Cybersecurity Incident Response Plan

1.0 Introduction

Evidence Action Cybersecurity Response Plan (CSRP) is crucial for keeping us vigilant and prepared to respond effectively in the event of any cyber breaches or incidents.

Given the inevitability of cybersecurity incidents, it's not a question of if they will occur, but rather when. Having a comprehensive plan in place ensures that we are equipped to take swift and appropriate actions when such situations arise.

1.1 Goals

1. Safeguard the confidentiality of employee data, and uphold the integrity and accessibility of Evidence Action's systems, networks, and associated data.

2. Assist Evidence Action's staff in restoring their operational workflows following a computer or network security breach or any form of data compromise.

3. Implement a coherent response strategy to combat system and network threats that jeopardize Evidence Action's data and infrastructure.

4. Establish and execute a communication plan encompassing initial incident reporting and ongoing updates as required.

5. Handle legal matters pertaining to cybersecurity incidents.

6. Coordinate closely with external Computer Incident Response Teams and law enforcement agencies.

7. Mitigate potential damage to Evidence Action's reputation.

1.2 Guidelines

This plan offers actionable guidelines and standard operating procedures for addressing cybersecurity incidents and data breaches effectively. It outlines the formation of a team of initial responders to such incidents, delineating clear roles, responsibilities, and communication protocols.

While primarily tailored for cyber-related incidents and breaches, this plan can also be adapted for handling data breaches unrelated to computer systems.

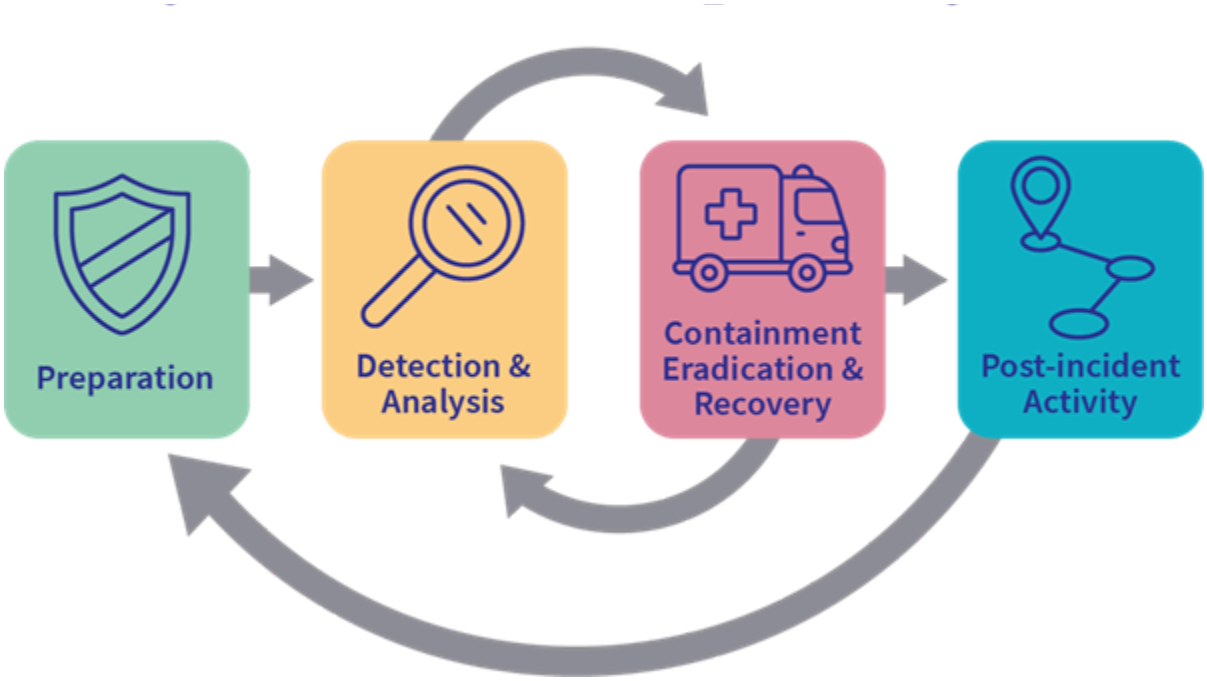
2.0 Incident Response Team (IRT)

Our Incident Response Team will comprise all members of the Global IT department, regional IT leads, as well as representatives from Operations, HR, and Communications. This team will operate across four layers, beginning with the Global IT team as the core members. The Global IT team (White team) will address issues specific to the US/GRS. For incidents that extend organization-wide, the regional IT leads will join as the Green team. If an issue impacts areas beyond IT, members from Operations and HR will be integrated as the Blue team. For incidents transcending Evidence Action, Communications and General Counsel will be involved as the Purple team. Below is the list of team members:

- Global IT Team (White Team)
- Regional IT Leads (Green Team)
- Operations Representative (Blue Team)
- HR Representative (Blue Team)
- External Communications Representative (Purple Team)
- General Counsel (Purple Team)

S/N	Team Member	Department	Function	Team Name
1	Allen Rozario	Global IT	IRT Lead	WhiteTeam
2	Kayode Yussuf	Global IT	Coordinator	WhiteTeam
3	Didas Kosenge	Global IT	Member	White Team
4	Ahmed Musa	Global IT	Member	WhiteTeam
5	Maria Kuniya	ESA IT Manager	Member	Green Team
6	Abhishek Kumar	India IT Manager	Member	Green Team
7		WCA IT Manager	Member	Green Team
8		Operations	Member	Blue Team
9		HR	Member	Blue Team
10		Communications	Member	Purple Team
11	Christopher Dunn	General Counsel	Member	Purple Team

3.0 Cyber Security Incident Response Process



courtesy: axaxl.com

Managing cybersecurity incident response is an ongoing process characterized by a cyclical pattern. The Cyber Incident Response Plan encompasses several specific elements within the incident response process, including:

3.1 Preparation:

The continuous process of enhancing incident response capabilities and preventing incidents, involves ensuring that systems, networks, applications, and data handling processes are adequately secured, and that employee awareness training is implemented. Practice exercises, commonly known as Table-top Exercises, are conducted periodically for the Incident Response Team (IRT), wherein various incident scenarios are simulated to facilitate practice sessions.

Preparation activities will be spearheaded by the CSIRT coordinator and executed by the Green Team. The CSIRT coordinator will oversee the availability of all necessary resources for the team's functioning and will report to and seek approvals from the CSIRT Lead.

3.2 Identification:

The process of confirming, characterizing, classifying, categorizing, scoping, and prioritizing suspected incidents is crucial for effective incident response.

The Cybersecurity IRT coordinator will assume leadership of this process, with support from both the Global IT team and the Green Team. The CSIRT coordinator will report findings to the White and Green Teams and seek approvals from the Global Director of IT.

How an incident becomes known significantly influences the response process and its urgency. Examples of how Evidence Action becomes aware of an incident include, but are not limited to, the following:

- Automated alerts triggered by intrusion detection systems or security monitoring tools.

- Reports from employees or users who notice suspicious activities or anomalies.

- Notifications from third-party vendors or partners.

- Analysis of system logs or network traffic revealing unusual patterns or behaviors.

- External reports or notifications from law enforcement agencies or regulatory bodies.

- Results of routine security assessments or penetration tests uncovering vulnerabilities or weaknesses.

- Notifications from customers or clients reporting unusual or unauthorized activities related to their interactions with Evidence Action systems or services.

3.3 Notification:

This section outlines procedures for notifying the Incident Response Team (IRT) of any incident occurrence and maintaining communication throughout the incident. It includes establishing an escalation process,

determining the initial point of contact, and identifying additional stakeholders who need to be informed in the event of a significant incident.

Notification will primarily be conducted through the **ticketing system** via email, unless the email system is suspected to be compromised. In such cases, alternative communication systems outside of Evidence Action, such as WhatsApp, will be utilized.

If notification needs to occur outside of office hours when recipients may not have access to email service, communication systems like WhatsApp will be employed.

Anyone suspecting an incident will notify the IRT by completing the Incident Response Form. Depending on the severity of the incident, the CSIRT coordinator will notify the CSIRT Lead and/or the White/Green Team accordingly.

3.4 Containment:

Containment efforts will focus on minimizing financial losses, safeguarding reputation, preventing service disruptions, and limiting the potential spread of infection. Initial communication with both internal and external stakeholders will be conducted as necessary.

For incidents affecting a single user and can be resolved remotely, either the CSIRT coordinator or the Green Team will be tasked with containment measures. An Incident Report Form will be logged with Operations to document the incident.

In the case of incidents impacting multiple users, all members of the White/Green Team will be mobilized under the leadership of the Global Director of IT.

For incidents causing service disruptions or affecting ongoing activities, both Operations and HR will be enlisted to assist with containment efforts. This ensures a coordinated response to mitigate the impact on operations and personnel.

S/N	Incidence	Severity	Responsible Party	Action
1	Malware/ Virus infections/ Botnets/ APTs	High	Green/ White Team	Green team isolates the end point, identifies malware, and cleans the endpoint. White team runs Bitdefender scan on endpoint
2	Unauthorized access to systems	High	Green/ White Team	Green team changes password to affected systems, implement MFA, install updates as applicable and train concerned staff
3	Hacking attacks	High	Green/ White Team	Identify and block sources of attack, carry out remediation.
4	Data breaches (within EA)	High	Green/ White Team	Identify and block source of leak, carry out remediation.

5	Data breaches (involving data outside EA)	High	Green/ White/ Blue and Purple Team	Identify and block sources of breach, carry out remediation. Inform communications so breach can be effectively communicated with external stakeholders.
6	Distributed denial of service (DDoS) attacks	High	Green/ White Team	Activate anti-DDos, activate failover system, Whitelist DDoS source IP
7	Insider threats	High	Green/ White Team	Define and detect unauthorized access
8	Privilege Escalation Attacks	High	Green/ White Team	
9	Man-in-the-Middle (MitM) Attacks	High	Green/ White Team	Change passwords, restore data to last known backup
10	Web Application Attacks	High	Green/ White Team	Setup a WAF, if possible, have a CDN. If necessary, shutdown service and have a staggered restore, testing each stage
11	Phishing/ Malvertising	Medium	White Team	Block phishing access, train user(s) and report to ticketing system
12	Password leaks	Medium	Green Team	Reset Password and report to ticketing system

3.5 Eradication: Eliminating the threat.

Threat eradication will be coordinated by the IT lead closest to the incident, with support from the CSIRT coordinator and under the leadership of the Global Director of IT.

For incidents occurring in the Africa Region, the Africa Region IT Manager will spearhead the eradication process. In India, the India IT Manager will take charge, and in the US, the IRT Co-ordinator will lead the effort.

Threat eradication activities may include conducting meetings with the affected staff to scan their computers thoroughly and ensuring the complete eradication of any infections present on their systems. This proactive approach aims to swiftly address and eliminate the threat to prevent further damage or spread within the organization.

3.6 Recovery:

Restoring computing services to normal operation and resuming business activities promptly and securely is essential for minimizing disruption and restoring confidence. Additionally, implementing measures to repair reputation and provide updates to news media, if necessary, is crucial.

For recovery efforts, the closest IT lead to the incident will take the lead, supported by the CSIRT coordinator and under the guidance of the Global Director of IT. In specific regions, such as Africa, India, or the US, designated IT managers will lead the recovery process accordingly.

Recovery is considered complete when the affected staff or services are restored to 100% functionality. A helpdesk ticket will be created via the incident form, and the ticket cannot be closed until the incident is fully resolved. This ensures that all necessary steps are taken to address the incident comprehensively and prevent future occurrences.

3.7 Post-incident Activities:

Assessing the overall effectiveness of the response and identifying areas for improvement is crucial for enhancing cybersecurity resilience. This involves analyzing lessons learned and addressing any weaknesses exploited during the incident.

The CSIRT coordinator will collaborate with the team to draft lessons learned documentation, consolidating insights and recommendations for improvement. Additionally, the Operations Incident Form will be closed upon completion of this process.

Furthermore, the insights compiled from the incident response will be incorporated into ongoing cyber fortification efforts and updates to the response plan as deemed appropriate. This iterative process ensures that the organization continuously evolves and strengthens its cybersecurity posture based on real-world experiences and emerging threats.