

CHECKLIST #22

CYBER SECURITY CHECKLIST

IMPACT SCALE	LIKELIHOOD SCALE
0 Impact is negligible	0 Unlikely to occur
1 Effect is minor; major agency operations are not affected.	1 Likely to occur less than once per year
2 Agency operations are unavailable for a certain amount of time, costs are incurred, public/customer confidence is minimally affected.	2 Likely to occur once per year
3 Significant loss of operations; significant impact on public/customer confidence.	3 Likely to occur once per month
4 Effect is disastrous; systems are down for an extended period of time; systems need to be rebuilt and data replaced.	4 Likely to occur once per week
5 Effect is catastrophic; critical systems are offline for an extended period; data are lost, irreparably corrupted; public health and safety are affected.	5 Likely to occur daily

THREATS	IMPACT (0-5)	LIKELIHOOD (0-5)	TOTAL (IMPACT X LIKELIHOOD)
<b>GENERAL THREATS</b>			
Human error:			
1. Accidental destruction, modification, disclosure, or incorrect classification of information.			
2. Ignorance: Inadequate security awareness, lack of security guidelines, lack of proper documentation, lack of knowledge.			
3. Workload: Too many or too few system administrators; highly pressured users.			
4. Users may inadvertently give information on security weaknesses to attackers.			
5. Incorrect system configuration.			
6. Security policy not adequate or not enforced.			
<b>SABOTAGE</b>			
1. Dishonesty: Fraud, theft, embezzlement, selling of confidential agency information.			
2. Attacks by "social engineering":			
<ul style="list-style-type: none"> <li>• Attackers may use telephone to impersonate employees to persuade users/administrators to give username/passwords/modem numbers, etc.</li> <li>• Attackers may persuade users to execute Trojan horse programs.</li> </ul>			
3. Abuse of privileges/trust.			
4. Unauthorized use of "open" terminals/PCs.			
5. Mixing of test and production data or environments.			
6. Introduction of unauthorized software or hardware.			
7. Time bombs: Software programmed to damage a system on a certain date.			

THREATS	IMPACT (0-5)	LIKELIHOOD (0-5)	TOTAL (IMPACT X LIKELIHOOD)
8. Operating system design errors: Certain systems were not designed to be highly secure.			
9. Protocol design errors: Certain protocols were not designed to be highly secure. Protocol weaknesses in TCP/IP can result in: <ul style="list-style-type: none"> <li>• Source routing, DNS spoofing, TCP sequence guessing, unauthorized access.</li> <li>• Hijacked sessions and authentication session/transaction replay; data is changed or copied during transmission.</li> <li>• Denial of service, due to ICMP bombing, TCP_SYN flooding, large PING packets, etc.</li> </ul>			
10. Logic bomb: Software programmed to damage a system under certain conditions.			
11. Viruses in programs, documents, e-mail attachments.			
<b>IDENTIFICATION/AUTHORIZATION THREATS</b>			
1. Attack programs masquerading as normal programs (Trojan horses).			
2. Attack hardware masquerading as normal commercial hardware.			
3. External attackers masquerading as valid users or customers.			
4. Internal attackers masquerading as valid users or customers.			
5. Attackers masquerading as helpdesk/support personnel.			
<b>RELIABILITY OF SERVICE THREATS</b>			
1. Major natural disasters: fire, smoke, water, earthquake, storms/ hurricanes/tornadoes, power cuts, etc.			
2. Minor natural disasters, of short duration, or causing little damage.			
3. Major human-caused disasters: war, terrorist incidents, bombs, civil disturbance, dangerous chemicals, radiological accidents, etc.			
4. Equipment failure from defective hardware, cabling, or communications system.			
5. Equipment failure from airborne dust, electromagnetic interference, or static electricity.			
6. Denial of service: <ul style="list-style-type: none"> <li>• Network abuse: Misuse of routing protocols to confuse and mislead systems.</li> <li>• Server overloading (processes, swap space, memory, "tmp" directories, overloading services).</li> <li>• E-mail bombing.</li> <li>• Downloading or receipt of malicious Applets, ActiveX controls, macros, Postscript files, etc.</li> </ul>			

THREATS	IMPACT (0-5)	LIKELIHOOD (0-5)	TOTAL (IMPACT X LIKELIHOOD)
<p>7. Sabotage: Malicious, deliberate damage of information or information processing functions.</p> <ul style="list-style-type: none"> <li>• Physical destruction of network interface devices, cables.</li> <li>• Physical destruction of computing devices or media.</li> <li>• Destruction of electronic devices and media by electromagnetic radiation weapons (HERF Gun, EMP/T Gun).</li> <li>• Theft.</li> <li>• Deliberate electrical overloads or shutting off electrical power.</li> <li>• Viruses and/or worms.</li> <li>• Deletion of critical system files.</li> </ul>			
<b>PRIVACY THREATS</b>			
<p>1. Eavesdropping:</p> <ul style="list-style-type: none"> <li>• Electromagnetic eavesdropping/Van Eck radiation.</li> <li>• Telephone/fax eavesdropping (via "clip-on," telephone bugs, inductive sensors, or hacking the public telephone exchanges).</li> <li>• Network eavesdropping: Unauthorized monitoring of sensitive data crossing the internal network, unknown to the data owner.</li> <li>• Network eavesdropping: Unauthorized monitoring of sensitive data crossing the Internet, unknown to the data owner.</li> <li>• Subversion of DNS to redirect e-mail or other traffic.</li> <li>• Subversion of routing protocols to redirect e-mail or other traffic.</li> <li>• Radio signal eavesdropping.</li> <li>• Rubbish eavesdropping (analyzing waste for confidential documents, etc.).</li> </ul>			
<b>INTEGRITY/ACCURACY THREATS</b>			
1. Malicious, deliberate damage of information or information processing functions from external sources.			
2. Malicious, deliberate damage of information or information processing functions from internal sources.			
3. Deliberate modification of information.			
<b>ACCESS CONTROL THREATS</b>			
1. Password cracking (access to password files, use of bad (blank, default, rarely changed) passwords).			
2. External access to password files, and sniffing of the network.			
3. Attack programs allowing external access to systems (back doors visible to external networks).			
4. Attack programs allowing internal access to systems (back doors visible to internal networks).			
5. Unsecured maintenance modes, developer backdoors.			
6. Modems easily connected, allowing uncontrollable extension of the internal network.			
7. Bugs in network software which can open unknown/ unexpected security holes. (Holes can be exploited from external networks to gain access. This threat grows as software becomes increasingly complex.)			
8. Unauthorized physical access to system.			

THREATS	IMPACT (0-5)	LIKELIHOOD (0-5)	TOTAL (IMPACT X LIKELIHOOD)
<b>REPUDIATION THREATS</b>			
1. Receivers of confidential information may refuse to acknowledge receipt.			
2. Senders of confidential information may refuse to acknowledge source.			
<b>LEGAL THREATS</b>			
1. Failure to comply with regulatory or legal requirements (e.g., to protect confidentiality of employee data).			
2. Liability for acts of internal users or attackers who abuse the system to perpetrate unlawful acts (e.g., incitement to racism, gambling, money laundering, distribution of pornographic or violent material).			
3. Liability for damages if an internal user attacks other sites.			