



173
*must-know
Cyber terms*

THE ABCs OF CYBER RISK

2012

The ABCs of Cyber Risk: 2012 is a Cyber Glossary compiled by ExecutivePerils, published by Advisen and made available to the entire Advisen Community. We invite you to comment and/or add Cyber words to this ongoing project by contacting editors@advisen.com

APage 2

BPage 2

CPage 3

DPage 6

EPage 6

FPage 8

GPage 8

HPage 8

IPage 9

KPage 10

LPage 10

MPage 11

NPage 11

OPage 12

PPage 12

QPage 14

RPage 14

SPage 15

TPage 17

UPage 18

VPage 18

WPage 19

XYZPage 19



Adware - Software installed on a computer for the sole purpose of producing advertisements as pop-ups or banner displays to generate revenue for the advertiser.

AIS - Automated Information System - any equipment of an interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, control, display, transmission, or reception of data and includes software, firmware, and hardware.

Alderson Loop - A special kind of infinite loop that traps the user by using a false exit condition, i.e., “click OK” when the “OK” function has been disabled.

Ankle-Biter - A person who aspires to be a hacker/cracker but has very limited knowledge or skills related to AIS's. Usually associated with young teens that collect and use simple malicious programs obtained from the Internet.

Anomaly Detection Model - A model where intrusions are detected by looking for activity that is different from a user's or system's normal behavior.

Anonymous - An on-line hackers group suspected as the party responsible for the massive Sony breaches in May 2011, which Anonymous denies. It has admitted responsibility for the system breaches at MasterCard and Visa following the Wiki leaks disclosures. The group slogan is “We Are Legion.”

ASIM - Automated Security Incident Measurement - Monitors network traffic and collects information on targeted unit networks by detecting unauthorized network activity.

Attacker Traps - Systems used to lure hackers or other information warriors into an attack so that they can be traced.



Back door - Also, Trapdoor. An intentional breach in the security of a computer system left in place by designers or maintainers. A hidden software or hardware mechanism used to circumvent security controls. A breach created intentionally for the purpose of collecting, altering or destroying data.”

Bastion Host - A system that has been hardened to resist attack at some critical point of entry, and which is installed on a network in such a way that it is expected to come under attack. Bastion hosts are often components of firewalls, or may be ‘outside” Web servers or public access systems. Generally, a bastion host is running some form of general purpose operating system (e.g., LINUX, VMS, WNT, etc.) rather than a ROM-based or firmware operating system.

BLOB - Binary Large Object. Can be stored in a database but normally not interpretable by a database program. Occasionally used as a mild hacker threat when mailed. Can also be used to hide malicious logic code.

Blog - From the term “web log,” a type of website, usually in reverse chronological order, maintained by an individual with regular entries. Unlike a static website, most blogs are interactive, allowing visitors to post comments.

Blue bomb (a.k.a. “the blue screen of death” or “WinNuke”) - Technique for causing the Windows operating system of someone you are communicating with to crash or suddenly terminate. The “blue bomb” contains information that the operating system can’t process. This condition causes the operating system to “crash” or terminate prematurely. Its name comes from the effect it sometimes causes on the display as the operating system is terminating – a white-on-blue error screen.

Bomb - A generic description for the crashing of software or hardware systems.

Botnet - A collection of software designed to forward transmissions (including spam and viruses) from one computer to another without the owner’s knowledge or consent. The computer is referred to as a “zombie” or “robot” (hence, “bot”) because it automatically follows instructions from the originator of the virus or spam. Typically a botnet gains access through an inadequate firewall. Computers in the “zombie army” may be directed to submit multiple transmissions to overwhelm and prevent access to a particular website, sometimes a competitor.

Breach -

1. The successful defeat of security, which could result in system penetration.
2. Violation of a system’s controls that exposes information assets or system components.

“Brute force” password cracker - Guessing the password until you get it either manually or automated by using a program that continually guesses passwords. Programs will try passwords like aa, ab, ac and so on until every legal character combination has been tried.

Browser - A software application used to view and interact with the web.



C2 - Stands for Command and Control. The arrangement and deployment of personnel, equipment, communications, facilities, and procedures employed in accomplishing a mission.

C2W - Stands for Command-and-Control Warfare. In addition to the traditional physical destruction aspect of war, this includes the integrated use of operations security, military deception, psychological operations and electronic warfare to degrade or destroy the adversary’s command and control capabilities.

CIAC - Computer Incident Advisory Capability -- Plans for establishing this team were prepared before November 1988. It was founded as a second incident response team in the Spring of 1989. Its constituencies are sites within the DOE.

CIAO - Critical Infrastructure Assurance Office. Created in May 1998 to assist in the coordination of the U.S. Federal Government's initiatives on critical infrastructure protection.

CIRT - "Computer Incident Response Team" Refers to an organization's procedures for handling a cyber attack. The team should be responsible for designing preventative measures, detecting the attack, preserving critical data and communicating with the public and law enforcement. Also known as Computer Security Incident Response Team (CSIRT).

Cloud Computing - "The data has left the building." Service delivery model characterized by delivery over the internet (the cloud); resources such as software and platforms are provided and payment is based on demand, like gas or electric utilities. Servers are located off-premises in a "server farm" and may be shared by several companies. Owners of the data lease server space away from its own location and outsource IT and server maintenance to save capital expenditures.

Command and Control Warfare (C2W) - The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction to destroy an enemy's command and control capabilities and to protect one's own. It is a subset of information warfare.

Communications Security (COMSEC) - Measures taken to deny unauthorized persons information derived from telecommunications of an entity concerning national or organizational security, and to ensure the authenticity of such telecommunications. Communications security includes crypto security, transmission security, emission security, and physical security of communications security material and information.

Computer system - Computer hardware, software, networks, networking equipment, applications, associated electronic devices, electronic data storage devices, input and output devices, and back up facilities operated by and either owned by or leased to the Insured by written contract for such purposes.

Conduit Injury - Injury sustained or allegedly sustained by a Person because a System cannot be used, or is impaired, resulting directly from:

- A. A Cyber-attack into an Insured's System, provided such Cyber-attack was then received into a third party's System; or
- B. A natural person who has accessed a System without authorization, through an Insured's System, provided such transmission or access occurred on or after the Retroactive Date and before the end of the Policy Period.

Cookies - Code which is transferred to an internet user's computer when visiting a web site. A type of message given to a web browser by a web server and then stored in the computer's hard drive. Cookies are used to save log-in information and create a personalized website that reads, for example, "welcome back Jack" when the website is next opened. Local shared objects, also known as "flash cookies" store more information and are not listed among the cookies stored on a hard drive. Many users are unaware of flash cookies or mistakenly believe they have been deleted. Several class action lawsuits charge media and technology companies with using flash cookies to create consumer profiles without their knowledge.

Copernicus - The codename under which the Navy reformulated its command and control structures in the age of Information Warfare. Copernicus enables those in the field to get the information they need to make tactical decisions.

COPPA - “Child Online Privacy Protection Act” Enacted in 1998, this federal legislation is intended to protect children under 13 years of age. The act places responsibilities on websites and online services operated for commercial purposes to protect children’s privacy and safety online. Many websites disallow underage children from using their services due to the amount of paperwork involved.

Core Leak - A programming error that causes the program to fail to reclaim discarded memory, leading to eventual collapse due to memory exhaustion. Not as critical a problem as it was before the advent of virtual memory.

Cracker - Like a hacker, it is someone who breaks into secure systems. A cracker’s primary aim is to break into secure systems, while hackers want to gain knowledge about computer systems and use this knowledge for pranks or to cause damage. Typically, the terms hack and crack are often used interchangeably.

Crimeware - A class of malware designed specifically to automate cyber crime. It is distinguished from adware, spyware and malware because it is designed to perpetuate identity theft in order to illegally access and use another’s online accounts. Crimeware includes stealing passwords, installing a keystroke logger to track confidential information or redirecting a web browser to a counterfeit website.

CSRC - Computer Security Response Center. Another acronym for CERTs.

Cyber Activities - The electronic display, electronic transmission, or electronic dissemination of information through a Network or through an Insured’s System.

Cyber Liability - Third-party coverage for liability arising from the failure of an insured to prevent unauthorized use or access of its network; transmission of a computer virus to a third party; theft of confidential information; or denial-of-service.

Cyber War - Actions taken to achieve information superiority over an adversary – to deny, exploit, corrupt or destroy an enemy’s information while protecting you own. See Information Warfare.

Cyberian Winter - The theoretical aftermath of an all-out Cyber War, characterized by “cold” disabled computer systems and businesses.

Cybersquatting - Use of trademarks belonging to others in registering a domain name (a web site’s address on the web).

Cyberstalking (Cyberbullying) - Repeatedly sending message that include threats of harm or are highly intimidating; engaging in other online activities that make a person afraid for his or her safety.



Daemon - Pronounced demon or damon, a process that runs in the background and performs a specified operation at predefined times or in response to certain events. Sometimes referred to as System Agents and services. Typical daemon processes include print spoolers, e-mail handlers, and other programs that perform administrative tasks for the operating system. The term comes from Greek mythology, where daemons were guardian spirits.

Dark-side Hacker - A malicious hacker.

Data - A representation of information, knowledge, facts, concepts, or instructions which are being processed or have been processed in a Computer.

Denial of Service - Action preventing an information system from functioning in accordance with its intended purpose, i.e. flooding a system to prevent it from servicing normal and legitimate requests. Denial of Service attacks make computer resources unavailable to users. The two most common DOS attacks are those that crash the system and those that saturate the target with so many communications it cannot respond. If an attacker mounts an attack from a single host, it is a DOS attack. If the attacker uses multiple systems to cripple another system, it is a Distributed Denial of Service (DDOS) attack. In December 2010, unidentified individuals in support of WikiLeaks' disclosure of confidential U.S. government documents initiated DDOS attacks on two credit card companies who refused donations to WikiLeaks, resulting in 30 lost internet hours for the credit card companies. Two days later, WikiLeaks' own site was the subject of a DDOS attack.

Denigration (Cyberbullying) - "Dissing" someone online. Sending or posting cruel gossip or rumors about a person to damage his or her reputation or friendships.

Dumpster diving - Spying the old-fashioned way: rummaging through garbage or recycling cans for information such as invoices, passwords, and account numbers.



Easter Egg - An undocumented function hidden in a program that may or may not be sanctioned by management. Easter Eggs are secret "goodies" found by word of mouth or accident. See Trapdoor.

ECHELON - A multi-national surveillance network centered at Sugar Grove, WV. It has been called the greatest spy network in history. Echelon intercepts all forms of electronic communications – phone, fax and e-mail – and automatically searches for pre-determined keywords. Member countries are the United States, Britain, Australia and New Zealand.

E-Communications Loss - Loss resulting directly from a Customer, automated clearing house, custodian, or financial institution having transferred, paid or delivered any funds or property, established any credit, debited any account or given any value on the faith of any fraudulent Communication purporting to have been directed by an Insured to any of the foregoing for the purpose of initiating, authorizing or acknowledging the transfer, payment, delivery or receipt of funds or property, but which Communication was either not sent by an Insured or was fraudulently modified during electronic transmission and for which loss an Insured is held to be legally liable.

E-mail Bombs - Code that when executed sends many messages to the same address(s) for the purpose of using up disk space and/or overloading the E-mail or web server.

EMP/T Bomb - Electromagnetic pulse transformer, which disables or destroys an electronic network. Similar to a HERF Gun but many times more powerful.

Encryption - Conversion of data into a form called “ciphertext” that cannot be easily understood by unauthorized users. In order to recover the contents of an encrypted signal, the correct decryption key is required. Modern cryptography is based on the use of algorithms to scramble or encrypt the original message (plain text) into unintelligible data (ciphertext). Some governments view strong encryption as a potential vehicle by which terrorist could function. These governments propose a key-escrow agreement in which those who use a cipher would be required to provide the government with a copy of the decryption key.

Encryption Cracking - Breaking the encryption that is used to protect the contents of e-mail, fax and voice transmissions, as well as software or other content.

Ethernet Sniffing - This is listening with software to the Ethernet interface for packets that interest the user. When the software sees a packet that fits certain criteria, it logs it to a file. The most common criteria for an interesting packet is one that contains words like login or password.

ExecutivePerils - National wholesaler specializing in Cyber/Privacy insurance. Wrote one of the first Cyber policies in the industry and often quoted in publications on cyber/privacy issues.

Exclusion (Cyberbullying) - Intentionally excluding someone from an online group, like a “buddy list” or a game.

Extranet - Limited access to a company’s intranet given to other companies or the public.

F

FACTA - “Fair and Accurate Credit Transaction Act” Enacted in 2003, this federal legislation is intended to protect consumers from identity theft. Among its provisions, the Act permits consumers to receive a free credit report annually and requires devices that print credit card numbers to truncate the number to the last four digits.

Firewall - A form of web security that stands between a private network and the Internet to prevent unwanted traffic from passing either way. Some firewalls have proxy functions built in. Often the distinction between a firewall and a proxy is blurry. True firewalls generally support packet-filtering, proprietary application filtering, and some proxy functions.

Fishbowl - To contain, isolate and monitor an unauthorized user to gain information about that user.

Flaming (Cyberbullying) - Online fights using electronic messages with angry and vulgar language.

Flooding programs - Code which when executed will bombard the selected system with requests in an effort to slow down or shut down the system.

Fork bomb - A disruptive piece of code directed toward a Unix-based system which replicates, or “forks,” until it eventually “explodes” and devours operating system processes causing the system to lock up.

Framing - Using hyperlinks to use another party's web site content to display one's own advertising.

G

GLBA - “Graham-Leach-Bliley Act” (Financial Services Modernization Act of 1999) repealed a 1933 law that barred the consolidation of financial institutions and insurance companies. Included within GLBA are multiple sections relating to the privacy of financial information. Companies must provide written notice to consumers of their privacy rights and explain the company's procedures for safeguarding data.

H

Hackers - Persons who use computer skills to trespass, uninvited, into another's computer system and compromises computer security or gaining unauthorized access to a computer file or system. They penetrate information systems; to browse, steal, or modify data; deny access or service to others; or cause damage or harm in some other way. To some, hackers are different from “crackers” who infiltrate computer systems for criminal purposes only.

Hacking Run - An extended hack session that goes beyond normal working times, especially if more than 12 hours long.

Harassment (Cyberbullying)- Repeatedly sending offensive, rude and insulting messages.

HERF Gun - High Energy Radio Frequency gun. They shoot a high power radio signal at an electronic target and knock it out of commission.

Hijacking - Where an active, established session is intercepted and co-opted by an unauthorized user.

HIPAA - “Health Insurance and Portability and Accountability Act” Enacted in 1996, the Act regulates the use and disclosure of certain health-related information held by “covered entities,” which include health plans, health care clearinghouses (i.e. billing services) and health care providers. HIPAA requires, among other things that covered entities notify individuals of the uses of their PHI; monitor disclosures of PHI; document privacy policies and procedures; and appoint a privacy official and contact person to receive complaints regarding privacy breaches. The HIPAA requirements were significantly expanded by HITECH.

HITECH - “Health Information Technology for Economic and Clinical Health Act” Enacted in 2009, this federal law requires physicians and medical facilities to adopt electronic health records. The Act also expands HIPAA privacy laws: medical providers must notify each patient of security breaches within 60 days and notify the federal government and social media if more than 500 patients are involved. Criminal and civil penalties up to \$1.5 million are possible.

Honeypot - A decoy server set up either inside or outside a firewall to lure and trick an intruder. It is designed to make hackers/crackers think they are on a valid production system. It is used to catch and stop an intruder or detect and track intruder techniques and test system vulnerability.

HTTP - Hyperlink transfer protocol, which allows words, graphics, video and sound to be transmitted via the web.



Impersonation (Cyberbullying) - Breaking into someone’s account, posing as that person and sending messages to make the person look bad, get that person in trouble or danger, or damage that person’s reputation or friendships.

Information Security Liability – Refers to liabilities that result from breaches of an electronic network.

Information Warfare - Abbreviated IW. Also known as third-wave war or knowledge war. Actions taken to achieve information superiority over an adversary – to deny, exploit, corrupt or destroy an enemy’s information while protecting you own. See cyber war.

INFOSEC - Military abbreviation for Information Security. The protection of classified information that is stored on computers or transmitted by radio, telephone tele-type, or any other means.

Internet - A group of connected networks that allow access to an Insured's System through service providers using telephone service, digital subscriber lines, integrated service digital network lines, cable modem access or similar transfer mediums. It is a three-level hierarchy composed of backbone networks, mid-level networks and stub networks, which includes many different physical networks worldwide.

Intranet - An internal TCP-IP network used for sharing information within an organization; not necessarily connected to the internet.

IP Sniffing - Stealing network addresses by reading the packets. Harmful data is then sent stamped with internal trusted addresses.

IP Spoofing - An attack whereby an active, established, session is intercepted and co-opted by the attacker.

ISPs - Internet service providers – companies providing access to the internet.

ITERA - "Identity Theft Enforcement and Restitution Act." Enacted in 2008, ITERA lowers the threshold for prosecutors to bring criminal charges for unauthorized access to a computer and provides for restitution to the victim "equal to the value of the time reasonably spent by the victim in an attempt to remediate the intended or actual harm incurred by the victim from the offense."

K

Key - A symbol or sequence of symbols (or the electrical or mechanical equivalent) applied to text to encrypt or decrypt.

Keystroke Monitoring - A device or software that records every key struck by a user and every character of the response that the user gets.

Kluge - A programming trick designed to solve a problem quickly, although why could remain a mystery. A classic "Rube Goldberg."

L

Leapfrog attack - An attack in which the hacker gains access to a site or server from a third party site. Use of user ID and password information obtained illicitly from one host to compromise another host. The act of TELNETing through one or more hosts in order to preclude a trace (a standard cracker procedure).

Letter bomb - E-mail containing live data intended to do malicious things to a machine or terminal.

Linking - Process by which a web site user clicks on a “link” (an icon, or underlined/highlighted text) and is transferred to another web page.

Logic bomb - A piece of unauthorized computer code, usually delivered via e-mail. It attacks a system after verifying certain conditions within that system.



Mailbomb - Sent to urge others to send massive amounts of e-mail to a single system with a goal of crashing the recipient's system.

Malicious Code - Any unauthorized, corrupting, or harmful virus, Trojan Horse, worm, logic bomb or other similar software program, code or script designed to insert itself onto a computer disk or into computer memory and migrate from one computer to another.

Malware - Abbreviated for “malicious software” it is designed to secretly access a computer system without the owner's consent and steal data for illegal purposes. Malware includes computer viruses, Trojan horses, crimeware, rootkits and worms.

Metatags - Hidden code embedded into web pages that enable search engines to quickly gather information about the pages.

MIPS - Stands for Million Instructions Per Second. A measure of computing speed.

Mockingbird - A computer program that mimics the legitimate behavior of a normal system feature, but launches into a malicious activity once activated by the user.



Nano Machines - Tiny robots that attack the hardware of a computer system, as opposed to the software. These robots (smaller than insects) can literally crawl through an office after being unleashed at a facility until they find a computer, then drop through slots in the computer and shut down the electronic circuits.

Network - The hardware and/or software making up a data communications system. Any and all services provided by or through the facilities of any electronic or computer communication system, including Fedwire, Clearing House Interbank Payment System (CHIPS), Society for Worldwide Interbank Financial Telecommunication (SWIFT) and similar automated interbank communication systems, automated teller machines, point of sale terminals, and other similar operating systems and includes any shared networks, **Internet** access facilities, or other similar facilities for such systems, in which an **Insured** participates, allowing the input, output, examination, or transfer of **Data** or programs from one computer to an **Insured's Computer**.

Network breach -

1. The alleged or actual unauthorized access to a computer system that results in:
2. The destruction, deletion or corruption of electronic data on a computer system; a data breach from a computer system; and denial of service attacks against Internet sites or computers; and
3. Transmission of malicious code from a computer system to third party computers and systems

Network Worm - A program or command file that uses a computer network as a means for adversely affecting a system's integrity, reliability or availability. A network worm may attack from one system to another by establishing a network connection. It is usually a self-contained program that does not need to attach itself to a host file to infiltrate network after network.

NIPC - National Infrastructure Protection Center. Established in February 1998, the NIPC is considered the U.S. government's focal point for threat assessment, warning, investigation, and response for threats or attacks against critical national infrastructures.



One-Time Password - In network security, a password issued only once as a result of a challenge-response authentication process. Cannot be "stolen" or reused for unauthorized access.

One-way hash function - In cryptography, an algorithm that generates a fixed string of numbers from a text message. The "one-way" means that is extremely difficult to turn the fixed string back into the text message. One-way hash functions are used for creating digital signatures for message authentication.

OODALoop - Observation, Orientation, Decision, Action Loop. Refers to the computerized cycle from data acquisition to information integration through to initiation of a response. Taking out the OODA loop is frequently mentioned as the goal of Information Warfare.

Outing and trickery (Cyberbullying) - Sharing someone's secrets or embarrassing information online. Tricking someone into revealing secrets or embarrassing information, which is then shared online.



Packet sniffing - A technique in which a software program is planted at remote junctions in a computer network. The program monitors information packets as they are sent through networks and reveals user names and passwords to the hacker, who is then able to break into the system.

PCIDSS - "Payment Card Industry Data Security System." A set of policies and standards for securing credit and debit cards information. It was created jointly in mid-2004 by four credit card companies (American Express, Visa, MasterCard and Discover). It addresses security requirements such as firewalls, encryption and anti-virus software.

PHI - "Protected Health Information" Information concerning the health status, provision of health care or payment for health care that can be linked to any individual; typically interpreted broadly to include any part of an individual's medical history or health-related payment history.

Phishing - Criminally fraudulent attempt to acquire sensitive personal information such as user names, passwords and credit card data by masquerading as a trustworthy site. It often originates as an email directing a person to click on the link to a fraudulent website that appears genuine and instructs the person to enter sensitive data by "verifying an account." "Ph" is a common substitute for the letter "f" among hackers (e.g. "phone phreaking"). Phishing should not be confused with Phish, an American band.

Phreaking - Hacking directed at the telephone system (as opposed to the data communications networks). Hacking with a telephone. Using different "boxes" and "tricks" to manipulate the phone companies and their phones, you gain many things, two of which are: knowledge about telephones and how they work, and free local and long distance phone calls.

PII - "Personally identifiable Information" Unique information that establishes an individual identity such as date of birth, social security or national identification number, race, gender, etc.

Ping of Death - The Ping of Death is a denial-of-service attack that crashes servers by sending invalid IP ping packets.

Point of Sale System - A system mostly used in restaurants and hotels in which a computer replaces a cash register. Besides recording transactions, a POS accepts credit and debit card data, usually with a bar code, tracks inventory and records employee hours.

Port Scanning - The act of systematically scanning a computer's ports. Since a port is a place where information goes into and out of a computer, port scanning identifies open doors to a computer. Port scanning has legitimate uses in managing networks, but port scanning also can be malicious in nature if someone is looking for a weakened access point.

Portal - Web site providing an entrance to the web usually by offering a search engine or useful links.

Privacy Liability - Incurred by a company when its computer system is breached by a third party or past, or present employee, as a consequence, personally identifiable information is released to unauthorized persons.

Privacy notification costs - Reasonable and Necessary:

1. Costs to hire a security expert to determine the existence and cause of any theft or unauthorized access to or disclosure of personally identifiable information,
2. Costs to notify consumers under a breach notification law, and
3. Fees incurred to determine the actions necessary to comply with a breach notification law.

Prowler - A daemon that is run periodically to seek out and erase core files, truncate admin log files, “nuke” lost & found directories and other wise clean up the system.

Proxy - Using one computer or device to make requests or to “stand in” in place of another. Proxies are often used for Internet security. You can use a proxy to pass data between an internal network and the Internet. The server on the Internet never knows that the request is coming from anywhere but the proxy. Some proxies have caching and site filtering built in.

Public Key - Method of encryption that uses a closed combination key that encrypts messages and an open combination key that decrypts the messages.



Quadrant - A short name referring to technology that provides tamper-resistant protection to cryptography equipment.



Ransomware - A form of malware in which an unauthorized user inserts a computer virus to encrypt data and then demands money for the decryption key in order to restore the data, a type of “cyber extortion.” Some ransomware locks the user’s keyboard and leaves a mobile phone number for the user to call to unlock the keyboard, for a fee.

Record - A natural person’s first name or first initial, and last name, in combination with:

- A. Their social security number, driver’s license number or other personal identification number (including an employee identification number or student identification number);
- B. Their financial account number (including a bank account number, retirement account number, or healthcare spending account number);
- C. Their credit, debit or payment card number;
- D. Any information related to their employment by an **Insured Organization**; or
- E. Any individually identifiable health information, pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), held by an **Insured Organization**.

Red Flag Rule - Effective in June 2010, this legislation requires all businesses who accept credit to have a written policy that addresses how it will prevent and handle identity theft. “Red flags” include tampered photo ids, unverified addresses. The law imposes fines of \$3,500 per violation. The legislation was modified in December 2010 to exempt physicians, lawyers and other professional service providers.

Regulatory Fine - Any civil fine or civil monetary penalty imposed in a regulatory proceeding payable by the Insured to the government entity bringing such regulatory proceeding in such entity’s regulatory or official capacity.

Regulatory Proceeding - A request for information, civil investigative demand, suit, civil investigation, or civil proceeding commenced by the service of a complaint or similar pleading by or on behalf of any local, state, federal or foreign governmental entity in such entity’s regulatory or official capacity which may reasonably be expected to give rise to a claim covered by this policy.

Rootkits - A form of malware in which an unauthorized program that tracks data is undetected because it subverts normal authentication and authorization systems. Some rootkits are installed intentionally, e.g. to prevent copying copyrighted materials on CDs.



Samurai - A hacker who hires out for legal cracking jobs, snooping for factions in corporate political fights, lawyers pursuing privacy-rights and First Amendment cases, and other parties with legitimate reasons to need an electronic locksmith.

Script Kiddie - A low-level amateurish hacker. They are generally regarded as mischief-makers as opposed to real threats.

Secure Electronic Transaction (SET) - A new standard that enables secure credit card transactions on the Internet. SET has been endorsed by virtually all the major players in the electronic commerce arena.

Secure Sockets Layer (SSL) - A protocol from Netscape that allows for “secure” passage of data. It uses public key encryption, including digital certificates and digital signatures, to pass data between a browser and a server. It is an open standard and is supported by Netscape’s Navigator and Microsoft’s Internet Explorer.

Self-Garbling Viruses - Viruses which attempt to hide from virus scanning programs by keeping most of their code garbled in some way. They change the garbling each time they spread. When such a virus runs, a small header de-garbles the body of the virus and then branches to it.

Skimming - The use of a counterfeit device that takes credit or debit card data including the magnetic “swipe” tape that contains credit or debit data. ATM skimming occurs when thieves create a fraudulent facade that fits over the ATM screen which is indistinguishable from the real ATM machine. When a debit card is inserted, the data may be accessed remotely. A small camera placed over the keypad copies pin numbers. An estimated \$350,000 per day is skimmed from ATMs worldwide.

SMiShing - A combination of phishing and SMS. SMiShing uses cell phone text messages to deliver a message with a hyperlink or a phone number to call which when completed may either download a Trojan horse or entice the recipient to provide personal information which is the used by the criminal party.

Smurf - A type of network security breach in which a network connected to the Internet is swamped with replies to ICMP echo (PING) requests. A smurf attacker sends PING requests to an Internet broadcast address.

Sneaker - A person hired to break into a system to test its security.

Sniffer - A program and/or device that monitors data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information off a network. Unauthorized sniffers can be extremely dangerous to a network’s security because they are virtually impossible to detect and can be inserted almost anywhere. This makes them a favorite weapon of hackers.

Solar Sunrise - A 1998 series of attacks that targeted Defense Department network domain name servers, to exploit the vulnerability in the Solaris Operating System computers that operated there. The attacks were thought to be a “reconnaissance” for a widespread attack on the entire Pentagon information infrastructure.

Spear Phishing - Unlike phishing which sends emails to a random group of people, spear phishing targets a select group of people with something in common, such as the same employer or bank or college. The targets are sent emails that appear to be from the genuine organization seeking personal information. Often the targets are asked to click on a link that takes them to another site that looks genuine. A phishing email is addressed “Dear customer” whereas a spear phishing email is addressed “Dear your name.” The recent Epsilon breach raises the likelihood of spear phishing.

Spoofing -

1. Faking the sending address of a transmission to make it look like it is coming from a trusted host or address in order to gain illegal entry into a secure system.
2. A generic label for activities in which trusted relationships or protocols are exploited. Impersonating, masquerading, and mimicking are forms of spoofing.

Spyware - A type of software that can be installed in computers to collect small pieces of information without the owner's knowledge. In addition to monitoring information, it can track websites visited, change computer settings to slow the computer's function or block internet access. It is seen most often on personal computers and to create a marketing profile. Microsoft's Internet Explorer is the browser most vulnerable to spyware in part because it is the most widely used and because of its tight integration with Windows.

SQL Injection - Malicious software consisting of an insertion or "injection" of a SQL (standard query language) from an unauthorized source, typically seen with database-driven web sites. Databases enable web applications to store and sort data. The web uses a "string query" to extract data from the database. The string query consists of the query and any parameters, for example, the user retrieves a product name and price by entering the product ID number. A SQL Injection inserts commands inside the parameters so the data retrieved from the database is not what the user requested. In the example above, if the word "delete" is inserted before "product ID number" then the server will delete the products ID table. SQL Injections are one of the most common forms of web attacks.

Stateful Inspection - Also referred to as dynamic packet filtering. A firewall architecture that works at the network layer. Stateful inspection checks both the header information and contents of the packet. As an added security measure against port scanning, stateful inspection firewalls close off ports until connection to the specific port is requested.

Stealth Viruses - Viruses that attempt to hide from detection programs by hiding their presence in boot records or files. When such viruses are run, they install a resident extension. This resident extension intercepts various disk accesses, determines if its own code is part of the disk access, and removes the code before giving the data to the calling program. The result is that the virus can be in several places on the disk. Normal reads of the disk will not reveal it.



TCP/IP - The data transmission standard used on the internet, which uses transmission control protocol and internet protocol.

Tempest - U.S. government code word for a program launched in the 1950's to reduce the chances of electromagnetic radiation "leakage" from devices used to process, transmit, or store sensitive information. It was believed that such leakage could pose a security threat.

Tentacle - An artificial identity created in cyberspace for malicious and deceptive purposes. The implication is that a single person may have multiple tentacles.

Tiger Team - A team of "sneakers" whose purpose is to penetrate and test security measures.

Trapdoor - A secret way of gaining access to a program or online service. See Easter Egg, Backdoor, Back Orifice and one-way hash function.

Trojan Horse - A program containing additional, hidden code that causes it to launch unauthorized functions, including possible data destruction.

Trolling (Cyberbullying) - Intentionally posting provocative messages about sensitive subjects to create conflict, upset people, and bait them into “flaming” or fighting.

Turn Commands - Commands inserted to forward mail to another address for interception.



Unauthorized Access - The use of or access to a computer system by a person unauthorized by the Insured to do so or the authorized use of or access to a computer system in a manner not authorized by the Insured.
Uniform Resource Locator (URL) - the full internet address of an internet file.

User Identification - User identification is the process by which a user identifies himself to the system as a valid user. (As opposed to authentication, which is the process of establishing that the user is indeed that user and has a right to use the system).



van Eck monitoring - Monitoring the activity of a computer or other electronic equipment by detecting low levels of electromagnetic emissions from the device. Named for Dr. Wim van Eck.

Venona Project - A secret cryptology project launched at the height of World War Two (February, 1943) by the forerunner to the National Security Agency. It was designed to examine and possibly exploit encrypted Soviet diplomatic communications, and is considered a tremendous success.

Virtual Private Networks (VPN) - Networks that are essentially private, but use the internet in lieu of expensive leased phone lines between offices.

Virus - A self-replicating code segment. Viruses may or may not contain attack programs or trapdoors.

Virus - A program that can infect other programs by modifying them.

VPN - “Virtual Private Network” A computer network that uses the internet to provide secure access to a private network by remote users. Its purpose is to avoid expensive leased lines or dial-up phone lines. VPN uses cryptographic “tunneling” protocols to provide confidentiality. Amazon’s EC2 offers VPN to link users to its cloud computing.

Vulnerability - This term refers to any weakness in any system (either hardware or software) that allows intruders to gain unauthorized access or deny service.



Wardriving - Act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer or PDA. Wardriving is used to hack into business networks and retrieve credit card information.

Warkitting - A combination of wardriving and rootkitting. In a warkitting attack, a hacker replaces the firmware of an attacked router. This allows them to control all traffic for the victim, and could even permit them to disable SSL by replacing HTML content as it is being downloaded.

Wiki - A collaborative website that allows anyone to edit, add or delete contents, in contrast to a blog which permits readers' comments but only allows the author to change the contents. The first wiki was developed in 1995. A common misconception is that Wiki is an acronym for "what I know is." The term "wiki" means "quick" in Hawaiian.

Worm - A program that replicates from machine to machine across network connections, often-clogging networks and information systems as it spreads.

Web Bug - A graphic on a Web page or in an e-mail message that monitors who is reading the Web page or e-mail message. Web bugs are often invisible because they are typically only 1- by-1 pixel in size. They are represented as HTML IMG tags. They are invisible to hide the fact that the monitoring is taking place.

Worm - An independent program that reproduces by copying itself in full-blown fashion from one computer to another, usually over a network. Unlike a virus, it usually doesn't modify other programs.

WinNuke - Technique for causing the Windows operating system of someone you are communicating with to crash or suddenly terminate. See "blue bomb."



Zombie - A computer that has been implanted with a daemon that puts it under the control of a malicious hacker or organization without the knowledge of the computer owner. Zombies are used by malicious hackers to launch DoS attacks. The hacker sends commands to the zombie through an open port. On command, the zombie computer sends an enormous amount of packets of useless information to a targeted Web site in order to clog the site's routers and keep legitimate users from gaining access to the site. The traffic sent to the Web site is confusing and therefore the computer receiving the data spends time and resources trying to understand the influx of data that has been transmitted by the zombies.

About **ExecutivePerils**

ExecutivePerils is an independent 100% wholesale insurance broker whose sole purpose is to bring product expertise, underwriter relationships, innovation and excellent service to our retail clients across the country in the desire to make them more successful. We focus on a limited number of insurance products. This allows us to develop a true understanding of the insurance marketplace, each carriers' unique policy and appetite as well as the legislative and judicial environments. This approach also facilitates developing deep relationships with the underwriters and claims personnel. We are active in meeting the needs of Insureds when securing coverage as well as adding value when there is a claim. Our products are: crime, D&O liability, employment practices liability (EPL), errors and omissions (E&O), fiduciary liability, general partnership and real estate investment trust liability, insuring agents E&O, media E&O, intellectual property insurance, kidnap/ransom and extortion, legal malpractice, and technology/digital/privacy insurance. We have been recognized as 2010 PowerBroker® nominee, 2011 Risk Innovator recipient and 2012 Power Broker® recipient. We introduced Super Continuity during the 2008 financial crises, Trilateral Coverage that changed the way D&O tail/run off is placed and in the mid 1990's was one of the first to write a cyber-liability policy and helped a major carrier write their cyber policy. Learn more at www.eperils.com or call us at 310.444.9333

About

Advisen generates, integrates, analyses and communicates unbiased, real-time insights for the global community of commercial insurance professionals. As a single source solution, Advisen helps the insurance industry to more productively drive mission critical decisions about pricing, loss experience, underwriting, marketing, transacting or purchasing commercial insurance. Advisen's data, analytics and news services are game-changers for more than 125,000 professionals.

For Cyber Liability, Advisen offers

- Insurance Program pricing data
- Loss insight data
- Cyber Policy Form wordings
- Front Page News Cyber edition email newsletter
- Cyber Liability journal, a quarterly edition
- Cyber Liability Insights Conference series

Visit us at www.advisen.com or contact support@advisen.com to learn more