Organization Level Security Controls

1. 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).

2. Enable **network segregation** (partitioning of a network to keep critical parts of the infrastructure away from the internet and from less secure internal networks) to contain malicious activity and prevent successful propagation of the malware. This can prevent direct attacks on systems 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.

3. 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.

4. 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.

5. 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.

6. Periodical **audit of IT systems** to be carried out.

7. **Legacy computers** (particularly internet facing servers) to be taken off so as to reduce attack surface.

8. **Educate staff** on phishing attacks and email Compromise frauds.

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

10. 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.

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