PRISM JOHNSON LIMITED

CIN: L26942TG1992PLC014033
Registered Office: 305, Laxmi Niwas Apartments, Ameerpet, Hyderabad – 500 016.
Corporate Office: "Rahejas", Main Avenue, V. P. Road, Santacruz (West), Mumbai – 400 054.

February 15, 2024

CYBER SECURITY POLICY

PURPOSE

The purpose of this document is to enable the IT security operations centre team, incident handlers and responders with sufficient information and guidelines to follow when a cyber-security crisis / incident occurs at Prism Johnson Limited (PJL). This document aims at providing detailed information on the steps and the workflow to be followed in the event a cyber-security crisis incident occurs.

SCOPE

The document applies to all the information technology assets, equipment and devices that are part of Prism Johnson Limited's cyber space environment such as desktops, laptops, applications, servers, databases, network devices, security devices equipment's etc.

The Cyber Crisis Management Plan (CCMP) shall be followed and executed by the employees and vendors deployed by PJL in the IT department providing services to various departments in PJL.

INVOCATION OF CYBER CRISIS MANAGEMENT PLAN (CCMP)

The major steps followed during invocation of CCMP are as below:

Primary objective of CCMP is to define the incident response actions during first hour is to contain the damage due to the incident, notify appropriate authorities about the incident and ensure continuity of essential activities and services.
Analyze the incident based on the data available, define the severity level based on the impact. Take all logs of affected systems for analysis and to correct, eradiate and recover.

1. **Identification**
   a. Identification of the incident from all possible channels involved
   b. Verification of the incident if it is a normal incident or a cyber-crisis
   c. Decision of invoking the CCMP shall be taken at this stage

2. **Response and Containment**
   a. Depending on the type of incident, take appropriate action
   b. Inform the affected parties

3. **Communication**
   a. Detailed inputs shall be taken along with other major incident
   b. Timely and continuous communication to all the interested parties viz. at the identification of incident, during the course of incident for action being taken.

4. Recovery and Preventive maintenance

a. Based on the incident resolved, preventive steps to be planned and executed

b. The recovery and preventive measures shall be discussed and communicated to all the relevant entities in PJL to avoid the happening in near future.

Severity Level	Description	Impact	Security Incident Examples
P1	Security breach has occurred and validated. Disclosure of information, user validated Security incident of any Tier 0 system	Highly Notable Outages – complete business interruption due to a breach of information security	Malicious attack or active hacking penetration, in progress for applications. Loss of customer or employee confidential information. Loss of PJL's intellectual property.
P2	Impaired operations due to a security incident resulting in significant business impact.	Impairment of the company's ability to use non-core applications with significant business impact affecting on individual areas with in enterprise	Slow performance of websites due to active web attack. Network bandwidth choke
P3	Minor business impact, isolated security incident on a single system. Unauthorised or inappropriate access.	Applications/components in sub network which is down, resulting is system unavailability to a set of employees, business users or customers in a defined area/location	Data classification error impacting multiple users, repeated failed logins attempts indicating a password cracks attempt. Network device down with workaround. Virus detected on a single machine
P4	Minimal or No Business Impact. Security events requiring additional research	Component, minor application, Sub network down or slow/difficult to use for the users	Non critical security events indicating a security may have occurred but needs to be validated. Data error with workaround , VPN issues, WiFi access point failures

P1 – Critical, P2 – High, P3 – Medium, P4 - Low

RACI Matrix

Stages	Responsible	Accountable	Consulted	Informed
Identification	IT Security Officer	IT Security Officer / IT Head	Information security team	CEO, COO, Top Management
Response and containment	IT Security Officer	IT Security Officer / IT Head	Information security team	CEO, COO, Top Management
Breach communication and notification	IT Security Officer	IT Security Officer / IT Head	IT and Digital head	CEO, COO, Top Management
Recovery and preventive measures	IT Security Officer	IT Security Officer / IT Head	Information security team	CEO, COO, Top Management

Throughout the cyber security crisis management stages, it is essential that appropriate teams/stake holders shall be notified. This involves communicating to IT and business management levels about the impact and progress of the crisis response.

Department heads will ensure to follow the procedures laid down for the crisis communication is followed.

Stages	Responsible	Accountable	Consulted
Identification	IT Security/Infra/ Digital SPOC	IT Security Head	Information Security Team
Response & Containment	IT & Digital Team	IT & Digital Head	Information Security Team
Communication and Notification	IT Security Head/ / IT Infra/Digital Team	IT & Digital Head	CFO
Recovery & Preventive Measures	System Owner	IT & Digital Head	Information Security Team

5.Exceptions

Where there is a justifiable business need that requires actions to be performed which are in conflict to this document, such exceptions shall be reported to the IT Head and CFO and approval shall be obtained. Such approvals shall be valid for a pre-defined period after which it shall be re-evaluated and re-approved.

6. Preventive Measures

In the present digital age, sensitive information is collected and transmitted through digital channels and IT tools, making it vulnerable to cyber threats such as hacking, phishing, malware, and ransomware. A successful cyberattack or data breach can compromise customer privacy, damage an organization's reputation, and result in financial losses.

The security of corporate data/information, applications, systems, and networks is fundamental to the continued success of (PJL) Prism Johnson Limited. Cyber Security management seeks to establish controls and measures to protect its IT infrastructure and data to minimize the risk of loss of information and system resources. The key controls can be classified in following broad categories.

a) **Blocking of USB ports**: The USB ports on all the end user devices like laptops and desktops are blocked so no data can be copied to another devices like pen drives. Top management employees are exempted from this.
b) **Secured Connectivity through VPN**: The business critical application like SAP which is used for financial transactions, pricing records, invoices etc. can be accessed only through secured VPN connections. Only authorised users are given role based permissions to make entries or run reports in the application.
c) **Multifactor Authentication**: Multifactor Authentication is also enable to connect to critical financial applications like SAP ERP
d) **Firewalls**: These are tools that help to protect edge computing devices, networks devices from cyber threats such as viruses, malware, and hacking attempts.
e) **Regular software updates**: Regularly updating software and systems can help to patch vulnerabilities and reduce the risk of cyberattacks.
f) **Employee training**: Educating employees about cybersecurity best practices and providing regular training can help to reduce the risk of human error, which is a common cause of cyber incidents.
g) **Antivirus Software**: Each end users devices like laptop, desktop, and servers are installed with antivirus software which runs are period intervals to scan and check the device for detect presence of any virus.
h) **Back up**: Backups are generally classified as full, differential, or incremental. Critical application like SAP data is backup daily to backup servers. Every 5 minutes the incremental data is backed up and full back-up at end of the day.

7. Cyber Security Monitoring and Incident Detection

Monitoring shall be carried out by SOC team 24*7 (proposed process). In case of any suspicious activities, the SOC team does the preliminary investigation and intimates the IT Security Officer in the respective division.
Based on the incident analysis and the suggested measures the IT Security Officer coordinates with the application team and/or the Infra team to get the problem resolved.

Responsibilities

The primary objective of incident response management team is to contain the damage due to the incident, notify appropriate authorities about the incident and ensure continuity of essential activities and services.

- Analyse the incident based on the reported information and available data.
- Limit access to the systems and networks from outside in the consultation with the service providers.
- Diagnose and restore service for all issues in the areas or expertise.
- Take all logs of effective system for analysis.
- Take all required corrective measures to eradicate and recover.
- Prepare the incident report with details and report to the concerned authorities/stakeholders

8.0 Possible Crisis Scenarios and Action Plan

8.1.0 Website Defacement Attack

Website defacement is a type of attack where the attacker changes the contents of your website to something intended to embarrass the company. The attacker finds a way to modify the files or contents of your website without your permission.
Website defacement attacks differ from other cybersecurity threats. Most malicious attackers try to hide their activities, but in website defacement, the activists deface websites to create noise and attract attention and raise awareness of what they see as that company's misdeeds. They're doing it to show off. Sometimes, they'll do this purely for the "fun" of it or to increase their online credibility. Other times, attackers are there to speak out about causes they believe in

In this scenario, the objective of the adversary is to bring reputation damage to the company by changing the content on the website with some other content, visual appearance of the whole site, home page or particular web page.

Below is the indicative list of security threat events that are related to Website defacement

- Compromise of system/user accounts in a web server (through PIM solution)
- Attempt of SQL Injection in the web server
- Unauthorized changes to the web server content
- Change in the pattern of the web server
- Frequent Comparison of web page checksum

8.1.1 Incident Response and Containment

Step 1: Disconnect the web server from the network.
Step 2: Redirect the web server traffic to the DR site or the standby server IP address
Step 3: Take a full backup of the defaced web server pages/directory to blank disk/tape
Step 4: Search for any traces of the adversary accessing the web server and making changes to the web pages.
Step 5: Search for trigger of clear audit log events
Step 6: Reset the passwords for all the accounts in the web server.

8.1.2 Recovery and Preventive Measures

Recovery Measures

- From the original backup of the clean web server, restore the web page.
- Harden the web server, disable all unwanted services
- Perform a complete AV scan to ensure there is no malware or backdoors to the adversary to redo the defacement.
- Ensure all the users and system accounts password are reset in the web server.
- Calculate and store the new checksum for the web server pages

Preventive Measures

Continuously monitor the access and changes to the web server

- In the Firewall/IPS, enable SQL Injection, Buffer Overflow attack protection for the web server.

8.2.0 Database Security Threats

Database security threat includes the misuse, damage and intrusion of not just the database management systems, but also the data within the database and the applications that accesses it. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a database via a malicious SQL statement. This gives them access to the sensitive information contained in the database.

A (DDoS) denial-of-service attack is where cybercriminals prevent a computer system from fulfilling legitimate requests by overwhelming the networks and servers with traffic. This renders the system unusable, preventing an organization from carrying out vital functions.

Below is the list of indicative threats related to DOS & DDOS attacks.

- Unauthorized port scanning.
- Dramatic increase in the number of spam emails received.
- Dramatic increase in the number of TCP, UDP traffic to Prism's network
- Unusually large number of connection requests from unknown regions.
- TCP Fragmentation Attack
- Incoming traffic exceeds the average rate of traffic.
- System CPU usage shooting high.
- Alert from load balancers, IPS, firewall.
- Unusually slow network performance (Opening files or accessing company's web sites)
- Unavailability of a particular web site / Application
- Long term denial of access to the web or any Internet services.

8.2.1 Incident Response and Containment

Step 1: Block the source IP address performing continuous aggressive port scanning.
Step 2: In the firewall or IPS, enable feature to block Smurf attack, SYN attack,
Step 3: Adding the filters at ISP level which can detect and stop the illegitimate before it clogs the relatively small line leading to the web servers firewall.
Step 4: Contact ISP. ISP and hosting providers might provide mitigation services. Be aware of the service-level agreement provisions.
Step 5: Black holing can be used, to send all the traffic of the attacker IP address to a "black hole" (null interface or a non-existent server). To be more efficient and avoid affecting network connectivity, it can be managed by the ISP
Step 6: Redirect real traffic to a backup server on a different network using routing devices like router or firewall, while attacker will continue attacking the old server.

8.3.1 Recovery and Preventive Measures

Recovery Measures

- In the Firewall, set the limit for the number of connections that can be initiated from one source IP address.
- Filter out the bad traffic at firewall itself.
- Update all latest patches in the servers and network devices.
- Employ service screening on edge routers where possible to decrease the load on security devices such as firewalls.
- One of the most viable teardrop attack preventions is disabling 139 and 445 ports for blocking server messages in systems that aren't receiving the patches from the vendors.

Preventive Measures

- Identify and prioritize critical services that shall be maintained during an attack and turn off or block the resources which are not needed to limit the effects of the attack.
- Close unnecessary services on the targeted system.
- Ensure that critical systems have sufficient capacity to withstand an attack.
- Keep network diagrams, IT infrastructure details and asset inventories current and available to help understand the environment. Have a baseline of the daily volume, type, and performance of network traffic
- Harden the configuration settings of the network, operating systems and applications by disabling unnecessary services and applications
- Separate or compartmentalize critical services, including public and private services; intranet, extranet, and Internet services; and create single-purpose servers for services such as HTTP, FTP, and DNS
- Simple attacks could be prevented by adding simple rule in firewall to deny all incoming traffic from the attackers, based on protocols, ports or the originating IP addresses
- Implement a reliable firewall system that filters unwanted data. Implement a reliable firewall system that filters unwanted data.
- In the Firewall/IPS, enable SQL Injection, Buffer Overflow attack protection for the web server.

8.4 Malware Attack

In this scenario, the objective of the adversary is to infect the network with specific malware and its variants to enable backdoor access to the network and system, steal sensitive information, generate unwanted traffic from internal network segment and clog the corporate network, collect system information like system processes, passwords and send to C2C servers, perform zombie activities for the adversary, use end points as platform for launching attacks etc..

8.4.1 Threat Events

Indicative list of security threat events that are related to Malware attacks

- Sudden increase in the TCP or UDP or DNS traffic in the network segment.
- Web proxy logs with file downloads from the internet with file names using key words such as download manager, cleaner, etc., (if logs are enabled in Proxy Server Logs)
- Multiple Malware alert from AV or end point security solutions.
- Detection of removable media (USB) connections on servers and end points, followed by changes to registry files or execution of autorun files, etc.
- Malware intrusion alert from IPS. Refer to the list of malware indicators with mapping to various types of malware.

8.4.2 Incident Response and Containment

Step 1: Identify the users, Network segments and end points that are infected.
Step 2: Isolate the network segments to a quarantined VLAN.
Step 3: Block the connection of the infected segments to any of file servers/ shared drives/network locations.
Step 4: List down the behaviour of the malware, mode of propagation, variants list.
Step 5: Identify the ports used by the malware for propagation.
Step 6: Based on the IOC for the malware, configure rules in internal interface of IPS and Firewalls to block the internal traffic related to the malware infected network segments.
Step 7: In case of critical web facing information systems malware infection, apply IPS configuration

to block traffic on the port used by malware to propagate

Step 8: Redirect the traffic to same server in DR site.

Step 9: If feasible, disconnect the endpoint system from the internet, malware could try to call C&C via Internet connection. Disconnecting from the Internet should be one of the important things to do in order to battle any form of malware.

Step 10: Check with the OEM vendor for the signatures for the malware, if not available collect the malware infected files and submit it for malware analysis.

Step 11: If still malware cleaning is not successful, handover to external investigation team for further malware analysis and response

8.4.3 Recovery and Preventive Measures

Ensure the anti-malware software is updated with latest signatures to detect and clean the malware. If required download the additional malware cleaner installers released by the OEM vendor.

- Clean Up temporary files and worthless programs.
- Run a full scan of the system.
- Change the system account Passwords, one should change the passwords of the infected systems to ensure that no information that was potentially obtained while the computer was infected can be continued to be used and cause the harm further.
- If malware cleaning is not successful, Boot in Safe Mode or with a Live Antivirus Rescue Disk Booting in Safe Mode will prevent any non-core components from running, allowing isolating problems. If system won't start at all, one can use an antivirus rescue disk. Repeat steps 2- 5. (In case of unsuccessful malware cleaning, format the system with a new hardened image)
- In case of the infected systems include servers, then restore the data from the backup systems and test the backup recovery data.
- Take approval from the asset owner for the completeness of the restored data.
- Upon approval, move the server back to production.
- Move the cleaned systems back to production and observe the behaviour of the systems against the malware and its variants related IOC

8.5 Advanced Persistent Threats

The primary function of APT cyber security is to penetrate the perimeter security systems of your organization so that they can access internal resources. An unauthorized person gains access to a network and stays there undetected for a long period of time.

8.5.1 Threat Events

Below is the indicative list of security threat events that are related to such attacks -

- High number of DNS requests occurring from a particular IP address compared to baseline
- High number of same-sized DNS requests from an internal host, patterns of same-sized DNS request - This could be found from the firewall that is placed between the internal segment and DNS server.
- Traffic with same periodicity - e.g. traffic to the same URL at the same interval every day
- Traffic to sites listed as 'none' or 'unknown' by a reputation service or category filter
- Traffic to or from blacklisted (internal list, threat intelligence sources) addresses/domains
- Unsupervised downloads, uploads or lateral movements of files are observed.

8.5.2 Incident Response and Containment

Step 1: Using Advanced Security Analytics solutions, analyses the network logs, web proxy logs, Firewalls for the systems sending abnormal traffics (malware beaconing)
Step 2: Identify the users and end points that might be infected by the APT and sending/receiving abnormal traffic
Step 3: Identify and list the systems and network segments that have been sending the abnormal traffic.
Step 4: Apply firewall configuration to block traffic used by APT to propagate.
Step 5: Identify the suspicious files, process, services and ports used by the APT.
Step 6: Check the log files of perimeter systems to determine ports that are unusually busy. If any traffic is happening through malicious ports, block it accordingly.
Step 7: Disconnect the end point system from the internet, malware could try to call C2C via Internet connection. Disconnecting from the Internet should be one of the important things to do in order to battle any form of malware.
Step 8: Capture the memory dump using forensic tools/Advanced end point protection software.
Step 9: Capture traffic between the systems for further examination, including malware analysis, decrypting packets, decompiling and examining contents, when required
Step 10: Notify external and forensic investigation team to do detailed malware analysis of the evidences captured.
Step 11: In case of critical or high web facing information, systems are infected by APT,
Step 12: Immediately observe the outward traffic and find whether the destination is a blacklisted IP address or regions.
Step 13: Apply firewall configuration to block traffic on the port used by malware to propagate

8.5.3 Recovery and Preventive Measures

The recovery actions for an APT will take various facades based on the multiple attack vectors involved in the attack. In general, recovery and prevention measure shall include the following:

- Use application whitelisting techniques to detect and prevent unauthorized change attempts on key applications.
- Use database activity monitoring tools to detect unauthorized access attempts
- Keep a close watch on sensitive data types using data loss prevention tool
- Configure Intrusion Detection systems and Mail Gateways to block traffic from fraudulent phishing websites domains.
- Configure the web proxies and Firewall for blacklisting the phishing websites or URL

9. Breach Communication, Notification and Investigation

Throughout the cyber security crisis management stages, it is essential that appropriate teams / stake holders shall be notified. This involves communicating to business heads and management levels about the impact and progress of the crisis response.

Department Heads will ensure to follow the procedures laid down for the crisis communication strategy mentioned in 'Cyber Crisis Management Plan'

Secretarial Department shall be responsible for communication with external stakeholders such as media, investors, necessary regulatory bodies etc. as required, basis the information received from Information Security/IT Team.

9.1.1 External and Forensic Investigation

Based on the extent of damage and the threat's prevalence, external or forensic investigation might be sought to identify the root cause. Prior to initiating the investigation, the approvals from Information Security Team and respective stakeholder/s needs to be sought –

- Capture the evidences at the time of the Crisis
- Maintain the Chain of Custody for all the digital evidence.
- Information Team (IT) personnel to act as the single point of contact for the investigation agency.

9.1.2 Law Enforcement

Cyber Crime Investigation Cell will support in responding and investigating cyber-attacks and CERT-In to be contacted for taking legal actions against the cyber criminals.

10. Annexure 1

Names of Identified IT Security Officers

IT Security Officers	Division	Location	Email	Contact no
Tapovardhan Singh	Cement	Satna	tapovardhan.singh@prismjohnson	9584693844
Sutanu Ganguly	HRJ	Mumbai	ganguly.sutanu@hrjohnsonindia.com	9594090254
Shymsunder Iyer	RMC	Mumbai	shyam.iyer@rmcindia.com	8879321181
Sutanu Ganguly	Corporate	Mumbai	ganguly.sutanu@hrjohnsonindia.com	9594090254

Escalation Matrix

While isolated incidents may be resolved with minimal involvement from outside the initial response team, some incidents may require escalation to notify appropriate entities, to obtain investigative assistance.
Escalation may be undertaken by the Security Officers /Incident Response Team as the case indicates. For escalation write to compliance@prismjohnson.in.

Policy Revision

This policy will be periodically reviewed in order to ensure its continued adequacy and relevance. It may be amended at any time with the approval of the Chief Financial Officer (CFO) of the Company.

Policy Endorsement

The CFO is responsible for reviewing and overseeing the implementation of the policy.