CRITICAL SECURITY CONTROLS CHECKLIST

Cyber crime is a significant threat, leading to downtime, costly data breaches, loss of reputation and more. Protect your business with these 18 critical controls created by the Center for Internet Security (CIS).

□ 1. Inventory Control of Endpoints
Inventory, track and correct all endpoints connected to your network. That includes computers, mobile devices, IoT, servers, including those in the cloud.

□ 2. Inventory Control of Software
Inventory, track and correct all software on your network, including operating systems and applications. Ensure that unmanaged software cannot be installed or executed.

□ 3. Control and Protect Data
Develop processes and technical controls for your data, including how to identify, classify, secure, handle, retain and dispose of data.

□ 4. Secure Your Configuration
Establish and maintain your own configurations for all endpoints and software. Default configurations are geared for ease of use, not security.

□ 5. Account Management
Develop processes to assign and manage authorization and user credentials for all assets and software, including administrator accounts and service accounts.

□ 6. Access Control Management
Beyond the management of accounts (above) is managing the tasks and privileges foreach and every user. You need a process to create, assign, manage and revoke.

□ 7. Continuous Vulnerability Management
Develop a plan to continuously assess for and track vulnerabilities on all your endpoints and software in order to fix or minimize opportunities for attackers.

□ 8. Audit Log Management
You need to log every event that could help you detect, understand or recover from an attack. This process defines how you collect and retain that data and send alerts.

□ 9. Email and Browser Protection
Improve your ability to detect and protect users from email and web-based attacks that are used to manipulate human behavior (social engineering attacks).

□ 10. Malware Defense
Note this doesn't say "antivirus software." That's because modern malware defense involves so much more, including detecting and responding to threats.

□ 11. Data Recovery
Establish and maintain a data backup and disaster recovery (BDR) plan that can quickly restore data and assets from before an incident or cyber attack.

□ 12. Network Infrastructure Management
Similar to controlling your endpoints, you need to track, report and correct network services and access points.

□ 13. Network Monitoring and Defense
Establish processes and tools (then use them) to monitor and defend your network against security threats.

□ 14. Security Awareness and Skills Training
Create and maintain an ongoing training program (not one and done) to influence end user behavior and reduce risk.

□ 15. Service Provider Management
Evaluate your vendors to see who has access to sensitive data or are responsible for IT platforms and make sure they are protecting them appropriately.

□ 16. Application Software Security
This applies to in-house developed, hosted or acquired software. Prevent, detect and fix weakness before they can be exploited.

□ 17. Incident Response Management
Establish and maintain a process to prepare, detect and quickly respond to attacks (policies, roles, training, etc.).

□ 18. Penetration Testing
Simulate cyber attacks to test the effectiveness of your cyber security processes and resilience of your assets.

P S M
TECHNOLOGY | TALENT

Need cyber help? Visit PSMPARTNERS.COM to learn more about how we can improve your cyber maturity.

ⓘ Ask us about our *free* network assessment