1. Focus on your accounts

Reduce the number of domain and enterprise administrator accounts. For both administrators and users you should restrict access rights to the minimum needed to perform work. Administrators should use standard user accounts for regular daily activity (such as email or utilizing Microsoft Office apps)

Utilize a password policy to require complex passwords for all users. If there is a suspected compromise, immediately reset all account passwords.

Two-factor authentication is highly recommended for securing accounts, especially when it comes to external-facing accounts or when working with highly confidential systems/networks.

Validate all new email accounts, particularly those which can be accessed externally. Utilize email scanning with anti-virus protection.

2. Work with your access controls

CERT says you should "Prevent external communication of all versions of SMB and related protocols at the network boundary by blocking TCP ports 139 and 445 with related UDP port 137. See the NCCIC/US-CERT publication on SMB Security Best Practices for more information."

Configure firewalls to block the web-based distributed authoring and versioning (WebDAV) protocol from coming in or going out of the network.Separate critical networks or systems on different segments away from day-to-day business systems - especially user workstations. Only permit necessary traffic and block all else.

Utilize application or application directory whitelisting to permit only authorized programs or programs to run only from specific locations. Also consider the implementation of controls which prevent unauthorized code execution.

SEE: Information security policy (Tech Pro Research)

3. Take control of your logging and alerting

Get staff assigned to comprehensive logging duties which encompass the entire environment. Ensure system logs for critical systems are stored in a centralized location for at least a year.

Monitor for and identify the deletion of log files, unauthorized administrator accounts, unauthorized or unusual internal access, unauthorized applications, downloads from sites without domain names, unusual firewall activity, activities conducted by privileged accounts, access to known bad external systems, and privilege escalations or role changes.

Implement application logging where possible, including that PowerShell (version 5 required for this feature).

4. Ensure your documentation is top-notch

All networks and systems should be thoroughly documented and kept up to date, as this helps in responding to security incidents. The documentation should include network diagrams, identify assets by type as well as owner. Build an incident response plan and review it regularly.

5. Work the loose ends

Controls are important, but user education can be equally critical. Develop training plans to guide users on proper activities and how to spot threats such as phishing emails. A notification system to alert administrators of suspicious activity is also important.

Finally, review public information on a routine basis to make sure nothing confidential has been inadvertently disclosed.