

CHECKLIST #21

CYBER SECURITY THREAT ASSESSMENT

SECURITY CHECKLIST	Yes	No
PHYSICAL SECURITY		
1. Is your computing area and equipment physically secured?		
2. Are there procedures in place to prevent terminals from being left in a logged-on state, however briefly?		
3. Are screens automatically locked after 10 minutes idle?		
4. Are modems set to Auto-Answer OFF (not to accept incoming calls)?		
5. Are your PCs inaccessible to unauthorized users (e.g., located away from public areas)?		
6. Does your staff wear ID badges?		
7. Do you check the credentials of external contractors?		
8. Do you have procedures for protecting data during equipment repairs?		
9. Is waste paper binned or shredded?		
10. Do you have procedures for disposing of waste material?		
11. Do your policies for disposing of old computer equipment protect against loss of data (e.g., by reading old disks and hard drives)?		
12. Do you have policies covering laptop security (e.g., cable lock or secure storage)?		
ACCOUNT AND PASSWORD MANAGEMENT		
13. Do you ensure that only authorized personnel have access to your computers?		
14. Do you require and enforce appropriate passwords?		
15. Are your passwords secure (not easy to guess, regularly changed, no use of temporary or default passwords)?		
16. Are your computers set up so that staff entering passwords cannot be viewed by others?		
CONFIDENTIALITY OF SENSITIVE DATA		
17. Are you exercising responsibility to protect sensitive data under your control?		
18. Is your most valuable or sensitive data encrypted?		
DISASTER RECOVERY		
19. Do you have a current business continuity plan?		
SECURITY AWARENESS AND EDUCATION		
20. Are you providing information about computer security to your staff?		
21. Are employees taught to be alert to possible security breaches?		