10 Things Small Business Leaders Should Confirm their IT Team Does

Here are ten information security best practices from Dave Christiansen, CISSP and Managing Director of Ezentria:

1. Limit the number of Privileged Accounts you have for administrative purposes
2. Use a Central User Repository or Directory Service (Active Directory) to manage identity information and credentials
3. Enforce your Password Policy (change passwords every 90 days, 30 days for privileged accounts)
4. Avoid shared logins - admins should have two accounts (privileged and standard user)
5. Automate screensaver locking (configured in Active Directory as a group policy, also limit password attempts)
6. Use a Change Control process to monitor and approve changes in your environment
7. Conduct continuous vulnerability scanning to identify the devices on your network that need attention
8. If you use multiple software products, ensure that regular vulnerability scans are conducted on your devices
9. Providing security awareness training for your employees helps minimize the risk of phishing events (30% is common, training can lower to 2%)
10. Conduct a WiFi or Network Assessment to check for security issues within your network