**Cyber351: Incident Response Planning Forum**

**October 10, 2024**

**Template**

This template is provided to facilitate your documentation of information, processes, questions and notes as you develop your Incident Response Plan

We have compiled a list of additional resources for you. The list and excerpts from some of these resources are provided for your convenience starting on page 18.

Table

Description automatically generated

(See Additional Resources, NYSAC Primer)

**PREPARATION**

Determine the stakeholders who will be part of the Cyber Incident Response Team (CIRT)

City/Town/School Leader:

|  |  |
| --- | --- |
| **Name:** | **Email:** |
| **Work Phone** | **Mobile Phone** |
| **Alternate Email:** | **Alternate Phone:** |

Incident Response Coordinator, CIO or Chief Privacy Officer:

|  |  |
| --- | --- |
| **Name:** | **Email:** |
| **Work Phone** | **Mobile Phone** |
| **Alternate Email:** | **Alternate Phone:** |

Information Technology Coordinator or Chief Information Security Officer:

|  |  |
| --- | --- |
| **Name:** | **Email:** |
| **Work Phone** | **Mobile Phone** |
| **Alternate Email:** | **Alternate Phone:** |

MSP Technology Staff:

|  |  |
| --- | --- |
| **Name:** | **Email:** |
| **Work Phone** | **Mobile Phone** |
| **Alternate Email:** | **Alternate Phone:** |
| **Name:** | **Email:** |
| **Work Phone** | **Mobile Phone** |
| **Alternate Email:** | **Alternate Phone:** |

Communications Coordinator:

|  |  |
| --- | --- |
| **Name:** | **Email:** |
| **Work Phone** | **Mobile Phone** |
| **Alternate Email:** | **Alternate Phone:** |

Organization Legal Counsel:

|  |  |
| --- | --- |
| **Name:** | **Email:** |
| **Work Phone** | **Mobile Phone** |
| **Alternate Email:** | **Alternate Phone:** |

Chief Financial Officer:

|  |  |
| --- | --- |
| **Name:** | **Email:** |
| **Work Phone** | **Mobile Phone** |
| **Alternate Email:** | **Alternate Phone:** |

Human Resources:

|  |  |
| --- | --- |
| **Name:** | **Email:** |
| **Work Phone** | **Mobile Phone** |
| **Alternate Email:** | **Alternate Phone:** |

Other:

|  |  |
| --- | --- |
| **Name:** | **Email:** |
| **Work Phone** | **Mobile Phone** |
| **Alternate Email:** | **Alternate Phone:** |
| **Name:** | **Email:** |
| **Work Phone** | **Mobile Phone** |
| **Alternate Email:** | **Alternate Phone:** |

Members of the CIRT should be tasked with contacting any additional business contacts, partners, and vendors to aid in the notification requirements under state law(s)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CIRT Owner** | **Vendor Name:** | **Name** | **Email:** | **Telephone:** |
| Information Technology Coordinator | Evaluation & Remediation MSP/Vendor |  |  |  |
| City/Town/School Leader | Cyber Insurance Company | MIIA  Other |  | 800-526-6442  xxx-000-xxxx |
| Incident Response Coordinator | Local Law Enforcement | Police Chief or Resource Officer |  |  |
| Information Technology Coordinator | EOTSS SOC | EOTSS Security Operations Center | [eotss-soc@mass.gov](mailto:eotss-soc@mass.gov) |  |
| Information Technology Coordinator | Mass Fusion Center | State Police | [fusion@pol.state.ma.us](mailto:fusion@pol.state.ma.us) | 508-820-2233 |
| City/Town/School Leader | Other Municipal Officials (Mayor/Select Board) or Superintendent |  |  |  |
| Chief Financial Officer | Mass Comptroller’s Office *(If an Incident Results in a Data Breach of Personally Identifiable Information Under M.G.L. C. 93h, Additional Reporting Is Required to the Following Entities:AG Office, Office of Consumer Affairs and Business Regulations, and Affected Massachusetts Residents)* |  | [CTREmergencyNotification@Mass.gov.](mailto:CTREmergencyNotification@Mass.gov) |  |
| Incident Response Coordintaor | Mass Attorney General’s Office *(Per M.G.L. ch. 93H*  *If you know or have reason to know that your organization has experienced a data breach covered by the Breach Notification Law, you must notify the Attorney General’s Office.)* |  | <https://www.mass.gov/info-details/reporting-data-breaches-to-the-attorney-generals-office> |  |
| Outside Legal Counsel |  |  |  |  |
| Credit Monitoring/Identity theft mitigation services |  |  |  |  |
| Finance 3rd Party Vendor |  |  |  |  |
| Assessing 3rd Party Vendor |  |  |  |  |
| HR Payroll 3rd Party Vendor |  |  |  |  |
| TBD 3rd Party Vendor |  |  |  |  |
| TBD 3rd Party Vendor |  |  |  |  |

**Cyber Insurance**

|  |  |
| --- | --- |
| **Company** |  |
| **Contact** |  |
| **Phone number** |  |
| **Email** |  |
| **Insurance coverage period** |  |
| **What’s covered** |  |
|  |  |
|  |  |
|  |  |

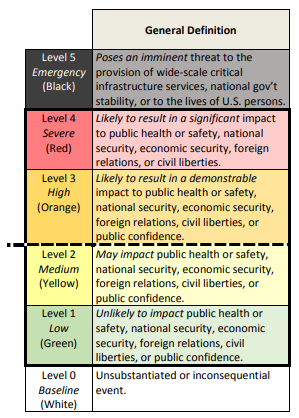
**Definitions**

|  |  |
| --- | --- |
| Cyber attack |  |
| Breach |  |
| PII |  |
|  |  |
| Destructive Attack |  |
| Disruptive Attack |  |
|  |  |
| Malware |  |
| Distributed Denial of Service - DDoS |  |
| Spoofing |  |
| APT (Advanced Persistent Threat) |  |
| Business Email Compromise (BEC/CEO Fraud) |  |
|  |  |
| Zero Trust |  |
| Multi Factor Authentication |  |
| Virtual Private Network (VPN) |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Severity Levels**

|  |  |  |  |
| --- | --- | --- | --- |
| **Level** | **Criteria** | **CIRT members involved** | **Communication Chain** |
| **Low** |  |  |  |
| **Medium** |  |  |  |
| **High** |  |  |  |

**Examples**

**Timeline

Description automatically generated**

**Policies and Procedures**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Title** | **Exists (Y/N)** | **Need to Create (Y/N)** | **Key points** | **Implementation (who will write it, how will it be delivered, is training needed, how will acceptance/compliance be tracked, etc.)** |
| **Asset Inventory** |  |  |  |  |
| **Acceptable Use** |  |  |  |  |
| **Cyber Training** |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Known Gaps**

|  |  |  |  |
| --- | --- | --- | --- |
| **Gap** | **Plan to Address** | **Team member responsible** | **Notes** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Communication Scripts**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Communication | Audience | Person responsible for writing | Legal Approval Needed | Frequency of communica- tion | Phone number for questions/ continuation of service |
| Incident Observed | Departments affected |  |  |  |  |
| Disruption in Service | Residents, Parents and Customer Services employees |  |  |  |  |
| Social Media Post | Employees and Residents |  |  |  |  |
| Progress made | Employees and Residents |  |  |  |  |
|  |  |  |  |  |  |
| Any/all of the above | Media |  |  |  |  |

**DETECTION & ANALYSIS**

|  |  |  |  |
| --- | --- | --- | --- |
| **Question** |  | **Date** | **Notes** |
| Where did the incident occur? |  |  |  |
| Who reported/ discovered the incident? |  |  |  |
| How was it discovered? |  |  |  |
| Are other areas compromised by the incident? What are they and when were they discovered? |  |  |  |
| What is the scope of the impact? |  |  |  |
| What is the business impact? |  |  |  |
| Have the source(s) of the incident been located? If so, where, when, and what are they? |  |  |  |

(SANS Institute, The Incident Handlers Handbook)

**Questions/Notes**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Known Gaps**

|  |  |  |  |
| --- | --- | --- | --- |
| **Gap** | **Plan to Address** | **Team member responsible** | **Notes** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**CONTAINMENT, ERADICATION & DISCOVERY**

|  |  |  |
| --- | --- | --- |
| **Process / Protocol** | **Description** | **Questions/Notes** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Question** |  | **Date** | **Notes** |
| Can the problem be isolated? |  |  |  |
| Are all affected systems isolated from non-affected systems? |  |  |  |
| Have forensic copies of affected systems been created for further analysis? |  |  |  |
| Have all commands and other documentation since the incident has occurred been kept up to date so far? |  |  |  |
| If the system can be taken offline proceed to Eradication phase |  |  |  |
| Can the system be reimaged and then hardened with patches and/or other countermeasures? |  |  |  |
| Have all malware and other artifacts left behind by attackers been removed? |  |  |  |

(SANS Incident Handlers Handbook)

**Questions/Notes**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Known Gaps**

|  |  |  |  |
| --- | --- | --- | --- |
| **Gap** | **Plan to Address** | **Team member responsible** | **Notes** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Documentation**

*\*see samples, page 26*

|  |  |
| --- | --- |
| **Form** | Description/Data included |
| Incident Report |  |
| Incident Detector Information |  |
| Incident Containment |  |
| Incident Eradication |  |
|  |  |
|  |  |

**POST INCIDENT ACTIVITY**

Damage Costs (include both damage cost and containment efforts)

|  |  |  |  |
| --- | --- | --- | --- |
| **Damage description** | **Cost** | **Notes** |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Policies and Procedures to update/create

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Policy | Update description | Notes | Was existing policy followed? |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Lessons Learned

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| What Worked | What Didn’t Work |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Investments to be made

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Description | Cost |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

IRP Revisions Needed

|  |  |  |
| --- | --- | --- |
| Phase | Description | Notes |
|  |  |  |
|  |  |  |
|  |  |  |

**Maintenance & Going Forward**

Tabletop Exercise Dates

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Date | Attendees | Time Allotted | Scenario | Outcome | Notes |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Additional Resources**

**CISA MS-ISAC Ransomware Guide**

<https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf>

**MS-ISAC Enhancement Incident Response**

<https://www.cisecurity.org/insights/white-papers/ms-isac-cybersecurity-enhancement-and-incident-response>

**MS-ISAC #StopRansomware Guide**

<https://www.cisa.gov/sites/default/files/2023-10/StopRansomware-Guide-508C-v3_1.pdf>

**Public Power Cyber Incident Response Playbook**

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

**SANS Cyber incident response handling forms**

<https://www.sans.org/information-security-policy>

**SANS Incident Handler’s Handbook**

<https://www.sans.org/white-papers/33901/>

**NYSAC Primer**

<https://www.nysac.org/media/amnldt2c/cybersecurity-primer-for-county-government-leaders-sept-2022-update-2.pdf>

**Cybersecurity is Everyone’s Job**

<https://www.nist.gov/system/files/documents/2018/10/15/cybersecurity_is_everyones_job_v1.0.pdf>

**NIST Incident Response Recommendations and Considerations for Cybersecurity Risk Management**

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.ipd.pdf>

**NIST Security and Privacy Controls for Information Systems and Organizations (3.8 Incident Response, p. 149)**

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>

**Collaboration: The Ultimate Cybersecurity Tool for Government**

<https://adlumin.com/resource/report/collaboration-the-ultimate-cybersecurity-tool-for-government/>

**KnowBe4 Ransomware Hostage Rescue Manual**

<https://info.knowbe4.com/ransomware-hostage-rescue-manual-0>

**Federal Government Cybersecurity Incident and Vulnerability Response Playbooks**

<https://www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf>

**Mass Cyber Center Incident Response Template and Checklist**

<https://masscybercenter.org/Response-Plan-Materials>

Selected excerpts from resource list

**CISA, MS-ISAC**

https://www.cisa.gov/sites/default/files/publications/CISA\_MS-ISAC\_Ransomware%20Guide\_S508C.pdf

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

**Public Power Cyber Incident Response Playbook**

https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf

**Overview**

* Identify your cyber incident response team
* Identify contacts and response service contracts for cybersecurity service providers and equipment vendors.
* Understand the system and environment
* Outline your incident reporting requirements and timelines
* Identify the response procedures the CIRT will take to investigate, contain, eradicate, and recover from a variety of different incidents
* Identify the external response organizations – including law enforcement, information sharing organizations, and cyber mutual assistance groups – you may engage during cyber incident response
* Develop strategic communication procedures for cyber incidents
* Define response procedures and responsibilities of the legal team during cyber incident investigation and response.

**10 Steps to Develop a Cyber Incident Response Plan**

1. Establish a Cyber Incident Response Team (CIRT)

Text

Description automatically generated with medium confidence

Text

Description automatically generated with medium confidence

Table

Description automatically generated

1. Develop a 24/7 Contact List for Response Personnel and Partners
2. Compile Key Documentation of Business-Critical Networks and Systems
3. Identify Response Partners and Establish Mutual Assistance Agreements
4. Develop Technical Response Procedures for Incident Handling
5. Classify the Severity of Cyber Incidents
6. Develop Strategic Communication Procedures
7. Develop Legal Response Procedures
8. Obtain leadership buy-in and sign off
9. Exercise the Plan, Train Staff, and Update the Plan Regularly

Graphical user interface, text, application, email

Description automatically generated

Text

Description automatically generated

Text, letter

Description automatically generated

Text

Description automatically generated

Text, letter

Description automatically generated

**SANS Cyber incident response handling forms**

https://www.sans.org/information-security-policy/

Table

Description automatically generated

Table

Description automatically generated

Table

Description automatically generated

**MS-ISAC Enhancement Incident Response**

https://www.cisecurity.org/insights/white-papers/ms-isac-cybersecurity-enhancement-and-incident-response

Diagram

Description automatically generated

Diagram

Description automatically generated

**NYSAC Primer – Questions for Executive Level Discussion**

https://www.nysac.org/media/amnldt2c/cybersecurity-primer-for-county-government-leaders-sept-2022-update-2.pdf

Table

Description automatically generated

Graphical user interface

Description automatically generated with medium confidence

**Collaboration: The Ultimate Cybersecurity Tool for Government; A Government Technology Thought Leadership Paper| Adlumin**

<https://adlumin.com/resource/report/collaboration-the-ultimate-cybersecurity-tool-for-government/>

Graphical user interface, text, application, chat or text message

Description automatically generated



Human behavior can affect your organization’s ability to response to a cyber incident. According to Sangster, managing the following leadership personas is key to building a collaborative, cohesive plan.

Graphical user interface, text, application, chat or text message

Description automatically generated

Part of the CISO’s responsibility is understanding how group dysfunctions and biases might manifest themselves, then empowering the team to make the best possible decisions rather than engage in finger-pointing and defensiveness.

***Incident response relies on making excruciating decisions quickly with not enough information to go on. It’s mapping a path for turning volatility, uncertainty, chaos and ambiguity (also known as VUCA) into the exact opposite: vision, understanding, clarity and action.***