# Cyber Terms Glossary

## Following are common cyber terms and their definitions.

### Advanced Persistent Threat (APT)
Usually refers an advanced type of cyber attack characterized by multiple integrated methods of increasing sophistication sufficient to permeate any perimeter defence. Also used to refer to groups who carry out this sophisticated style of attacks such as, but no longer limited to a foreign government. Characteristic of APT attackers is the capability and the intent to persistently and effectively target a specific entity. The term is often used to refer to Internet-enabled espionage using a variety of intelligence gathering techniques to access sensitive information, but is also applied to other threats such as that of traditional espionage or attack. Other recognized attack vectors include infected media, supply chain compromise, and social engineering. Individuals, such as an individual hacker, are not usually referred to as an APT as they rarely have the resources to be both advanced and persistent even if they are intent on gaining access to, or attacking, a specific target.

### Adware
A form of malware which display unwanted advertisements to the computer user, often by launching numerous pop-ads in the user's browser. Adware is frequently a form of spyware, monitoring computer activity and collecting information without the user's consent. The term adware is also used to describe legitimate free or low-cost advertising-supported software.

### Annualized Loss Expectancy (ALE)
An annually expected financial loss to an organization from a threat. Single Loss Expectancy (SLE) X Annualized Rate of Occurrence (ARO) = Annualized Loss Expectancy (ALE).

### Annualized Rate of Occurrence (ARO)
A value that represents the estimated frequency at which a threat is expected to occur. Can range from 0 up to very large numbers. For instance a cataclysmic volcano destroying the entire facility might be expected to happen once every 100,000 years and would have an ARO of 0.00001. Whereas100 employees accessing web pages that contain malicious payloads could be estimated at 5 times per year per employee and have an ARO of 500.

### Anti-Virus Software
A program that monitors a computer or network with the goal of preventing, identifying and/or removing malware.

### Asset
A resource, process, product or other tangible piece of information that an organization has decided must be protected. The loss of the asset could affect the CIA Triad overall or it could have a discrete monetary value.

### Automatic Data Processing (ADP)
The assembly of computer hardware, firmware, and software used to categorize, sort, calculate, compute, summarize, store, retrieve, control, process, and/or protect data with minimum human intervention.

### Back-up Operation
A method of operations to complete essential tasks as identified by a risk analysis. These tasks would be employed following a disruption of the MIS and continue until the MIS is acceptably restored.

### Big Data
A general term used to describe the voluminous amount of unstructured and semi-structured data a company creates – data that would take too much time and cost too much money to load into a relational database for analysis. Although big data doesn't refer to any specific quantity, the term is often used when speaking about petabytes and exabytes of data.

A primary goal for looking at big data is to discover repeatable business patterns. It's generally accepted that unstructured data, most of it located in text files, accounts for at least 80% of an organization's data. If left unmanaged, the sheer volume of unstructured data that's generated each year within an enterprise can be costly in terms of storage. Unmanaged data can also pose a liability if information cannot be located in the event of a compliance audit or lawsuit.

Big data analytics is often associated with cloud computing because the analysis of large data sets in real-time requires a framework to distribute the work among tens, hundreds or even thousands of computers.

### Black Hat
The villain or bad guy, especially in a western movie in which such a character would wear a black hat in contrast to the hero's white hat. The phrase is often used figuratively, especially in computing slang, where it refers to a hacker that breaks into networks or computers, or creates computer viruses for malicious purposes.

### Bluebugging
A form of Bluetooth attack. A Bluebug program allows the user to take control of the victim's phone. Not only can they make calls, they can send messages, essentially do anything the phone can do. This also means that the Bluebug user can simply listen to any conversation his victim is having.

### Bluejacking

Sending unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers.

### Bluesnarfing

The unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs. This allows access to a calendar, contact list, emails and text messages, and on some phones users can steal pictures and private videos.

### Botnet

A jargon term for a network of computers and software robots, or bots, that run autonomously and automatically. They run on groups of zombie computers controlled remotely. A computer can be unknowingly added to a botnet as a result of being penetrated by malware. The botnet creator or owner can then use the network for malicious activity, commonly denial of service attacks.

### CAN-SPAM Act

A law that sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to have you stop emailing them, and spells out tough penalties for violations. Despite its name, the CAN-SPAM Act doesn't apply just to bulk email. It covers all commercial messages, which the law defines as any electronic mail message with the primary purpose of commercial advertisement or promotion of a commercial product or service, including email that promotes content on commercial websites. The law makes no exception for business-to-business email. That means all email – for example, a message to former customers announcing a new product line – must comply with the law. Each separate email in violation of the CAN-SPAM Act is subject to penalties of up to $16,000.

### CERT

Acronym derived Carnegie Mellon University's (CMU) Computer Emergency Response Team. The CERT program develops and promotes the use of appropriate technology and systems management practices to resist attacks on networked systems, to limit damage, and to ensure continuity of critical services. Numerous CERTs have now been deployed worldwide to perform similar functions although not all are related to CMU.

### Cardholder Data Environment

The people, processes and technology that store, process or transmit cardholder data and sensitive authentication data, including any connected system components.

### Clear or Clearing (MIS Storage Media)

The removal of data from an information system, its storage devices, and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using common system capabilities (i.e., through the keyboard); however, the data may be reconstructed using laboratory methods.

### Click Fraud

A type of internet crime that occurs in pay per click online advertising when a person, automated script, or computer program imitates a legitimate user of a web browser clicking on an ad, for the purpose of generating a charge per click without having actual interest in the target of the ad's link. Click fraud is the subject of some controversy and increasing litigation due to the advertising networks being a key beneficiary of the fraud.

### Cloud Computing

Cloud computing is a general term for anything that involves delivering hosted computer resources over the Internet (or other large network). These services are often divided into three broad categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). The name cloud computing was inspired by the cloud symbol that's often used to represent the Internet in flowcharts and diagrams. A cloud service has three distinct characteristics that differentiate it from traditional hosting. It is sold on demand, typically by the minute or the hour; it is elastic – a user can have as much or as little of a service as they want at any given time; and can be fully managed by the provider (the consumer needs nothing but a personal computer and Internet access). Significant innovations in virtualization and distributed computing, as well as improved access to high-speed Internet and a weak economy, have accelerated interest in cloud computing.

### Commercial-Off-The-Shelf (COTS)

Products that are commercially available and can be utilized as generally marketed by the manufacturer.

### Computer Virus

A computer program that can copy itself and infect a computer without permission or knowledge of the user. The term virus is also commonly used, albeit erroneously, to refer to many different types of malware and adware programs.

### Computer Worm

A self-replicating computer program. It uses a network to send copies of itself to other computer terminals on the network and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms almost always cause harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer. Many worms have been created which are only designed to spread, and don't attempt to alter the systems they pass through. However, as the Morris worm and Mydoom showed, the network traffic and other unintended effects can often cause major disruption.

### Configuration Management (CM)

The management of changes made to MIS hardware, software, firmware, documentation, tests, test fixtures, test documentation, communications interfaces, operating procedures and installation structures throughout the development and operational life-cycle of the MIS.

### Controlled Access Protection (C2)

Minimum set of security functionality that enforces access control on individual users and makes them accountable for their actions through login procedures, auditing of security-relevant events, and resource isolation.

### Cookie

A small data file that a web site installs on your computer's hard drive to collect information about your activities on the site or to allow other capabilities on the site. Web sites use cookies to identify returning visitors and profile their preferences on the site. For example, many online shopping sites use cookies to monitor what items a particular shopper is buying to suggest similar items. Cookies are somewhat controversial as they raise questions of privacy and can be used by hackers as spyware.

### Crimeware

Computer program designed specifically to conduct illegal activity online.

### Cryptanalysis (Cryptography/Cryptology)

The mathematical science that deals with analysis of a cryptographic system (encryption and decryption) in order to gain knowledge needed to break or circumvent the protection that the system is designed to provide without knowing the key.

### Cyber

A prefix used to describe a person, thing, or idea having to do with computers, information technology or management information systems.

### Cyber Insurance

Insurance products that provide protection for risks associated with computer systems, information technology, management information systems, network security and the use and storage of sensitive or confidential data. These risks include (but are not limited to) sensitive data breaches, computer hacking, dumpster diving, computer virus and employee sabotage or pilferage of information and identity theft.

### Cyber Liabilities

The first- and third-party risks to countries, companies and individuals associated with computers, information technology, management information systems and sensitive data. These risks include (but are not limited to) sensitive data breaches, computer hacking, dumpster diving, computer virus and employee sabotage or pilferage of information and identity theft.

### Cyber Risk Management

The process of managing risks associated with computers, information technology, management information systems and sensitive data.

### Cyber Security

The body of technologies, processes and practices designed to protect computers, information technology, management information systems and sensitive data from attack, damage or unauthorized access.

### CyberEdge®

Comprehensive risk management solution for cyber insurance offered by AIG. In a rapidly changing landscape, CyberEdge provides innovative protection to help businesses safeguard against sensitive data breaches, computer hacking, dumpster diving, computer viruses, employee sabotage or error, and pilferage of information and identity theft. CyberEdge helps businesses stay ahead of the curve and provide responsive guidance based on years of experience. CyberEdge provides a valuable additional layer to companies' most powerful first lines of defence against cyber threats – their own IT systems.

### Cybercrimes

Offenses that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS).

### Cyberlaw

Rapidly evolving area of civil and criminal law applying to the use of computers and the Internet and the exchange of communications and information thereon, including related issues concerning such communications and information as the protection of intellectual property rights, freedom of speech, and public access to information.

### Cyberstalking

Using the internet to monitor or harass an individual or group of individuals. Cyberstalking often involves repeatedly sending messages that include threats of harm or are highly intimidating and engaging in other online activities that make a person fear for his or her safety.

### Data Breach

An incident involving the unauthorized access to, theft of, or disclosure of non-public information.

### Data Encryption Standard (DES)

A widely-used method of data encryption using a private (secret) key. DES is an encryption block cipher defined and endorsed by the U.S. government in 1977 as an official standard (FIPS PUB 59).

### Denial-of-Service Attack (DoS attack)

Or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to, motives for, and targets of a DoS attack may vary, it generally consists of the concerted, malevolent efforts of a person or persons to prevent legitimate users from using a networked service by crashing the service or flooding the service with illegitimate requests and/or information.

### Department of Defense (DOD) Trusted Computer System Evaluation Criteria

Created by the National Computer Security Center (NCSC), these criteria are intended for use in the design and evaluation of systems that will process and/or store sensitive data. This document contains a uniform set of basic requirements and evaluation classes used for assessing the degrees of assurance in the effectiveness of hardware and software security controls built in the design and evaluation of MIS.

### Discretionary Access Control (DAC)

A means of restricting access to objects based on the identity of subjects and/or groups to which they belong or in the possession of an authorization granting access to those objects.

### E-mail spoofing

A term used to describe fraudulent email activity in which the sender address and other parts of the email header are altered to appear as though the email originated from a different source. E-mail spoofing is a technique commonly used for spam e-mail and phishing to hide the origin of an e-mail message.

### Encryption or Enciphering

Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure.

### Exposure Factor

The percentage loss that a realized threat would have on a specific asset.

### FIPS

Acronym for Federal Information Processing Standards. Standards that are publicly recognized by the U.S. Federal Government; also for use by non- government agencies and contractors.

### False Flag Operations

Covert operations conducted by governments, corporations, or other organizations, which are designed to appear like they are being carried out by other entities.

### Firewall

A collection of components or a system that is placed between two networks and possesses the following properties: 1) all traffic from inside to outside, and vice-versa, must pass through it; 2) only authorized traffic, as defined by the local security policy, is allowed to pass through it; and 3) the system itself is immune to penetration.

### Firmware

Computer programs and data that are stored in hardware and cannot be dynamically written or modified during execution of the programs or normal device operations.

### Hacker

Common nickname for an unauthorized person (or organization) who breaks into or attempts to break into a management information system by circumventing software security safeguards.

### Hashing

Process of rendering cardholder data unreadable by converting data into a fixed-length message digest via Strong Cryptography. Hashing is a mathematical function in which a non-secret algorithm takes any arbitrary length message as input and produces a fixed length output. A hash function should have the following properties: In the context of PCI DSS, hashing must be applied to the entire PAN for the hash code to be considered rendered unreadable. It is recommended that hashed cardholder data includes a salt value as input to the hashing function.

### Identity Theft

The unauthorized assumption of a person's identity in order to misappropriate that person's money, credit or other resources. Identity theft most frequently occurs when an unauthorized person gains access to the personally identifiable information of another person to commit fraud or other crimes.

### International Cybercrime Reporting and Cooperation Act

Bipartisan legislation introduced by Senators Orrin Hatch (R-UT) and Kirsten Gillibrand (D-NY) to enhance U.S. cooperation with other countries to confront this threat.

### Intrusion Detection System (IDS)

Software or hardware used to identify and alert on network or system intrusion attempts. Composed of sensors that generate security events; a console to monitor events and alerts and control the sensors; and a central engine that records events logged by the sensors in a database. Uses system of rules to generate alerts in response to security events detected.

### Key Distribution Centre

A system that is authorized to transmit temporary session keys to principals (authorized users) in order to reduce the risks inherent in exchanging keys. Each session key is transmitted in encrypted form, using a master key that the key distribution shares with the target principal.

### Keystroke Logging

A method of capturing and recording user keystrokes. Keylogging can be useful to determine sources of errors in computer systems, to study how users interact and access with systems, and is sometimes used to measure employee productivity on certain clerical tasks. Such systems are also highly useful for law enforcement and espionage—for instance, providing a means to obtain passwords or encryption keys and thus bypassing other security measures.

### MIS Security

Measures or controls that safeguard or protect a management information system against accidental or intentional unauthorized disclosure, modification, destruction of the MIS and data, or denial of service. MIS security provides an acceptable level of risk for the MIS and the data contained in it.

### Malicious Code

Software or firmware that is intentionally included in a management information system for an unauthorized purpose.

### Malware

A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the users' data, applications, or operating system or of otherwise annoying or disrupting the user.

### Management Information System (MIS)

An assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

### Merchant

For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.

### National Institute of Standards and Technology

A unit of the U.S. Commerce Department and formerly known as the National Bureau of Standards, NIST promotes and maintains measurement standards and also encourages and assists industry and science to develop and use these standards.

### National Telecommunications and Information Systems Security Policy

Directive for Federal agencies, as of July 15, 1992, to provide automated Controlled Access Protection (C2 level) for MIS, when all users do not have the same authorization to use the sensitive information.

### Network Security and Privacy Insurance

Protection of networks and their services unauthorized modification, destruction, disclosure, and the provision of assurance that the network performs its critical functions correctly and there are no harmful side-effects. Privacy insurance offers protection for both the expenses and the legal liabilities associated with security privacy breaches.

### Nigerian 419 Fraud Scheme

A confidence fraud in which the target is persuaded to advance relatively small sums of money in the hope of realizing a much larger gain.

### Overwrite Procedure

A process, which removes or destroys data recorded on a computer storage medium by writing patterns of data over, or on top of, the data stored on the medium.

### Payment Card

For purposes of PCI DSS, any payment card/device that bears the logo of the founding members of PCI SSC, which are American Express, Discover Financial Services, JCB International, MasterCard Worldwide, or Visa.

### Payment Card Industry Data Security Standard (PCI DSS)

The global data security standard that any business of any size must adhere to in order to accept or process payment card transactions. The standard includes twelve requirements for any business that stores, processes or transmits payment cardholder data.

### Payment Card Industry Security Standards Council

The Payment Card Industry Security Standards Council, or PCI SSC is an open global forum, launched in 2006, that develops, maintains and manages the PCI Security Standards, which include the Data Security Standard (DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) Requirements. The Council works to educate stakeholders about the PCI Security Standards, operates programs to train and qualify security professionals in assessing and achieving compliance with PCI Security Standards, and promotes awareness of the need for payment data security to the public.

The Council's five founding global payment brands – American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa – have incorporated the PCI DSS as the technical requirements for their data security compliance programs. Each founding member also recognizes the practitioners and companies – Qualified Security Assessors and Approved Scanning Vendors – certified by the PCI Security Standards Council as being qualified to validate compliance to the PCI DSS, making the Council a centralized resource for access to standards and services approved by all five payment brands.

### Personally Identifiable Information (PII)

Information that can be used to identify, contact or locate a specific individual, either alone or when combined with other personal or identifying information. PII can include a person's name, address, phone numbers, social insurance number, bank account number, credit card account number, family members' names or friends' names. Finding this information is often the goal of hackers looking to steal identity or money.

### Phishing

Is an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. PayPal, eBay and online banks are common targets. Phishing is typically carried out by e-mail or instant messaging, and often directs users to enter details at a website, although phone contact has also been used.

### Piggybacking

A term used to refer to access of a wireless internet connection by bringing one's own computer within the range of another's wireless connection, and using that service without the subscriber's explicit permission or knowledge. It is a legally and ethically controversial practice, with laws that vary in jurisdictions around the world. While completely outlawed in some jurisdictions, it is permitted in others. Piggybacking is used as a means of hiding illegal activities, such as downloading child pornography or engaging in identity theft. This is one main reason for controversy.

### Pod Slurping

The act of using a portable data storage device such as an iPod digital audio player to illicitly download large quantities of confidential data by directly plugging it into a computer where the data is held, and which may be on the inside of a firewall. As these storage devices become smaller and their storage capacity becomes greater, they are becoming an increasing security risk to companies and government agencies. Access is gained while the computer is unattended.

### Protected Health Information (PHI)

Individually identifiable health information that is related to an individual's past, present or future physical or mental health or condition, the provision of health care to an individual, or the past, present or future payment for health care provided to an individual. PHI is protected under the U.S. HIPAA Privacy Rule.

### Public Law 100-235

Established minimal acceptable standards for the government in computer security and information privacy.

### Qualitative Risk Assessment

Attempts to categorize the seriousness of given threats, and in doing so the relative sensitivity of an asset is given a ranking or qualitative grading.

### Quantitative Risk Analysis

Attempts to assign independently objective numeric values (hard dollars) to the components of the risk assessment and to the assessment of potential losses.

### Residual Risk

The remaining potential risk after all IT security measures are applied. There is a residual risk associated with each threat.

### Risk Management [Risk Assessment]

The process of managing/identifying risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Note: Risk analysis is part of risk management and synonymous with risk assessment.

### Rootkit

A program designed to take fundamental control (in Unix terms root access, in Windows terms Administrator access) of a computer system, without authorization by the system's owners and legitimate managers. Access to the hardware is rarely required as a rootkit is intended to seize control of the operating system running on the hardware. Typically, rootkits act to obscure their presence on the system through subversion or evasion of standard operating system security mechanisms. Often, they are also Trojans as well, thus fooling users into believing they are safe to run on their systems. Techniques used to accomplish this can include concealing running processes from monitoring programs, or hiding files or system data from the operating system.

### SEC Cybersecurity Guidance a/k/a CF Disclosure Guidance: Topic No. 2 , Cybersecurity

In October 2011, the SEC's Division of Corporation Finance provided guidance regarding disclosure obligations relating to cybersecurity risks, cyber incidents and related insurance. Essentially, the guidance advises that although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents:

1. A number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents; and
2. Material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading.

Depending on the registrant's particular facts and circumstances, and to the extent material, appropriate disclosures may include: Discussion of aspects of the registrant's business or operations that give rise to material cybersecurity risks and the potential costs and consequences; to the extent the registrant outsources functions that have material cybersecurity risks, description of those functions and how the registrant addresses those risks; description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences; risks related to cyber incidents that may remain undetected for an extended period; and description of relevant insurance coverage.

### SQL Injection
Computer attack in which malicious code is embedded in a poorly-designed application and passed to the backend database. The malicious data then produces database query results or actions that should never have been executed.

### Safeguard
A mitigating control or countermeasure designed and employed to reduce the risks associated with a specific threat or group of threats.

### Security Requirements
Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policies.

### Security Specifications
A detailed description of the security safeguards required to protect a system.

### Security Violation
An event, which may result in disclosure of sensitive information to, unauthorized individuals, or that results in unauthorized modification or destruction of system data, loss of computer system processing capability, or loss or theft of any computer system resources.

### Service Provider
Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. Entities such as telecommunications companies that only provide communication links without access to the application layer of the communication link are excluded.

### Single Loss Expectancy
The dollar figure that is assigned to a single event. It represents the organization's loss from a single occurrence of a threat. Asset Value ($) x Exposure Factor (EF) = Single Loss Expectancy (SLE).

### Social Engineering
The art of manipulating people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery for information gathering or computer system access and in most cases the attacker never comes face-to-face with the victim.

### Software Cracking
The modification of software to remove protection methods: copy prevention, trial/demo version, serial number, hardware key, CD check or software annoyances like nag screens and adware.

### Spamming
The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, mobile phone messaging spam, Internet forum spam and junk fax transmissions.

### Spear Phishing
Targeted versions of phishing have been termed spear phishing. Several recent phishing attacks have been directed specifically at senior executives and other high profile targets within businesses, and the term whaling has been coined for these kinds of attacks.

### Spyware
Software that is secretly installed into a management information system to gather information on individuals or organizations without their knowledge; a type of malicious code.

### Standalone System
A single-user MIS not connected to any other systems.

### Standard Security Procedures
Step-by-step security instructions tailored to users and operators of MIS that process sensitive information.

### Stealware
Refers to a type of software that effectively transfers money owed to a website owner to a third party. Specifically, stealware uses an HTTP cookie to redirect the commission ordinarily earned by the site for referring users to another site.

### Symmetric Encryption
A form of cryptosystem in which encryption and decryption are performed using the same key.

### System Integrity
The attribute of a system relating to the successful and correct operation of computing resources.

### Threat
The occurrence of any event that causes an undesirable impact on the organization. Threats may be man-made or naturally occurring.

### Threat Agent
Any person or thing, which acts, or has the power to act, to cause, carry, transmit, or support a threat.

### Trojan Horse
Piece of software which appears to perform a certain action but in fact performs another such as transmitting a computer virus. Contrary to popular belief, this action, usually encoded in a hidden payload, may or may not be actually malicious, but Trojan horses are notorious today for their use in the installation of backdoor programs. Simply put, a Trojan horse is not a computer virus. Unlike such malware, it does not propagate by self-replication but relies heavily on the exploitation of an end-user (see Social Engineering).

### Trusted Computer System (TCSEC)

A system that employs sufficient hardware and software assurance measures to allow its use for processing a range of sensitive or classified information simultaneously.

### Uninterruptible Power Supply (UPS)

A system of electrical components to provide a buffer between utility power, or other power source, and a load that requires uninterrupted, precise power.

### Virus

A program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in Microsoft Office programs that allows users to generate macros.

### Vishing

Is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private personal and financial information from the public for the purpose of financial reward. The term is a combination of voice and phishing. Vishing exploits the public's trust in landline telephone services, which have traditionally terminated in physical locations which are known to the telephone company, and associated with a bill-payer. The victim is often unaware that VoIP allows for caller ID spoofing, inexpensive, complex automated systems and anonymity for the bill-payer. Vishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals.

### VoIP Spam

Proliferation of unwanted, automatically-dialed, pre-recorded phone calls using Voice over Internet Protocol (VoIP). Some pundits have taken to referring to it as SPIT (for Spam over Internet Telephony).

### Vulnerability

The absence or weakness of a safeguard or mitigating control. Vulnerabilities may have the ability to transform minor threats into greater threats or more persistent threats.

### White Hat

The hero or good guy, especially in computing slang, where it refers to an ethical hacker that focuses on securing and protecting IT systems. Such people are employed by computer security companies where these professionals are sometimes called sneakers. Groups of these people are often called tiger teams.

### Wide Area Network (WAN)

A network of Local Area Networks (LANs), which provides communication, services over a geographic area larger than served by a LAN.

### Worm

A computer worm is a program built to reproduce itself and spread across a network, rendering it ineffective. A worm may be designed to complete several different malicious activities. However, one common denominator is that a worm can harm a network by consuming large amounts of bandwidth, potentially shutting the network down. Viruses, on the other hand, are more limited to targeting computers one-at-a-time. A virus also requires other programs to execute and replicate, whereas a worm can act independently of other programs.

### Zombie Computer

Computer attached to the Internet that has been compromised by a hacker, a computer virus, or a Trojan horse. Generally, a compromised machine is only one of many in a Botnet, and will be used to perform malicious tasks of one sort or another under remote direction.

For more information on AIG's cyber coverage and services, contact us at cyberedge@aig.com.

The information, suggestions and recommendations contained herein are for general informational purposes only. This information has been compiled from sources believed to be reliable. Risk Consulting Services do not address every possible loss potential, law, rule, regulation, practice or procedure. No warranty, guarantee, or representation, either expressed or implied, is made as to the correctness or sufficiency of any such service. Reliance upon, or compliance with, any report in no way guarantees any result, including without limitation the fulfillment of your obligations under your insurance policy or as may otherwise be required by any laws, rules or regulations. No responsibility is assumed for the discovery and/or elimination of any hazards that could cause accidents, injury or damage. The information contained herein should not be construed as financial, accounting, tax or legal advice and does not create an attorney-client relationship.

AIG Insurance Company of Canada is the licensed underwriter of AIG property casualty insurance products in Canada.Coverage may not be available in all provinces and territories and is subject to actual policy language. Non-insurance products and services may be provided by independent third parties.