

Bandhan Financial Service Ltd.

Head Office, Kolkata – 700091



Cyber Crisis Management Plan (CCMP)

Doc ID: BFSL-CCMP-001

Prepared By: Chief Financial Officer

Reviewed By: Managing Director

Recommended By: Company Secretary

Date of Approval of the Board:

Effective Date of this chart:

Revision History

Date	Version	Description
29-September- 2020	1.0	Base documentation

Contents

1. INTRODUCTION	3
2. NATURE OF CYBER CRISIS	3
3. CYBER SECURITY THREAT LANDSCAPE	3
4. PREVENTION AND PRECAUTIONARY MEASURES	4
5. MITIGATION STEP	5
5.1 Web Application attack:	5
5.2 DDOS attack	5
5.1 DNS attack	6
5.2 Mitigation steps for Attack attempts/scanning / probing on Servers, Routers, Firewall (for Network /Server /Application Team)	6
5.3 Email server attack	6
5.4 Spam attack	7
5.5 Social Engineering attack	7
5.6 Application attack:	8
5.7 Internal Threat:	8
6. INCIDENT REPORTING PROCEDURES	9
6.1 Reporting of an Incident	9
6.2 Contents of Incident Report	9
6.3 Verification	9
6.4 Incident Response	10
6.5 Incident Reporting Form	10
7. INCIDENT HANDLING TEAM STRUCTURE	10
7.1 Level 1:	10
7.2 Level 2:	10
7.3 Level 3:	11

1. INTRODUCTION

The Cyber Crisis Management Plan (CCMP) provides the strategic framework and guides actions to prepare for, respond to, and begin to coordinate recovery from a cyber-incident.

CCMP Covers different type of cyber crisis, possible targets and related impact, actions and responsibilities of concerned stakeholders, cyber incident response coordination among Ministries/Departments of Central/State Government and Critical Information Infrastructure organizations to deal with cyber crisis situations.

CCMP for BANDHAN FINANCIAL SERVICES LTD. shall assist to put in place mechanisms to effectively deal with cyber security crisis such as interruption or manipulations of critical functions/services are brief, infrequent and manageable and cause least possible damage.

2. NATURE OF CYBER CRISIS

The field of cyber security is technology intensive and new vulnerabilities emerge with progress in technology giving rise to new types of incidents. BANDHAN FINANCIAL SERVICES LTD. being in a financial sector company, following may be the applicable possible Cyber-attacks

- Individual systems to gain access of person information.
- Data theft which can cause business interruption

3. CYBER SECURITY THREAT LANDSCAPE

Cyber security threat landscape classified based on attack target, motive, Attack vector, attack elements. Following are the possible applicable landscape for BANDHAN FINANCIAL SERVICES LTD..

- Attack Targets
 - Critical infrastructure such as IT network
 - Business intelligence of IT network
 - Personally identifiable information for Individuals, Management
- Attack Motives
 - Disruption of Services and by launch cyber war
 - Cyber espionage
 - For fun
 - Financial frauds such as tariff manipulation, individual's personal account manipulation.

- Attack Actors/elements
 - Nation / states sponsored attackers
 - Cyber criminals
 - Hacker groups
 - Malicious Insiders
- Attack vectors and medium
 - Botnets
 - Vulnerabilities and Exploit tool kits
 - Social engineering
 - Ignorant users

4. PREVENTION AND PRECAUTIONARY MEASURES

Cyber crisis management of BANDHAN FINANCIAL SERVICES LTD. is defined as ability of organization to

- **Anticipate:** Maintain a state of informed preparedness in order to forestall compromises of business functions from adversary attacks
- **Withstand:** Continue essential business functions despite successful execution of an attack by an adversary
- **Contain:** Localize containment of crisis and isolate trusted systems from untrusted systems to continue essential business operations in the event of cyber attacks
- **Recover:** Restore business functions to the maximum extent possible subsequent to successful execution of an attack by an adversary
- **Evolve:** To change missions/business functions and/or the supporting cyber capabilities, so as to minimize adverse impacts from actual or predicted adversary attacks

To address cyber crises, at BANDHAN FINANCIAL SERVICES LTD. has defined following set of actions aimed at rapid response & remedial measures and recovery & restoration of normalcy in the event of a build-up or emergence of a crisis

- Nomination of Chief Information Security Officer CISO
- Information Security Policy & implementation
- Follow best practice of best practices
- Defining Business Continuity Plan(BCP)
- Conducting Security audit of Information infrastructure and network
- Network traffic scanning
- Isolation of critical networks
- Implementation of Security guidelines issued by concerned authorities
- Background checks
- Audit & Assurance
- Security training & awareness
- Sharing of information pertaining to incidents

5. MITIGATION STEP

Following are the defined best practices of cyber security mitigation steps to be followed at BANDHAN FINANCIAL SERVICES LTD..

5.1 Web Application attack:

Serious weaknesses or vulnerabilities allow criminals to gain direct and public access to databases in order to churn sensitive data – this is known as a web application attack. Many of these databases contain valuable information (e.g. personal data and financial details) making them a frequent target of attacks.

Mitigation steps for Web application attacks (for Server/Application Team)

- Isolate affected server from internet or Disable the affected module in application.
- Scan all files for web shells or any malicious footprint.
- Take a copy of all the logs at the server, permit level (IDS/IPS, Firewall) and traffic trends.
- Identify the type of attacks and vulnerability exploited.
- Patch the vulnerability /issue by modifying insecure code/configuration by secure code.

5.2 DDOS attack

DDoS is short for Distributed Denial of Service. DDoS is a type of DOS attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack. Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack. In a DDoS attack, the incoming traffic flooding the victim originates from many different sources – potentially hundreds of thousands or more. This effectively makes it impossible to stop the attack simply by blocking a single IP address; plus, it is very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin.

Mitigation steps for DOS/DDOS/NTP Based DDOS attacks (for Network Team)

- Take a copy of all the logs at the perimeter level (IDS/IPS, firewall) and traffic trends.
- Identify the type of attacks such a flooding of particular types of packets/requests.
- Allocate traffic to unaffected available network paths.
- Implement egress and ingress filtering to block spoofed packets.
- Use appropriate DOS prevention and mitigation tools.
- Install updated software patches on all the network devices such as routers, firewalls, IDS,IPS and switches.

5.1 DNS attack

A DNS attack is an exploit in which an attacker takes advantage of vulnerabilities in the domain name system (DNS). When an end user types the people-friendly domain name into a client's browser, a program in the client's operating system called a DNS resolver looks up domain name's numerical IP address. First, the DNS resolver checks its own local cache to see if it already has the IP address for domain name. If it doesn't have the address, the resolver then queries a DNS server to see if it knows the correct IP address for domain name. DNS servers are recursive, which simply means that they can query each other to either find another DNS server that knows the correct IP address or find the authoritative DNS server that stores the canonical mapping of the domain name to its IP address. As soon as the resolver locates the IP address, it returns the IP address to the requesting program and caches the address for future use.

Mitigation steps for DNS attacks (for Server Team)

- Check for version updates at the DNS server and install latest software patches.
- Implement spoofing countermeasures.
- Use unicast reverse path forwarding to mitigate problems that are caused by malformed or forged IP source addresses.
- Adopt source IP address verification.
- Implement DNS Security.

5.2 Mitigation steps for Attack attempts/scanning / probing on Servers, Routers, Firewall (for Network /Server /Application Team)

- Check for effectiveness of filtering rules in the routers, firewall and IPS and reconfigure if required.
- Check the logs of these devices for source of attacks.
- Change all user / root / administrator passwords in all network devices.

5.3 Email server attack

In Internet usage, an email bomb is a form of net abuse consisting of sending large volumes of email to an address in an attempt to overflow the mailbox, overwhelm the server where the email address is hosted in a denial-of-service attack (DoS attack) or as a smoke screen to distract the attention from an important email messages indicating a security breach.

Mitigation steps for Mail Server attacks (for Email Administrator)

- Deploy hot standby mail servers in physically separated networks and places which can be made operational when the mail server is attacked.
- Disable all other ports and services on mail servers.
- Enforce strong password policy and encourage users to change passwords periodically.

5.4 Spam attack

Email Spam is the electronic version of junk mail. It involves sending unwanted messages, often unsolicited advertising, to a large number of recipients. Spam is a serious security concern as it can be used to deliver Trojan horses, viruses, worms, spyware, and targeted phishing attacks. Spam is any kind of unwanted, unsolicited digital communication, often an email that gets sent out in bulk. Spam is a huge waste of time and resources. The Internet service providers (ISP) carry and store the data. When hackers can't steal data bandwidth from the ISPs, they steal it from individual users, hacking computers and enslaving them in a zombie botnet. Software providers invest resources creating email applications that try to filter most of the spam out. Consumers waste time sifting through whatever makes it past the spam filters.

5.5 Social Engineering attack

Social engineering, in the context of information security, is the psychological manipulation of people into performing actions or divulging confidential information. This differs from social engineering within the social sciences, which does not concern the divulging of confidential information. One example of social engineering is an individual who walks into a building and posts an official-looking announcement to the company bulletin that says the number for the help desk has changed. So, when employees call for help the individual asks them for their passwords and IDs thereby gaining the ability to access the company's private information. Another example of social engineering would be that the hacker contacts the target on a social networking site and starts a conversation with the target. Gradually the hacker gains the trust of the target and then uses that trust to get access to sensitive information like password or bank account details.

Mitigation steps for advanced targeted attacks including spoofing, spam attacks and social engineering

- Examine incoming emails for social engineering attempts/spoofing through header/content analysis.
- Report suspicious emails with attachments and headers to administrator.
- Identify the target entities and sensitize them about the targeted attacks.
- Isolate systems found to be connecting to suspicious domains/hosts after
- Preserving volatile data and create forensic image for further analysis.
- Based on analysis of incident, apply appropriate security controls such as patching the targeted application, updating antivirus signature to detect crafted malware and detecting connections to call back domains/hosts through perimeter devices.

5.6 Application attack:

Serious weaknesses or vulnerabilities allow criminals to gain direct and public access to databases in order to churn sensitive data – this is known as a web application attack. Many of these databases contain valuable information (e.g. personal data and financial details) making them a frequent target of attacks. Although such acts of vandalism (often performed by the so-called script kiddies) as defacing corporate websites are still commonplace, nowadays attackers prefer gaining access to the sensitive data residing on the database server because of the immense pay-offs in selling the results of data breaches. In the framework described above, it is easy to see how a criminal can quickly access the data residing on the database through a dose of creativity and, with luck, negligence or human error, leading to vulnerabilities in the web applications. If web applications are not secure, i.e. vulnerable to at least one of the various forms of hacking techniques, then your entire database of sensitive information is at serious risk of a web application attack. SQL Injection attack types, which target the databases directly, are still the most common and the most dangerous type of vulnerability. Other attackers may inject malicious code using the user input of vulnerable web applications to trick users and redirect them towards phishing sites. This type of attack is called Cross-Site Scripting (XSS attacks) and may be used even though the web servers and database engine contain no vulnerability themselves. It is often used in combination with other attack vectors such as social engineering attacks. There are many other types of common attacks such as directory traversal, local file inclusion, and more.

Mitigation steps for application level attacks

- Take all logs (system, application, security, access, error) of affected system and data there in and keep them separately for analysis and forensics.
- Change all user / root / administrator passwords in all systems.

5.7 Internal Threat:

A threat originating inside a company, government agency, or institution, and typically an exploit by a disgruntled employee denied promotion or informed of employment termination. Such exploits also can be launched by an attacker who has sought temporary employment with a target and uses social engineering skills to get on the inside. An insider threat is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems. The threat may involve fraud, the theft of confidential or commercially valuable information, the theft of intellectual property, or the sabotage of computer systems. The insider threat comes in three categories:

- Malicious insiders, which are people who take advantage of their access to inflict harm on an organization;

- Negligent insiders, which are people who make errors and disregard policies, which place their organizations at risk; and
- Infiltrators, who are external actors that obtain legitimate access credentials without authorization.

Insiders may have accounts giving them legitimate access to computer systems, with this access originally having been given to them to serve in the performance of their duties; these permissions could be abused to harm the organization. Insiders are often familiar with the organization's data and intellectual property as well as the methods that are in place to protect them. This makes it easier for the insider to circumvent any security controls of which they are aware.

Mitigation steps for internal threats (user related)

- Take all logs (system, application, security, access, error) of affected system and data there in and keep them separately for analysis and forensics.
- Check for effectiveness of filtering rules in the routers, firewall and IPS and reconfigure if required.
- Change all user / root / administrator passwords in all systems and network devices.

6. INCIDENT REPORTING PROCEDURES

6.1 Reporting of an Incident

Employees can report an adverse activity or unwanted behaviour which they may feel as an incident to IT administrator/CSO.

6.2 Contents of Incident Report

The following information (as much as possible) may be given while reporting the incident:

- Time of occurrence of the incident
- Information regarding affected system / network
- Symptoms observed
- Relevant technical information such as security systems deployed, actions taken to mitigate the damage.

6.3 Verification

Emergency Response Team (ERT) will verify the authenticity of the report.

6.4 Incident Response

Information Security Wing will assist the concerned branch / office in the following broad aspects of incident handling:

- Identification: To determine whether an incident has occurred, if so analysing the nature of such incident, identification and protection of evidence and reporting of the same.
- Containment: To limit the scope of the incident quickly and minimize the damage.
- Eradication: To remove the cause of the incident.
- Recovery: Taking steps to restore normal operation.

6.5 Incident Reporting Form

Cyber Event / Incident should be reported in the defined format to RBI

Event /Incident Reporting Form is enclosed in this policy as Annexure -1.

7. INCIDENT HANDLING TEAM STRUCTURE

7.1 Level 1:

Information Security Wing (Incident Resolution Team)

The Information Security Wing (ISW) is the place where all security incidents are to be registered and analysed. Incidents that cannot be resolved immediately by the Information Security Wing (ISW) are to be assigned to the concerned functional group. Resolution or work around should be established as quickly as possible in order to restore service to users with minimum disruption to their work. After resolution of the cause of the incident and restoration of service, the incident is closed.

The functions of ISW are as follows:

- Identify the correctness of the severity level.
- Contain, Eradicate and recover.
- Seek necessary resources and support from functional group/team.
- Provide regular update to corresponding level II incident resolution team.
- Escalate to the corresponding level II incident resolution team, if unable to resolve within the prescribed timeframe/reasonable time frame.

7.2 Level 2:

Emergency Response Team (ERT)

Cyber Incident is an adverse event whereby some aspect of a computer/information system is threatened. Incidents that are to be reported include below:

- Attempts from unauthorized sources to access systems or data e.g., ransomware, malware, virus found incidents.
- Unplanned disruption to a service e.g., Distributed Denial of Service (DDoS) attack, Denial of Service (DoS) attack
- Unauthorized processing or storage of data.
- Unauthorized transactions involving Point of Sale (POS), Automated Teller Machine (ATM) cards.
- Unauthorized changes to system hardware, firmware, or software along with any other incidents which causes any unplanned interruption to any service, a reduction in the quality of any service or an event that has impacted the service to any customer.

The functions of ERT are as follows:

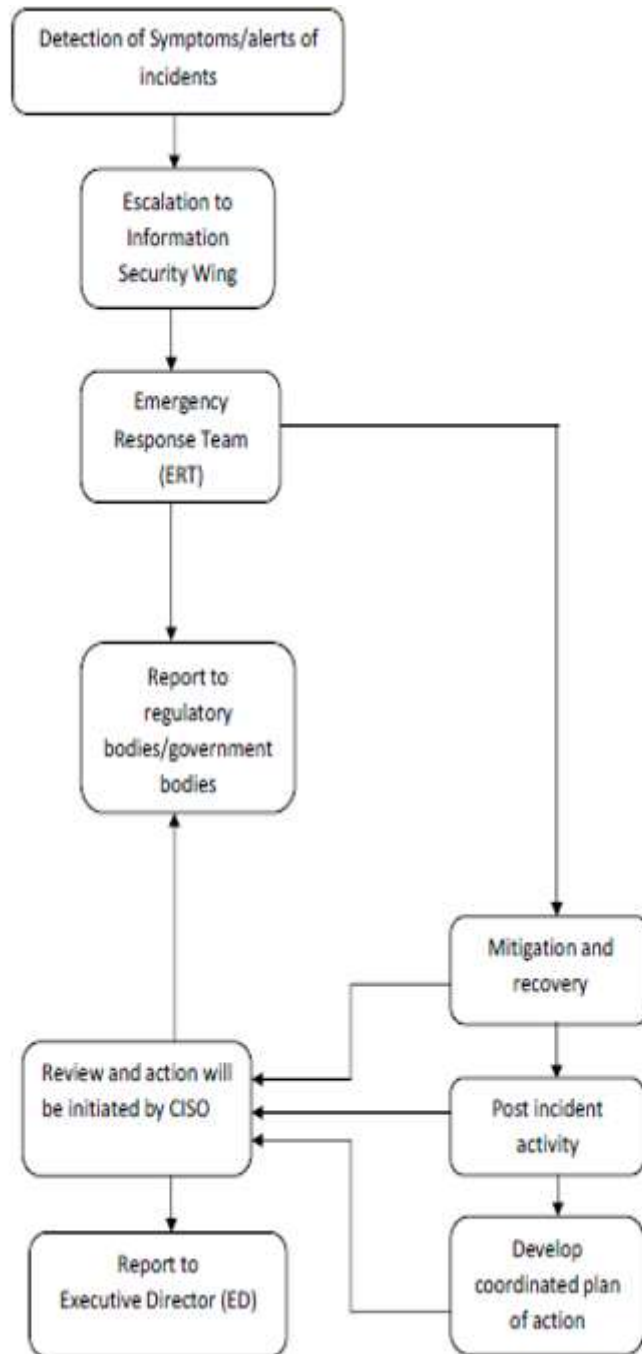
- Provide support to the level I incident resolution team to facilitate prompt containment, eradication and recovery of the affected site.
- Maintain contact with CERT-In and respective nodal agency.
- Supervise and coordinate and information sharing on security incident to government regulatory bodies on time bound manner.

7.3 Level 3:

Top Management Information System Security Committee (TMISSC)

All the incidents reported and occurred will be discussed and remedial actions will be taken with the proper approval from the committee and board.

Flow Chart for Incident Handling & response:



Cyber Event/Incident Report:

1. Contact information for this incident				
Name				
Place of Incident				
Email				
Mobile Number				
2. Security Event Occurrence Date and Time				
Date :		Time:		
3. Physical location of affected system				
IP Address of affected system	Operating System	MAC Address	Host name & Server Name	No of Files Impacted/Size of Files Impacted (Should be in Figure)
4. Description of the Incident:				
5. Date of application of Last Patch / Updation				
6. Data Encrypted(Y/N):				
7. How many Host(s) are affected?				
8. Interface Affected (Public network/ Internal Network)				
9. Is the compromised machine connected to a network? Yes/No. If yes , details				
10. System Isolated from network(Y/N)?				
12. Whether the system is having antivirus? Y/N				
13. Has this problem been experienced earlier? If yes, details.				
14. Expected loss of Amount(Should be in Figure):				
15. Control Measures taken, if any:				