Chapter 5
Office Systems and Technology
Key Terms

1.	Acceptance test	D
2.	Antivirus program	J
3.	Biometric control	N
4.	Conversion	P
5.	Cracker	R
6.	Data tampering	X
7.	Database administrator	Z
8.	Denial of service	B
9.	Digital certificate	K
10.	Digital signature	U
11.	Digital wallet	CC
12.	Encryption	F
13.	Fault-tolerate system	L
14.	Firewall	T
15.	Hacker	Y
16.	Help desk	BB
17.	Hot site	EE
18.	Information center	FF
19.	Information policy	G
20.	Network engineer	O
21.	Programmer	S
22.	Security protocol	W
23.	Spam	AA
24.	Steering committee	DD
25.	Systems analyst	A
26.	Systems audit	I
27.	Systems life-cycle	E
28.	Technology support group	H
29.	Trojan horse	M
30.	Virus	Q
31.	Web designer	V
32.	Webmaster	C

A. The liaison between information technicians and business users who translates business requirements and problems into information technology requirements; often considered change agents within the organization. **(25) Systems analyst**

B. Attacks where crackers flood a network or Web server with information requests in an attempt to crash the network. **(8) Denial of service**

C. Information technology employee who monitors and maintains Web servers. **(32) Webmaster**

D. The final systems test where users evaluate the entire system and indicate how well it meets the standards established at the beginning of the design or purchase of the system. **(1) Acceptance test**

E. A dynamic process that requires interaction with personnel at all levels within the organization for analysis, design, development, implementation, and operation and maintenance of the organization's computer-based information system. **(27) Systems life-cycle**

F. Coded messages requiring the receiver to have an authorized decryption key to read the message; one-key, two-key, and a hybrid system. **(12)Encryption**

G. Guidelines often posted on the organization's intranet for easy access and updates regarding the use, distribution, and security of information for the entire organization; formation is typically the responsibility of the Chief Information Officer with input from all organizational levels. **(19)Information policy**

H. Individuals proficient with productivity software and technology who are identified to provide assistance to other end users within the organization. **(28)Technology support group**

I. Comprehensive audits on the computer-based information system to determine the effectiveness of all the security controls; includes external audits, internal audits, and data audits. **(26) Systems audit**

J. A software program on the organization's network, as well as desktop PCs, notebooks, and workstations, to detect and delete computer viruses. **(2) Antivirus program**

K. An attachment to an electronic document that verifies the sender to be whom he/she claims. **(9) Digital certificate**

L. An information system designed with duplicate hardware, software, and power supply so processing will continue during a system failure; important for mission critical operations. **(13) Fault-tolerate system**

M. A destructive program that masquerades as a benign application; does not replicate. **(29) Trojan Horse**

N. A security control that identifies an individual based on physiological or behavioral characteristics; (i.e. iris, fingerprints, signature, and keystrokes) **(3) Biometric control**

O. An information technology position typically staffed by an electrical engineer with a specialization in networks who can address the information technology infrastructure-hardware, software, data storage, and networks. **(20) Network engineer**

P. The process of changing from the old system to a new one; methods include direct, parallel, phased, and pilot. **(4) Conversion**

Q. A rogue software program that spreads throughout the network disrupting processing and memory operations and possibly destroying data; thousands exist, and approximately 50 new ones are created each month. **(30) Virus**

R. A malicious hacker with the intent of disabling the computer system for a profit. **(5) Cracker**

S. Technical specialists who write and maintain software instructions (code) for the computer; specialize in system software. **(21) Programmer**

T. System that consists of software and hardware placed between the organization's internal network(s) and an external, unsecured network to ensure that only authorized personal have access to the organization's private network; also recommended for a traveling professional's notebook. **(14)Firewall**

U. A digital code attached to a document to identify the sender and message contents; to be legally binding, someone must verify that it belongs to the person who sent the data and that the data were not altered. **(10) Digital signature**

V. One who possesses the technical and aesthetic skills for developing Web sites. **(31) Web designer**

W. Standards for providing a secure information technology environment. **(22) Security protocol**

X. Intentionally or unintentionally entering incorrect or fabricated data or changing or deleting existing data stored in the organization's files and databases; typically done by organization insiders. **(6) Data tampering**

Y. A person who gains unauthorized access to a computer network for mischief. **(15) Hacker**

Z. The information technology person responsible for the logical database design, development of the data dictionary, security of the data, and monitoring how others use data. **(7) Database administrator**

AA. Unsolicited junk e-mail that interferes with work and can slow down the network to the point where efficient business communication and operations are affected by consuming valuable network bandwidth. **(23) Spam**

BB. A support station staffed by an information technology specialist where end users can call, e-mail, or drip in to receive both hardware and software assistance; sometimes technology assistance is available 24/7. **(16) Help desk**

CC. Software that stores credit card and owner identification to be used for e-commerce purchases. **(11) Digital waller**

DD. A committee that focuses on policies for the use of the information system, priorities for system development, budgets for information technology, system security, system maintenance, and system issues;. **(24) Steering committee**

EE. An external location that contains a fully configured backup data center; includes all required hardware and software for a computer-based information system **(17) Hot site**

FF. A unit staffed with technology specialists responsible for supporting end users in using hardware and software, maintaining hardware and software, providing technology workshops and seminars, and recommending new purchases for the user's area of specialty. **(18) Information center**