Pioneer Online

Best Practices - Cyber Security (Organization Level)

- Implement Application Whitelisting to ensure only approved application can be executed on user machines. This will be able to prevent attackers from running malware and executing malicious code on a system. Ransom ware attacks by sophisticated cyber threat actors and cyber fraud attacks can be prevented (or made difficult) with this solution.

- Enforce Multi-Factor Authentication (MFA) to prevent phishing attacks that steal email credentials. In case MS Office 365 is being used, MFA should be enabled. MFA should also be enabled for Windows logins, which would be effective against brute force attacks particularly using Remote Desk Protocol (RDP)

- Enable Network segregation (partitioning of a network to keep critical parts of the infrastructure away from the internet end from less secure internal networks) to contain malicious activity and prevent successful propagation of the malware. This can prevent direct attacks on system that should not be internet facing. Effective monitoring of log-ins and auditing of sensitive data can be put in place to ensure that the data is tracked.

- Install anti-phishing software that can run on the mail server and examine emails for any hyperlinks containing phishing websites/ malwares. This can prevent credential loss and malicious code execution through phishing.

- Ensure Patch Management (software running on the network is patched and up-to-date) is done on regular basis especially on servers where unpatched remote desktop software if present could lead to cyber-attacks. Else remove unused or unpatched software from computers, particularly remote desktop software. Close ports that need not be connected to the internet.

- Enforce password policy in the organization to ensure that a minimum strength of password is complied with across the network. This would help in preventing brute force attacks and from attackers taking advantage of default passwords.

- Periodical audit of IT systems.

- Legacy computers (particiilar1y internet facing servers) to be taken off so as to reduce
  Attack surface.

- Educate staff on phishing attacks and email compromise frauds.

- Use Firewall Access Control Lists to restrict direct network access to user machines so Only approved devices are allowed to connect to them.

- Perform regular backups to allow quick restoration of impacted devices. Ensure backups
  Are kept offline and make sure there is a recovery plan in place
  .

- To secure the web application, regular Vulnerability Assessment and Penetration Testing (VPAT) of the entire ICT systems from competent auditors and testers, may be carried out.

Remedial measures in case the system is compromised

- Disconnect the infect computers from LAN/ Internet immediately.
- Remove unused or unpatched software from computers, particularly remote desktop software, if any.
- Change passwords of all emails and online services from another secure computer.
- Hard disks of the infected computers may be formatted after taking backup of data files.
- Operating systems and applications should be re-installed from clean software.
- Backup data should be scanned for virus before restoring it.