Cybersecurity checklist for IT admins

As cyberattacks continue to evolve and grow more complicate over time, companies are tasked with a great deal of challenges to protect their online infrastructure. IT admins must identify vulnerabilities, remediate security issues, and enforce proactive strategies to secure their online infrastructure. This checklist comprises of six key areas an IT admin must focus on to implement a strong cybersecurity strategy at work.

1. Enforce network security and protect infrastructure from online threats
2. Enforce a strong endpoint security strategy
3. Secure applications, software, and data
4. Manage identities and enforce authentication
5. Secure and manage BYO devices
6. Plan and prepare for all contingencies

Enforce network security and protect infrastructure from online threats	Checkbox
1. Ensure your corporate Wi-Fi network is accessible to employees only	☑
2. Segment your network and enforce separate access credentials	☐
3. Mandate VPN for secure access to corporate networks	☐
4. Adopt commercial-grade firewall and anti-virus tools	☐
5. Perform regular scans on your network to identify and remediate potential vulnerabilities	☐
6. Enforce web-filtering policies to block access to unauthorized websites	☐
7. Automatically scan emails for malware or phishing attacks	☐
8. Maintain records of the network data usage incurred by software & apps on company devices	☐

Cybersecurity checklist for IT admins

Enforce a strong endpoint security strategy	Checkbox
1. Enforce a strong password policy	☐
2. Enforce restrictions and security configurations on endpoints to minimize gaps in security	☐
3. Enforce auto-lock policies on devices after a specified period of inactivity	☐
4. Automate OS updates and patches	☐
5. Maintain tools to perform remote operations (lockdown, data wipe, password reset, shutdown/restart, etc.) on company devices	☐
6. Adopt tools to monitor the key metrics (health, network status, battery level, etc.) of company devices and proactively resolve issues	☐

Secure applications, software, and data	Checkbox
1. Limit the installation of apps and software to just the known and approved ones	☐
2. Enforce encryption on both data-at-rest and data-in-transit	☐
3. Review permissions for installed apps and software and revoke any unauthorized permissions	☐
4. Adopt a secure file-sharing solution and block all other unapproved file sharing options	☐
5. Perform data backups on regular timely intervals	☐

Manage identities and enforce authentication	Checkbox
1. Maintain a directory with details of users, devices, and groups in a company	☐
2. Implement well-defined access control policies for users and devices	☐
3. Adopt the principle of least administrative privileges when assigning access	☐
4. Perform regular audits to identify and delete unauthorized privileges	☐
5. Enforce secure authentication using MFA and SSO	☐

Cybersecurity checklist for IT admins

6. Verify elements like user location, timing, frequency of requests, and more, before granting users access to the network	☐
7. Maintain detailed logs of user access to corporate infrastructure	☐

Secure and manage BYO devices	Checkbox
1. Enforce BYOD security policies on personal devices	☐
2. Block work apps and software from sharing data with personal apps	☐
3. Containerize data on personal devices	☐
4. Enforce tools to enable admins to remotely wipe the work container on personal devices	☐

Plan and prepare for all contingencies	Checkbox
1. Conduct routine security awareness training for employees	☐
2. Test on the training with mock drills and exercises to ensure it is being followed	☐
3. Perform penetration tests to discover and resolve potential vulnerabilities	☐
4. Have an incident management and response plan ready	☐
5. Perform regular audits on incident response plans and update relevant strategies	☐