (Event Viewer), OT/SCADA Human Machine Interface (**HMI**) logs, security software logs
* Reviewing physical security access logs and looking for signs of forced entry
* Identifying an indicator of compromise (**IOC**) and looking for it across all systems
* Physically visiting every facility to inspect computers and equipment condition
* Event correlation by comparing time stamps
* Reviewing router statistics
* Reviewing OT / SCADA parameter trends
* Revisiting network drawings for clues on access
* Checking for public reports and blogs on similar incidents
* Obtaining expert help from commercial cybersecurity services, the FBI, CISA, the local Fusion Center, etc.
* Asking operators, IT staff, OT staff, and administrative staff about unusual system behavior
* Trying to distinguish between malicious action and unintentional error

**Incident Identification and Severity, cont.**

**Incident Severity Level Classification**

Once a cybersecurity incident has been identified and the extent of the problem has been tentatively determined, we need to classify the incident severity level to help guide our response and who to notify. This is a relative quick step. As we learn more about the incident over time, we will want to reassess the severity level and our actions. (The following examples and possible response steps should be customized for your organization)

|  |  |  |
| --- | --- | --- |
| **Severity** | **Example Symptoms, Impact and Extent** | **Possible Response Steps** |
| **Low** | Cybersecurity software such as antivirus identifies a known virus on a single end user’s computer and can quarantine or remove it | * Notify senior IT person * Research likely cause and remediate across the board * Keep staff aware of phishing attempts |
| End user reports unsuccessful standard phishing attempts |
|  |
| **Medium** | Attempted but unsuccessful business email compromise or vendor email compromise | * Notify senior IT person and senior management * Share attempted incident information with financial staff, technical staff, etc. |
| Targeted but unsuccessful phishing attempt against higher value targets such as IT administrators or OT engineers or technicians |
|  |
| **High** | Ransomware | * Notify senior management * Assemble Incident Response Team * Notify the Mass. DEP if water service is disrupted or could be * Notify cybersecurity insurance firm * Reach out to incident response firm * Contact CISA or FBI if appropriate * Follow any breach notification rules such as require by the Health Insurance Portability and Accountability Act of 1996 * Notify media if appropriate * Consider manual operations of water and wastewater facilities |
| Business email compromise |
| Intrusion into the OT system with possible impact to water/wastewater service |
| Disruption to payroll or revenue collection |
| Criminal activity such as platform being used for child pornography, drug sales, etc. |
| Part of a regional or national incident |
| Intrusion by suspected advanced persistent threat (APT) / state actor |
| Compromise of the Domain Controller |
| FBI or other agency reports we have a breach |
| Outside organization reports that our email system has been compromised and is being used for phishing |
| Stolen personally identifiable information (PII) |
|  |

**Notifications and Contacts**

**Internal Contacts**

This is a maintained list of internal contacts:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Cell Number** | **Alternate Contact Information** | **Notes** |
| (Board of Directors) |  |  |  |
| (CEO / Utility Director) |  |  |  |
| (Operations Manager) |  |  |  |
| (IT Manager) |  |  |  |
| (IT technical staff) |  |  |  |
| (OT Manager) |  |  |  |
| (OT technical staff) |  |  |  |
| (Public relations) |  |  |  |
| (Legal staff) |  |  |  |
| (Local representatives) |  |  |  |

Internal contacts last checked and updated on:  **(date)**

**Mass DEP Regional Office Contacts**

**Note**: Massachusetts PWSs are required to notify MassDEP and their local Board of Health as soon as possible, but not more than 2 hours after obtaining knowledge of a potential or actual Emergency in accordance with 310 CMR 22.15(9)(b)1. See MassDEP “Appendix O- Handbook for Water Supply Emergencies”. Web link to document listed in Appendix K below.

Check for updated DEP Regional Office contacts at: <https://www.mass.gov/service-details/drinking-water-program-public-notification-emergency-contacts>

|  |  |  |
| --- | --- | --- |
| **Region** | **Person** | **Contact Information** |
| Northeast | Tatyana Karpenko | [Tatyana.Karpenko@mass.gov](mailto:Tatyana.Karpenko@mass.gov), 978-694-3233 |
|  | Melissa Privetera | [Melissa.Privetera@mass.gov](mailto:Melissa.Privetera@mass.gov), 978-694-3403 |
|  | Kristin Divris | [Kristin.Divris@mass.gov](mailto:Kristin.Divris@mass.gov), (978)-694-3260 (Drinking Water Program Chief) |
| Central | Paula Caron | [Paula.Caron@mass.gov](mailto:Paula.Caron@mass.gov) 508-767-2719 |
|  | Andrea Lemerise | [Andrea.Lemerise@mass.gov](mailto:Andrea.Lemerise@mass.gov), 508-767-2723 |
|  | Bob Bostwick | [Robert.Bostwick@mass.gov](mailto:Robert.Bostwick@mass.gov), 508-849-4036 (Drinking Water Program Chief) |
| Southeast | Karen Dube | [Karen.Dube@mass.gov](mailto:Karen.Dube@mass.gov), 508-946-2720 |
|  | Scott Sayers | [Scott.Sayers@mass.gov](mailto:Scott.Sayers@mass.gov), 508-946-2780 |
|  | Jim McLaughlin | [james.m.mclaughlin@mass.gov](mailto:james.m.mclaughlin@mass.gov), 508-946-2805 (Drinking Water Program Chief) |
| West | Douglas Paine | Douglas.Paine@mass.gov, 413-755-2281 |
|  | Deirdre Doherty | Deirdre.Doherty@mass.gov, 413-755-2148 (Drinking Water Program Chief) |

Mass DEP Regional Office Contacts last checked and updated on:  **7/20/2022**

**Notifications and Contacts, continued**

**External Contacts**

This is a maintained list of external contacts.

|  |  |  |  |
| --- | --- | --- | --- |
| **Organization** | **Individual’s Name** | **Phone Number** | **Alternate Contact Information / Notes** |
| Commonwealth Fusion Center |  | 978-451-3700 | General phone number |
| CISA, Region 1 | Daniel King  Ryan Barnes  Richard “Rick” Rossi  Roland “Mike” Tetreault  Cheri Ayoub |  | CT & MA, [daniel.king@cisa.dhs.gov](mailto:daniel.king@cisa.dhs.gov)  ME, [ryan.barnes@cisa.dhs.gov](mailto:ryan.barnes@cisa.dhs.gov)  NH, [richard.Rossi@cisa.dhs.gov](mailto:richard.Rossi@cisa.dhs.gov)  RI, [roland.tetreault@cisa.dhs.gov](mailto:roland.tetreault@cisa.dhs.gov)  VT, [cheri.ayoub@cisa.dhs.gov](mailto:cheri.ayoub@cisa.dhs.gov) |
| CISA, national |  | 888-282-0870 | <https://us-cert.cisa.gov/report> and [report@cisa.gov](mailto:report@cisa.gov), asset response |
| (Cybersecurity Consultant |  |  |  |
| FBI Boston |  | 857-386-2000 |  |
| FBI, national |  | 855-292-3937 | CyWatch, [cywater@fbi.gov](mailto:cywater@fbi.gov), threat response |
| (Insurance Company) |  |  | Contact very early in incident |
| (Incident Response Firm on retainer) |  |  |  |
| (Legal firm) |  |  |  |
| (Local Board of Health) |  |  |  |
| (Local Police Department) |  |  | As needed or if required by insurance policy |
| MassDEP, 24 hr. |  | 888-304-1133 | If there is or could be a water system impact |
| MassDEP Regional Office |  |  | If there is or could be a water system impact *(See prior contact category for contact info)* |
| MS-ISAC (multi state) |  | 866-787-4722 | [soc@msisac.org](mailto:soc@msisac.org) / Remote assessment assistance may be available if a member |
| (Vendor) |  |  |  |
| WaterISAC |  | 866-426-4722 | [analyst@waterisac.org](mailto:analyst@waterisac.org) / For incident sharing |

External contacts last checked and updated on:  **(date)**

**Response Team**

**Incident Response Team**

There are a wide variety of roles that can be assigned to respond and recover from a cybersecurity incident. The following is a list of possible roles with individuals assigned to them. Vacations and leaves of absence require identifying alternates. Response resources can be stretched if the incident has public safety implications and around-the-clock staffing is needed for multiple days. Depending on the size of the organization, single individuals may be assigned multiple roles.

|  |  |  |
| --- | --- | --- |
| **Role Title** | **Primary / Alternate and Phone Numbers** | **Role Description** |
| Team Lead |  | Directs the incident response team; sets objectives; ensures regular reports are provided as appropriate to internal and extern constituents; helps identify and deliver needed resources; makes sure response staff get relief when needed |
| Technical Lead |  | Oversees the technical aspect of the response |
| Technical Support |  | Provides hands on capabilities and reports on status |
| Operations Lead |  | Water or wastewater operations manager, who can assess the criticality of IT and OT system impacts on providing service. Will potentially direct a switch to manual operations and notify the regulatory authorities such as the state primacy agency of serious or potential serious impacts. |
| Legal Support |  | Ensures that laws and regulations are followed |
| Public Relations Support |  | Provides the one external voice to media if required, helps communicate to internal staff |
| Assistant |  | Note taker for the Team Lead, handy everything person |

**Response Steps**

**Response Goal**

The overarching goal of the whole incident response is to:

Maintain (water/wastewater) service at the highest level possible and to safely restore IT and OT systems in a way that prevents a recurrence of a similar incident.

**Possible Response Steps**

All individuals participating in the response should take notes on what they see and do. Taking photographs can be a big help in documenting screens, etc.

* Assemble the incident response team, consider using out-of-band communications
* Isolate known contaminated/breached computers by disconnecting from network
  + - * Isolate infected and breached computers by disconnecting network cables and disabling Wi-Fi connections, or possibly by disconnecting switches
      * Isolate infected and breached networks or subnetworks by disconnecting routers
      * In all cases, try to keep the equipment powered on to preserve forensic evidence that would be lost if the equipment is turned off or unplugged
* Retrieve asset inventory and network diagrams
* Identify extent and nature of the breach
* Provide updates to appropriate parties as more is learned and at determined intervals
* Seek additional external assistance as needed for threat hunting or other skills
* Identify the source of the breach and the mechanism, to prevent a repeat incident
* Continue to provide updates as more is learned

**Specific Responses Based on Incident Type**

Some responses are specific to the incident type.

* Ransomware – Have a high-level discussion on whether to pay a ransom
* BEC / VEC – Contact your bank and the FBI. The FBI has a good record of recovering money if the illicit electronic fund transfer happened within 72 hours
* Insider Threat – Work with HR and legal
* Advanced Persistent Threat / State Actor - Contact CISA or the FBI for assistance

**Water / Wastewater Manual Operations**

If the OT system has failed or needs to be disconnected to restore it, manual operations of the water / wastewater system may be necessary. Be sure to contact the regulatory agency.

**Recovery**

**Possible Recovery Steps**

System recovery is difficult and time consuming. Here are some basic steps.

* Determine the priority order for rebuilding systems
* Check spares inventory
* Purchase required hardware and software
* Bring out backups and configuration documentation
* Rebuild systems from scratch or decontaminate as appropriate
* Harden, patch and/or remediate the identified vulnerability
* Reintroduce restored system components and services sequentially
* Regularly communicate restoration status and anticipated timeline to stakeholders
* Monitor system status during restoration for reinfection or return intrusions
* Notifying all contacted parties on closure and resolution of the incident

**Appendix A – Preparation Steps**

**Preparation Steps**

This is the most time-consuming part of a cybersecurity incident response plan. The more time you spend on the following topics the better off your response and recovery will be. On the right-hand side, opposite some of the topics is a very rough estimate of how much time they might take. You may choose to refine these values to help with budgeting time, or to just delete them. Some topics have an optional entry for when you last completed the activity.

**Maintaining the IRP** ( ~ 5 – 15 hrs./yr. )

Once you have developed a basic incident response plan, maintaining it requires at least an annual:

* Review and update of contact information and incident response team members
* Updating other parts of the plan to reflect IT and OT system changes.
* Look to improve the plan over time

**External Resources** ( ~ 5 – 100 hrs. / yr. )

External resources can be essential for incident response.

* Keep in touch with CISA, FBI and other agencies’ points of contact
* Procure or maintain cybersecurity insurance contract if appropriate
* Procure or maintain an incident response retainer contract if appropriate
* Talk to other utilities to see if response resources could be pooled or shared

**IT and OT Backups**

The importance of backups does not need to be stated. Make sure you are backing up and documenting what you will need to restore your system if everything is compromised. This can include:

* Data
* Software
* Firmware
* Device configuration
* Critical OT set points

Keep backup media off site and off the network. You may choose to encrypt it.

**Appendix A – Preparation Steps, continued**

**Restoration Priorities**  ( ~ 1 - 6 hrs. )

Identify your system restoration priorities. Think through the internal and external IT and OT services you could lose and rank them in order of restoration priority. Some steps may be dependent on others.

1. Critical parts of the OT system
2. Payroll functionality
3. Revenue collection
4. …

**Reloading Operating Systems Preparations**  ( ~ 1 – 3 hrs. per USB )

There is a good chance that you will want to wipe and reimage computers and servers that have been infected or compromised, before putting them back in service. Here are two possible options for reinstalling Windows 10 on wiped drives that you can do ahead of time:

* Using new USB thumb drives and a clean computer, follow Microsoft’s directions to “**create a recovery drive**” which should include the system’s drivers. This approach should only be used for reimaging the same make and model of computer.
* Using new USB thumb drives, go online to “**create Windows 10 installation media**” per Microsoft’s directions. Consider creating a number of these drives in proportion to the number of systems you might need to restore. So, if you have 100 computers, you might want to create 10 Installation media drives so multiple people can be working on this part of restoration simultaneously. After reinstalling the operating system, you will need to download device drivers from your computer manufacturer.

Windows 10 restoration media created on:  **(date)**

With both approaches you may need to access the computer’s UEFI (bios) to allow the system to boot from the USB thumb drive. Note that some malware can persist in a drive’s firmware or a computer’s UEFI firmware and reinfect the contents of a hard disk drive (HDD) or solid-state drive (SSD) that has been wiped and reloaded. This is considered very uncommon because of the difficulty to achieve it. However, if this is a concern, new drives or new computers should be considered.

(Add pre-incident preparation requirements for restoring other operating systems or devices)

**IT and OT Restoration Practice**

Even the relatively simple sounding step of wiping a hard drive and reinstalling the operating system can cause headaches. Find time to incrementally practice and document your various hardware, software, firmware and data restoration steps. (Add an Appendix with the technical step-by-step instructions for critical computer and device restoration)

**Appendix A – Preparation Steps, continued**

**Spare Parts**

What IT and OT devices are critical? If they get “bricked”, do you have enough spares to get systems up and running? Even something as simple as a PC may take a while to procure with supply chain issues. Consider keeping on hand spare parts that might need including PCs, laptops, tablets, servers, hard disk drives, solid state drives, programable logic controllers (PLCs), routers, managed switches, etc. For some equipment, firmware versions matter for compatibility.

|  |  |  |
| --- | --- | --- |
| **Count** | **Spare Parts** | **Storage Location** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

If you pull a spare part for a new project or normal failure replacement, be sure to restock.

Inventory as of:  **(date)**

**Manual System Control**

One of the best defenses against a successful cybersecurity attack against a utility’s OT control system, is being able to seamlessly shift from automated control to manual control. If full manual control is not possible, there may be ways to manually operator important parts of a distribution, collection, or treatment system. Identify system operations that require a functioning Human Machine Interface and/or PLC. Perhaps the system can be redesigned to isolate and protect the PLC from attack? Perhaps there is a way to temporarily and safely remove interlocks? If a water system can manually provide flow and pressure but not full treatment, at least firefighting is possible, and treatment could perhaps be covered by a boil order? Practicing manual control is a valuable exercise but must be done carefully to prevent creating problems. Be sure to coordinating with your regulatory agency before doing so. (Add an Appendix or reference a separate document that details how to operate the water or wastewater system manually.)

**Training and Exercise Record**

Annual training of staff on this incident response plan is important to its success. Keep a record of training activities and who participated.

|  |  |  |
| --- | --- | --- |
| **Training / Exercises Description** | **Date(s)** | **Participating Staff** |
| (Tabletop Exercise for ransomware) |  |  |
| (Incident Response Class) |  |  |
| (Forensics Class) |  |  |
| (Tabletop Exercise on an OT system failure) |  |  |
|  |  |  |
|  |  |  |

**Appendix A – Preparation Steps, continued**

**Jump Bag**

A jump bag is for equipment and tools that could be handy for an incident response. An organization may have one or more jump bags that might contain things like:

* **Hardware** – multiple new USB thumb drives, hard disk drives or solid-state drives with USB or SATA interfaces, network tap, clean laptop, tool set with Philips head and Torx screw drivers, patch cable, cross-over cable, router cables, OT device cables, and flashlight.
* **Software** – pre-burned CD or DVD with binaries of critical operating system executables such as , or on USB Thumb drive with write protect switch, SysInternals, image copying software, forensics software
* **Supplies** – blank notebooks, pens, permanent markers, this IRP, extra copies of chain-of-custody form, extra copies of Incident Action Plan, aspirin/Tylenol, anti-static evidence bags, desiccants,

(If you create a jump bag, use the above space to list the intended contents and its location)

Jump bag created or last inventoried on:  **(date)**

**Independent Monitoring and Alarming**

If the OT system is compromised or it fails for any reason, manual operation of the water or wastewater system can be greatly aided by pre-installing an independent logging system that tracks critical values such as tank levels, system pressure, chemical feed rates, water quality parameters. This may not be too expensive to do.

A secondary benefit is that critical parameter alarms from the OT system and the independent monitoring system can be compared. If a high or low alarm comes in on the independent system but not the OT system, then there may be an instrument problem, a communications or cybersecurity incident with the attackers masking an OT value.

**Ransomware Discussion**

Staff and managers should discuss ahead of time how they plan to respond to ransomware. Are there any conditions that a ransom might be paid? If so, document how to quickly procure various types of digital currency such as Bitcoin or Ethereum, and consider identifying service providers that specialize in negotiating cybersecurity ransoms.

**Appendix B – Status and Incident Action Plan**

**Status and Incident Action Plan Report**

This is very loosely based on FEMA’s incident action plan and should be used to document incident status for briefing purposes and to organize the response. Try to establish a fixed update frequency.

**Team Lead**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Date**: \_\_\_\_\_\_\_\_\_\_\_\_ **Time**: \_\_\_\_\_\_\_\_\_\_

**Water/wastewater system impacts or potential impacts**:

**Status of IT and OT Systems**:

**Active Incident Response Team Members**:

**Incident Objectives** (specific, measurable, action-oriented, realistic, time-sensitive):

**Actions, Strategies and Tactics**:

**Work Assignments**:

**Appendix C – Draft Communications Language**

**Draft Communications Language**

Basic draft messages for the press or staff can be prepared for a variety of cybersecurity incidents to help in the crunch of an incident. Even outlines can be an aid.

**…**

**Appendix D – Chain of Custody Form**

**Chain of Custody Form**

Digital evidence from a cybersecurity incident may be use for technical investigations to understand what happened to prevent a repeat of the same breach. It may also be used in legal proceedings. A very high standard of data handling and copying is required for legal evidence, which is beyond the scope of this document. This basic version of a chain of custody form is to help keep track of who has handled the evidence.

**Description of Digital Evidence Source** *(e.g. disk image from server X, files from PLC Y, memory image from PC w/ID # locate in, etc.)*

**Description of Digital Evidence Media** *(e.g. original hard drive, original solid state drive, copy made to a new USB drive using a particular technique and tools, etc.)*

**Evidence Stored In** *(e.g. tape sealed plastic bag with air holes, in a box, loose, etc.)*

**Handed Over By**

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Organization: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Received By**

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Organization: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Appendix E – Logs and Traffic Capture**

**Event Logs**

Keeping logs helps with incident response and recovery. Experienced cybersecurity forensics analysts can use logs to understand what happened and to identify what to harden to prevent it from happening again. Staff, vendors and/or consultants can identify what devices and systems are currently storing logs and for what duration. They may include firewalls, routers, switches, HMI software, PCs, servers, etc. (A basic list of active logging devices could be recorded here or in a new Appendix)

**Windows Logs**

Windows PCs and servers are a great source of security and event logs. The UK’s National Cyber Security Centre (NCSC) has a projected called “Logging Made Easy” with advice for low-resourced organizations. Actual configuration advice is available from Microsoft

Longer term, consolidating your logs into a security information and event management (SIEM) solution will help experienced incident responders investigate what happened and may help keep an adversary from modifying logs.

**Traffic Capture**

If there is not an existing cybersecurity system gathering network traffic, traffic at critical points in the OT system or between the OT and IT systems can be collected inexpensively using network taps and less expensive computers.

**Appendix F – Forensic Imaging**

**Forensic Imaging**

Forensic analysis is outside the scope of this document, but memory forensic imaging can be very valuable to an analyst. The current volatile memory of important computers and representative computers can be captured for future comparison against the same compromised computer or standard configuration computer. This section introduces a couple of approaches for capturing a volatile memory image.

**…**

**Appendix G – Incident After Action Report**

**Incident After Action Report**

An Incident After Action Report captures the details of an incident and presents the lessons learned that can be incorporated into future training and into the updated Cybersecurity Incident Response Plan. Here are some elements to consider including:

**…**

**Appendix H – Incident Command System Overview**

**Incident Command System (ICS)**

The Incident Command System (ICS) is promoted by the Federal Emergency Management Agency (FEMA) and is used as a framework by utilities in responding to emergencies. There are advantages to using ICS for cybersecurity incidents if the utility’s staff is already familiar with it. If it is a new concept to staff, it is one more thing to learn and the focus should probably be on cybersecurity. Here are some basic terms and concepts that might be useful as a reference. The Incident Action Plan is worth paying attention to.

**ICS Terms**

**…**

**ICS Concepts**

**…**

**Incident Action Plan**

**…**

 **Appendix I – Public Water Supply Cybersecurity Incident Response Plan Template**

Drinking Water Program

**Purpose and Caution**

This cybersecurity incident response plan template is here to help create a basic cybersecurity incident response plan (**IRP**) or to help think of ways that may improve your current plan. ***Each organization is responsible for its actions during an incident and there is no assurance that the advice and steps presented in this template are appropriate for a given situation.***

**How to Use**

Freely edit this template to match your organization’s needs. Text in blue font is there to highlight content to add and change to black font or as possible suggestions on what to do. The template is organized into two broad sections, the first is for the actual response and the second is a set of appendices with preparation steps, maintenance steps, and references.

**Basic Plan First**

If this is your first version of a written cybersecurity incident response plan, start with the basics of who to contact and when. Then fill out the plan with more substance over time.

**Preparation Steps**

Incident response preparation steps include developing and maintaining this plan, and

* Cataloging assets of your enterprise information technology (**IT**) and operational technology (**OT**) systems (e.g. SCADA, DCS, single loop controller, etc.)
* Identifying internal and external resources to reach out to during an incident
* Keeping backups of software, firmware, and important data files
* Documenting and practicing manual control of your water and wastewater operations
* Holding tabletop exercises to practice and improve your cybersecurity IRP

**More About This Template** **and Acknowledgements**

This Cybersecurity Incident Response Plan Template was created for the Massachusetts Department of Environmental Protection (**MassDEP**) under their Small System Technical Assistance, Training and Outreach for Public Water Systems program by Andrew Hildick-Smith of OT Sec, LLC. The goal is to help water and wastewater utilities with operational resilience and specifically with cybersecurity incident response. While geared towards water and wastewater utilities, this template can be applied and modified for any type of organization. The content and structure of this plan comes from experience with general emergency planning in the water sector, subsequent work in the sector on OT cybersecurity, and talking to utilities that experienced an incident. The layout is loosely modelled after Information Mapping, but with easier editing in mind. The content is also influenced by various publications and classes, which are included in the Reference appendix, and can be used for further insight. Thanks goes to the late Russell J. Murray, Jr. for his early draft of a utility’s cybersecurity IRP. **This template is freely available for anyone’s use**. **Current version: 1.1**.

**Appendix J – Acronyms and Common Computer Terms**

**Acronyms**

Some abbreviations and acronyms used in the cybersecurity world.

|  |  |  |
| --- | --- | --- |
| **Acronym** | **Stands For** | **Description** |
| AWIA | America’s Water Infrastructure Act of 2018 | Safe Drinking Water Act update w/ risk assessment section |
| BEC | Business Email Compromise | Using emails to trick a utility into misdirecting electronic funds |
| C2 | Command and Control | Server(s) used by an adversary to interact w/ victim’s system |
| CI | Critical Infrastructure | Water is one of 16 CI sectors recognized in the US |
| CIA | Confidentiality, Integrity, and Availability | A goal of IT cybersecurity is to maintain data CIA |
| CIE | Cyber-Informed Engineering | Engineering design with cybersecurity in mind |
| CISA | Cybersecurity and Infrastructure Security Agency | Part of the Department of Homeland Security |
| CPSS | Cyber-Physical Safety System | Protects infrastructure from damage caused by a cyber attack |
| DCS | Distributed Control System | A control system type, usually within a single plant or campus |
| DMZ | Demilitarized Zone | Area separating 2 networks that have different levels of trust |
| EDR | Endpoint Detection and Response | Security software that detects and responses to host attacks |
| ERP | Emergency Response Plan | Part of the AWIA requirement for water utilities |
| FOIA | Freedom of Information Act | Law providing for disclosure of non-protected federal records |
| HMI | Human Machine Interface | Operator provided display that represents the water process |
| ICS | Industrial Control System | Automated process control system such as SCADA and DCS |
| INL | Idaho National Laboratory | National energy laboratory that works on cybersecurity |
| IOC | Indicators of Compromise | Digital trail of evidence left by cyber adversaries |
| IRP | Incident Response Plan | Written guide to help staff respond to a cybersecurity incident |
| ISAC | Information Sharing and Intelligence Center | Helps CI sectors with security threat info and resilience |
| ISRP | Incident-Specific Response Plan | A more focused AWIA response plan, as compared to the ERP |
| IT | Information Technology | Hardware and software that runs your business network |
| LAN | Local Area Network | Covers a fairly small area, often w/ in-house communications |
| MFA | Multifactor Authentication | Using more than just a password to logon to an account |
| ML | Machine Learning | Type of artificial intelligence using data to improve over time |
| MSSP | Managed Security Services Provider | A firm that monitors the security of your IT or OT system |
| NIST | National Institute of Standards and Technology | Federal organization w/ many good cybersecurity standards |
| OPSEC | Operations Security | Being careful about what you reveal about your system |
| OSINT | Open-Source Intelligence | Information about your utility and staff that is on the Internet |
| OT | Operational Technology | Hardware and software that runs your process operations |
| PCS | Process Control Systems | Hardware and software to facilitate process automation |
| PII | Personally Identifiable Information | Private information about people that is protected by laws |
| PLC | Programmable Logic Controller | Industrial computer used to automate your water process |
| RRA | Risk and Resilience Assessment | Part of the AWIA requirement for water utilities |
| SCADA | Supervisory Control and Data Acquisition | Process monitoring and control system with remote sites |
| SIS | Safety Instrumented System | Rigorous safety system typically used in hazardous industries |
| SLA | Service Level Agreement | Contractually agreement specifying service quality, etc. |
| SME | Subject Matter Experts | Individuals with expertise in specific fields |
| SSO | Single Sign On | Logging on once, will give you access to multiple services |
| TTP | Tools, Tactics and Procedures | Methods used by cyber adversaries |
| TTX | Tabletop Exercise | Practicing incident response by talking through scenarios |
| VLAN | Virtual Local Area Network | A way to provide software defined network segmentation |
| WAN | Wide Area Network | Over long distances, frequently w/ 3rd party communications |

**Appendix J – Acronyms and Common Cybersecurity Terms, continued**

**Common Cybersecurity Terms**

Here are some common terms used in cybersecurity.

|  |  |
| --- | --- |
| **Term** | **Description** |
| Access Control | The various ways of limiting user access to a system, including passwords |
| Administrative Rights | The highest level of access rights on a computer. It gives the owner complete control. |
| Business Continuity | Sustaining the business or mission of the organization during a severe disruption |
| Controls, Security | Security controls are measures put in place to reduce cyber risk |
| Data Diode | Security device that only allows data communications in one direction |
| Disaster Recovery | In the IT world, this typically means activating infrastructure at a backup location |
| End Point | User device connected to a network, such as a computer or a cell phone |
| Firewall | Security device that helps you limit data communications to only what is required |
| Governance | Organizational oversight and control of something, in this case a cybersecurity program |
| Hardening | Configuring a computer or other device to make is less vulnerable to attack |
| Hash | Computer’s representation of a password, that cannot be converted back to the password |
| Hovering | Moving your mouse cursor over an Internet link to see the actual destination |
| Jump Server | Computer that is hardened and used as the access point to a more secure network zone |
| Least Privilege | Giving a user only enough access that is required to do their job |
| Macro | Computer code that can be run within Microsoft Office programs and be made malicious |
| Password Spraying | When an adversary tries to apply a few common passwords to multiple user accounts |
| Phishing | Social engineering technique to get a user to open a malicious file or link |
| Policies | Documents describing high level intent |
| Procedures | Documents detailing how to achieve policy goals |
| Risk | Likelihood of a bad outcome. Sometimes seen as Risk = Threat x Vulnerability x Consequence |
| Risk Management | Identifying risks and determining what to do about them: mitigate, accept, transfer, etc. |
| Router | A network component that directs traffic between local networks and across the internet |
| Sandbox | Temporary virtual system isolated in your computer’s memory to safely run malicious code |
| Segmentation | Providing some level of separation between different parts of a network |
| Supply Chain | The external resources that go into supporting your system and operations |
| Switch | A network component that direct traffic in a local network |
| Tabletop Exercise | A way of practicing incident response by talking through emergency scenarios |
| Test Bed | Computer network that you used to test new hardware, software, or software patches |
| Threat | The actor or event that could adversely impact something |
| Virus | Malicious code that requires a used to take an action before it executes |
| Vulnerability | A weakness that can be taken advantage of |
| Worm | Malicious code that can propagate on its own |

**Appendix K – Incident Response References**

APPA, Public Power Cyber Incident Response Playbook, <https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf>, August 2019

Carnegie Mellon Information Security Office, Computer Security Incident Response Plan, <https://www.cmu.edu/iso/governance/procedures/docs/incidentresponseplan.pdf>, May 2016

Center for Internet Security, Cyber Incident Response Information Technology Standard, <https://www.cisecurity.org/wp-content/uploads/2020/06/Cyber-Incident-Response-Standard.docx>, June 2020

Center for Internet Security / MS-ISAC / NIST, Policy Template Guide, <https://www.cisecurity.org/wp-content/uploads/2021/11/NIST-Cybersecurity-Framework-Policy-Template-Guide-v21.11.Online.pdf>, November 2021

CISA, Cybersecurity Incident & Vulnerability Response Playbooks, <https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf>, November 2021

EPA, Incident Action Checklist – Cybersecurity, <https://www.epa.gov/sites/default/files/2017-11/documents/171013-incidentactionchecklist-cybersecurity_form_508c.pdf>, February 2021

Federal Trade Commission, Data Breach Response, A Guide for Business, <https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business>, May 2019

FEMA, Incident Action Plan Guide, <https://www.fema.gov/sites/default/files/2020-07/Incident_Action_Planning_Guide_Revision1_august2015.pdf>, August 2015

Healthcare and Public Health Sector Coordinating Councils, Health Industry Cybersecurity Operational Continuity – Cyber Incident, <https://healthsectorcouncil.org/occi/>, May 2022

Massachusetts Department of Environmental Protection, Cybersecurity Incident Response Plan Template v.1.0, Word document, July 2022

Natural Resources Canada, IACS Cyber Security Incident Response Playbook, <https://s3.ca-central-1.amazonaws.com/medias.bba.ca/documents/pdf/BBA_Cybersecurity_final7.pdf>, March 2022

NIST, SP800-61 rev.2, Computer Security Incident Handling Guide, <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>, August 2012.

SANS, SEC504: Hacker Tools, Techniques, and Incident Handling class, <https://www.sans.org/cyber-security-courses/hacker-techniques-incident-handling/>, 2022

**Appendix L – Incident Response Resources and Miscellaneous Resources**

Incident Response Services

* MS-ISAC: free incident response services possible including log analysis, malware analysis, computer forensics, development of a mitigation and recovery strategy as well as network and application vulnerability scanning. Requests for these services can be requested by calling 1-866-787-4722 or sending an email to [soc@msisac.org](mailto:soc@msisac.org).
* CISA: assistance depending on the incident and availability of resources (focused on the asset)
* FBI: assistance depending on the incident and availability of resources (focused on the threat)

Incident Response Tabletop Exercises

* “Backdoors & Breaches, Incident Response Card Game”, ~ $20, <https://www.blackhillsinfosec.com/projects/backdoorsandbreaches/>
* CISA Water scenario and template: <https://www.cisa.gov/sites/default/files/publications/Water%20Wastewater%20Cyber%20CTEP%20%28JUNE%202021%29%20Situation%20Manual_FINAL_508.docx>, June 2021.
* CISA custom exercise engagement: [cisa.exercises@cisa.dhs.gov](mailto:cisa.exercises@cisa.dhs.gov) (6+ months lead time)
* FEMA holds tabletop cybersecurity exercises. You can request to be an observer by contacting their Emergency Management Institute

MassDEP Resources

* MassDEP Appendix O- Handbook for Water Supply Emergencies, <https://www.mass.gov/doc/guidelines-for-public-water-systems-appendix-o-handbook-for-water-supply-emergencies-0/download>
* MassDEP posters with cybersecurity tips to help keep your systems secure, <https://www.mass.gov/info-details/public-drinking-water-system-operations#cybersecurity->

Mitigation Guidance

* **Australian Cyber Security Centre** – Essential Eight controls
* **AWWA** – Water Sector Cybersecurity Risk Management Guidance & Cybersecurity Tool
* **Center for Internet Security** – Top 20 Controls
* **CISA, FBI, EPA, NSA** - Joint Cybersecurity Advisory “Ongoing Cyber Threats to U.S. Water and Wastewater Systems”, <https://www.cisa.gov/uscert/ncas/alerts/aa21-287a>
* **NIST** – Cybersecurity Framework v.1.1
* **NIST** – SP 800-82 Rev.3, Guide to Operational Technology (OT) Security (2022 Draft)
* **WaterISAC** – 15 Cybersecurity Fundamentals for Water and Wastewater Utilities

**Appendix M – Incident Response Resources and Miscellaneous Resources, continued**

Organizations to Consider Joining

* **E-ISAC** – Electricity Information Sharing and Analysis Center open to cross-sector water members
* **InfraGard** – Loose affiliation with FBI, multi-sector critical infrastructure (background check required)
* **MS-ISAC** – Multi-State Information Sharing and Analysis Center
* **MAWARN** – Massachusetts Water/Wastewater Agency Response Network
* **WaterISAC** – Water Information Sharing and Analysis Center, monthly security related webinars, twice a week curated threat and vulnerability emails (annual fee, $100 - $7,700 depending on utility size), <https://www.waterisac.org/membership>)

Security Assessments (free)

* **AWWA Cybersecurity Guidance and Tool** – American Water Works Association self-assessment aid
* **CISA Cyber Hygiene Services** – recurring external vulnerability scans, <https://www.cisa.gov/cyber-hygiene-services>
* **CISA Phishing Campaign Assessment** – three months of live phishing tests
* **CISA CSET** (Cyber Security Evaluation Tool) – detailed ICS oriented self-assessment aid
* **EPA Cybersecurity Assessment and Technical Assistance** – by Horsley Witten**,** <https://www.cisa.gov/cyber-hygiene-services>

Security Training Resources

* **DHS CISA Virtual Learning Platform** – Idaho National Lab SCADA/ICS classes
* **S4 Highway videos** – SCADA/ICS lectures by knowledgeable people
* **NICE** – FedVTE, CISA, National Initiative for Cybersecurity Education, all categories; for federal, state, local gov employees
* **InfoSec Institute** - relatively low cost option (~ $300 / yr.)
* **SANS** – 5-day classes with hands-on labs (~ $3k w/ MS-ISAC discount)

Threat Intelligence and Vulnerability Announcements

* **CISA Advisories and Alerts** – subscribe
* **Dale Peterson’s Friday News and Notes** – insightful information and opinions on ICS security
* **HSIN** (Homeland Security Information Network) – for sensitive but unclassified information, submit a request to joint to the Critical Infrastructure COI (community of interest)
* **SANS NewsBites** – twice a week email newsletter with editorial comments
* **SCADASEC list** – email list with commentary on current ICS events and topics
* **WaterISAC Security and Resilience Update** – twice a week summary on cybersecurity and all hazards, as well as training opportunities