Responding to Cyber Attacks on Government's Information Technology Systems and IT-Enabled Public Services

CYBER SECURITY CENTRE OF EXCELLENCE

CYBER SAFE BENGAL

Prepared by:

Cyber Security Centre of Excellence (CS-CoE)
Department of Information Technology and Electronics (DIT&E)
Government of West Bengal

Responding to Cyber Attacks on Government's Information Technology Systems and IT-Enabled Public Services

1. **Purpose of this SOP:** Responding to Cyber Attacks on Government's Information Technology Systems and IT-Enabled Public Services.

2. **Scope:** The landscape of Information Technology Systems includes web portals, applications, databases, networks, servers and user terminals. All these elements are targets for cyber-attacks. Also, IT-enabled public services like e-Governance, traffic management, CCTV, health management systems, etc are delivered through Information Technology systems. Hence, cyber-attacks on these services will be carried out on their underlying IT systems.

   Cyber-attacks on critical IT systems and software may render the critical services unavailable or corrupt. This necessitates the creation of Standard Operating Systems for responding to such attacks. Employees who are on a regular basis required to operate and maintain such systems/software need a SOP for responding to perceived cyber-attacks happening to such systems.

3. **List of Stakeholders:** Stake holders for whom the SOP is relevant-

   (a) End-users – regular and contractual staff.

   (b) System administrators – employees and third-party IT support teams.

   (c) Service desk team.

   (d) Incident response team.

   (e) Program managers, team leads, developers.

   (f) Decision making authorities.

4. **Definitions**

   a. **"Website defacement"** means an attack on a website that changes the visual appearance of the site or a webpage.

   b. **"Root cause analysis (RCA)"** is a systematic process for identifying "root causes" of problems or events and an approach for responding to them.

   c. **"Security information and event management (SIEM)"** is an approach to security management that combines SIM (security information management) and SEM (security event management) functions into one security management system.

   d. **"Security protocols"** functions that performs a security-related function and applies describes how the security algorithms should be used.

   e. **"Cyber Crisis Management Plan"** means countering cyber-attacks and cyber terrorism through a framework for dealing with cyber related incidents for a coordinated, multidisciplinary and broad based approach for rapid identification, information exchange, swift response and remedial actions to mitigate and recover from malicious cyber related incidents impacting critical government process.

f. **"Cyber Security"** means cyber security as defined in section 2(1)(nb) of the Information Technology Act 2000.

g. **"Information"** means information as defined in section 2(1)(v) of the Information Technology Act 2000.

h. **"Vulnerabilities"** means existence of flaws or weakness in hardware /software of a computer resources that can be exploited resulting in their adverse or different functioning other than the intended functions.

i. **"Cyber Security Incident"** any event related to computer systems which may cause the loss of availability, integrity and confidentiality of information.

j. **"Cyber Attack"** means any attack on computer systems to steal or alter any information residing in that computer system.

k. **"Computer System"** means computer, computer system, computer network, data, computer database or software. This definition shall include including smart phones, tablets and other devices used for internet access.

l. **"Hacking"** means any unauthorized entry into any computer system or network which may or may not be for malicious purposes.

m. **"State Data Centre"** means any computer system or collection of computer systems used to store, process, store and disseminate data belonging to any government organization or department of the State Government. The Data Centre may not necessarily be located physically in the State of West Bengal for being considered a State Data Centre.

n. **"Security Audit"** means a computer security audit is a manual or systematic measurable technical assessment of a system or application. Manual assessments include interviewing staff, performing security vulnerability scans, reviewing application and operating system access controls, and analysing physical access to the systems.

o. **"CERT-In"** means the Indian Computer Emergency Response Team created on 19 January 2004. It is the nodal agency to deal with cyber security threats. It strengthens security-related defence of the Indian Internet domain.

5. **Standard Operating Procedure (SOP) for cyber-attacks on Web-Portals**

Web portals can be broadly classified into following categories - Government, Institutional and Individual. While for the purpose of cyber security, web-portals can be classified into two categories

- Static (view only) and
- Dynamic (responsive).

This document would deal with the common types of cyber-attacks that can affect web-portals and establish a broad level SOP for countering them.

SOP for responding to various cyber-attacks:

Website defacement (for Static web pages)

a. Create a backup repository of the web-page source code. Store the source code in a ready to deploy environment.

b. Ensure the backup source code repository is updated in case of any changes to the web-page.

c. In case website defacement is detected, immediately lower the website with a notice "Website is under maintenance."

d. Deploy the back-up source code on an alternate web-server.

e. Update domain routing information for the website to point to the alternate domain server.

f. Conduct a root cause analysis (RCA) to investigate how the security protocols of the web-page were breached.

g. Publish the report of the RCA and ensure that identified security vulnerabilities are corrected.

h. Restore routing to original hosting address (if required).

i. Lodge an FIR of website defacement with the police under Section 65 of the Information Technology Act, 2000.

j. Assist the police in conducting forensic investigation as and when required.

k. Create a log of the whole incident, identify the lacunae that resulted in the said compromise and put in place a constant monitoring of the web-page for further/repeat attacks.

Denial of Service (DOS) Attack

A denial-of-service (DOS) attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

For example, the infamous ransomware attacks occurred in 2016-17 viz. WannaCry and Petya/NotPetya.

DOS attacks are very common against government websites all over the world and the result is to render the web-services un-usable.

SOP for DOS in static web-portals –

SOP for DOS for static web portals would follow the same steps as for website defacement.

In addition, configure the perimeter firewall of the web-server allowing only stateful connections into the environment so as to not allow unauthorized web traffic.

SOP for DOS in transactional/ dynamic web-portals –

Dynamic web-portals can be for either financial/non-financial or composite purposes.

For financial web-portals SOP is specific to the services extended. Hence, tailor-made SOP is required for countering cyber-attacks. Individual web-site owners are responsible for formulating and implementing it.

For non-financial dynamic web-portals (email server, information exchange, eOffice, etc) the SOP for responding the cyber-attacks can be broadly enumerated as under -

a. Implement all security protocols for protecting the web-portals from inside and outside the perimeter attacks.

b. Implement an SIEM solution for monitoring of the server on which the web-portal is hosted.

c. Mirror server ought to be implemented at a Disaster Recovery (DR) site.

d. In case of a suspected cyber-attack on a dynamic government server, immediately isolate the server and disconnect it from all networks *by unplugging the network cable from network port*.

e. Mirror server has to be activated from the Disaster Recovery (DR) site with real time data backup so that citizen-centric services are not disrupted.

f. Lodge an FIR of website defacement with the police under Section 65 of the Information Technology Act, 2000.

g. Assist the police in conducting forensic investigation as and when required.

h. Create a log of the whole incident, identify the lacunae that resulted in the said compromise and put in place a constant monitoring of the web-page for further/repeat attacks.

6. **SOP for responding to Cyber Attacks on Government Public Services**

We are considering the following public services for the scope of this SOP –

A. Traffic management (Police)

B. CCTV surveillance (Police)

C. Health Management Systems (Health Department)

<u>SOP for countering cyber-attacks on traffic management systems</u>

a. Deploy parallel instances of server running on at least one primary and one DR site. The more redundancies available, the better.

b. Ensure geographical and network separation of the primary and redundant servers to ensure that a cyber-attack on one site does not affect operational functionality.

c. Conduct a network and application layer vulnerability analysis and penetration testing. Mitigate all major vulnerabilities discovered.

d. Conduct site audit and ensure security of Information Systems Infrastructure.

e. If required, deploy honeypot/ honey net servers to divert cyber attacks.

f. For contingencies - prepare a plan for carrying out manual traffic management for any part of the city or for the entire city as required.

g. Test the plan by carrying out a table top activity

h. Train staff and conduct mock drills.

i. In case any cyber-attack is detected on an individual server, isolate the server from network and manage operations through back-up server/mirror server from DR site.

j. Conduct an incident analysis and mitigate the vulnerability.

k. If foul play is suspected, file FIR under section 65 of IT Act, 2000 and conduct forensic analysis

l. In case of major cyber-attack affecting all systems (including DR site), explore possibility of mitigation without taking all systems offline.

m. First try to conduct operations by shifting fully to DR and trying to mitigate attack on primary site, and vice versa.

n. If IT services are rendered fully unavailable, immediately invoke manual operations plan to ensure continuity of operations is not affected.

o. Team responsible for putting manual operations into action need to be identified in the plan and their responsibilities defined and memorized by them.

p. All staff members need to be communicated the contact details of team members responsible for manual operations.

q. Ensure urgent resolution and restoration of IT services – ensure the systems are resilient to future similar attacks.

r. If foul play is detected, file FIR under section 65 IT Act, 2000.

s. Conduct an RCA and take necessary sustained preventive actions.

SOP for countering cyber-attacks on CCTV surveillance

CCTV surveillance has opened a new avenue for potentially deadly cyber-crimes as cameras can be hacked and used to relay incorrect visuals.

SOP for countering any suspected cyber-attack at CCTV systems is as under -

a. Conduct a background verification of all personnel involved in monitoring CCTV consoles and having management access to the cameras.

b. Conduct a risk assessment for assessing possible cyber-attacks in hacking and controlling CCTV cameras.

c. Take all possible action for ensuring all vulnerabilities identified in the risk assessment are removed.

d. Deploy parallel instances of server running on at least one primary and one DR site.

e. Ensure geographical and network separation of the primary and redundant sites to ensure that a cyber-attack on one server does not affect other servers.

f. Deploy a SIEM solution (customized for CCTV oversight).

g. Train staff on how to recognize manually the tell-tale signs of any camera being hacked.

h. In case any discrepancy is recognized immediately isolate the camera/system from the network and start investigations.

i. In case whole network is suspected to be compromised, disable all feeds until investigation is complete and all suspected attacks are mitigated.

j. If foul play is detected, file FIR under section 65 IT Act, 2000

k. Conduct an RCA and take necessary sustained preventive actions.

SOP for countering cyber-attacks on Health Management Systems

IT infrastructure belonging to the Health Management Systems are very sensitive and critical. Compromise of availability and unauthorized access to these systems can have severe consequences with regard to public health and welfare.

SOP for cyber-attack on Health Management Systems –

a. For systems maintaining life support and critical patient information ensure separation from all external networks. All such systems must only be running on internal LAN with no interface with systems connected to internet/ public networks.

b. There must be multiple redundancies in terms of availability of servers, so that in case of unavailability of one node (server) due to an attack, other servers can ensure continuity of service.

c. Conduct site audit and ensure security of Information Systems Infrastructure.

d. For all systems apart connected to public networks conduct a network and application layer vulnerability assessment and penetration testing, to identify and mitigate all vulnerabilities.

e. Conduct a background verification of all personnel involved in monitoring and management of systems.

f. For contingencies - prepare a plan of action for manual continuity of health services

g. Rigorously test the plan by conducting mock drills and make any required changes

h. In case any cyber-attack is detected on an individual server, isolate the server from network and manage operations through back-up server.

i. If IT services are rendered fully unavailable, immediately invoke manual operations plan to ensure continuity of operations is not affected.

j. Ensure urgent resolution and restoration of IT services – ensure the systems are resilient to future similar attacks.

k. If foul play is detected, file FIR under section 65 IT Act, 2000

l. Conduct an RCA and take necessary sustained preventive actions.

7. **Employee Dos and Don'ts**

Employee dos and don'ts for dealing with cyber-attacks.

What to do –

a. Watch for signs of abnormality in terms of system behavior viz. *abnormally slow booting, long buffering, system dysfunctional by becoming non-responsive, conflicting error message flash, multiple action against single command, undesired opening of browser, uncontrollable cursor (mouse pointer) activities, inability to defrag the machine and/or clearing registry, filling up inbox with unwarranted spam emails, inability to delete emails, unwanted segregation of emails, receiving executable files and/or hyperlinked files as attachments etc.*

b. In case any abnormality is detected, immediately contact service desk/ system administrator.

c. Close all unnecessary services, functions and applications running on the system and shut-down with unplugging from power source along with network socket.

d. Affected system should be revived for checking and restoration in isolation.

What not to do –

a. Do not panic.

b. Do not send or forward emails with attachments.

c. Do not use a USB for taking back-up from an affected system.

d. Do not attempt to trouble shoot problems without contacting system administrator/ help desk.

e. Do not attempt to force shut down systems without backup.

f. Do not fail to report any systems abnormalities and take screenshot as well as save them as image files in drive other than C: (System) and D: (Image of system/Backup) of as many instances as possible.
