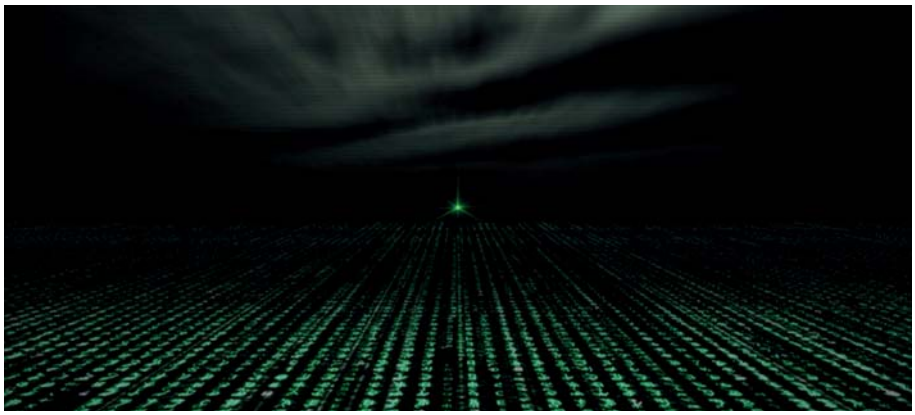
Cyber Risks

Definitions

CHUBB®



As cyber risks become an increasing part of our broker's dialogue with clients we thought it would be helpful to offer a brief guide on some of the terminology that is now associated with the cyber risk landscape. The terms and definitions below are for information purpose only and meant to provide a general description of some common cyber terms. They do not form part of Chubb's insurance policies.

If you require further assistance with the language of Cyber risks, please contact your local Chubb distribution team for assistance.

- **Applications software (also called end-user programs)** - Includes database programs, word processors, and spreadsheets. Figuratively speaking, applications software sits on top of systems software because it is unable to run without the operating system and system utilities.

- **Botnet** - A botnet refers to a network of "robot" computers that automatically transmit spam,malware or viruses without the owner's knowledge. Computers in the botnet are referred to as "Zombies" as the computers usually injected by a trojan are controlled by the botnet creator not the computer owner.

- **CERT (Computer Emergency Response Team)** - Expert teams that handle cyber security incidents. Cert Australia is the national computer emergency response team that provides advice and support on cyber threats and vulnerabilities to the owners and operators of Australia's critical infrastructure and other systems of national interest.

- **Cloud Computing** - A type of computing that relies on sharing computing resources via the internet rather than having local servers or personal devices to handle applications.

- **Cyber** - A prefix used in a growing number of terms to describe anything related to the internet. Cyberspace is the non-physical terrain created by computer systems.

- **DDoS Attack (Distributed Denial of Service)** - The incoming data that floods the victim network originates from many different sources, effectively making it difficult to distinguish legitimate user- traffic from attack-traffic and almost impossible to stop as the origin is spread across so many points.

- **DoS Attack (Denial-of-Service Attack)** - A type of attack on a network that is designed to bring the network to its knees by flooding it with useless data.

- **E2EE (End-to-End Encryption)** - is a system of communication where only the communicating users can read the messages. The systems are designed to defeat any attempts at surveillance or tampering because no third parties can decipher the data being communicated or stored.

- **ICS (Industrial Control System)** - is a general term that encompasses several types of control systems used for industrial process control. For example a SCADA or PLC system.

- **IDS (Intrusion Detection System)** - A passive monitoring system designed to warn you of suspicious activity that might result in a virus, worm or hacker by looking for intrusion signatures. IDS is NOT a firewall as it only signals an alarm as opposed to preventing an intrusion

- **Incident Response Plan (IRP)** - IRP form part of business continuity plan (BCP) that documents a set of instructions for, responding to and limiting the effects of an event that may or may not be an attack or threat to a computer system or corporate data security. An IRP should not only address IT functions but identify appropriate team members and their roles both internal and external to ensure a holistic organisational response to a cyber event

- **IPS (Intrusion Prevention System)** - A combination of IDS and an application layer firewall for protection, IPS is generally considered to be the "next generation" of IDS.

- **Malware** - An abbreviation for "malicious software", generally 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.

- **PCI DSS (Payment Card Industry Data Security System sometimes referred to as PCI)** - A proprietary information security standard developed by MasterCard, Visa, American Express, Discover and JCB International to assist merchants in preventing payment card fraud and to improve security around processing and storing payment card details. PCI addresses minimum security requirements such as firewalls, encryption and anti-virus software.

- **Pen Testing** - A penetration test is an authorised simulated attack on a computer system that looks for security weaknesses, potentially gaining access to the system's features and data. A useful tool to better understand the appropriateness of network defences.

- **Phishing** - A "con game" on the internet to collect personal information. Spear phishing is a more targeted phishing attempt on a specific user to collect personal or confidential information.

- **PII (Personally Identifiable Information)** - Unique information that establishes an individual identity.

- **PKI (Public Key Infrastructure)** - A system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction. PKIs are currently evolving and there is no single PKI nor a single agreed-upon standard for setting up a PKI.

- **PLC (Programmable Logic Controller or Programmable Controller)** - is an industrial control system first used in the automobile industry. These systems are used in control manufacturing processes and the robotic devices of assembly lines.

- **Rootkits** - Malicious software that is activated each time your system boots up. They are difficult to detect because they are activated before your system's operating system has completely booted up. Rootkits are able to intercept data from terminals, network connections and the keyboard.

- **SCADA (Supervisory Control and Data Acquisition)** - A computer system typically used to monitor and control industrial plant or equipment for a wide range of industries such as sewage, waste control, energy, oil & gas refining and transportation. These systems were developed in the 1960's.

- **SIEM (Security Incident Emergency Management)** - A security management system that deals with real-time monitoring, correlation of network events, notifications via console view. A key focus of a SIEM is to monitor and help manage user privileges, directory services and other system-configuration changes; as well as providing log auditing and review.

- **SMSphising** - The use of social engineering techniques by SMS to masquerade as a trusted party and gain access to a smart phones private and/or financial information.

- **Sniffer** - A program and/or device that monitors data travelling over a network. These programs can be used both for legitimate and illegitimate network purposes.

- **SQL Injection (Standard Query Language)** - A form of attack on a database-driven website in which the attacker "injects" unauthorised SQL commands to bypass firewalls. SQL injection is a very common intrusion tool in cyber crime.

- **Table-Top Exercise** - A simulated cyber attack conducted via authorised vendors for training purposes. These exercises can explore the effectiveness of defensive strategies or test preparedness of an organisation as a whole. These tests serve to ensure real event readiness and/or deployment of recovery strategies for major cyber events.

- **Tokenisation** – is the process of substituting sensitive data with a non-sensitive equivalent, referred to as a token. The token has no extrinsic or exploitable meaning or value.. In essence the token is a reference / an. identifier that can be mapped back to the original sensitive data through a tokenization system.

- **Trojan or Trojan Horse** – A destructive program that disguises itself as a benign network application but is designed to destroy and delete files. They often go undetected by antivirus software.

- **2FA (Two-Factor Authentication)** – Two-factor authentication is a method used to confirm a user's claimed identity by a combination of two different components. Typically something that the user possesses (eg. debit card) and something that only the user knows (eg. a PIN code).

- **Virus** – A program that is loaded onto a computer and runs without the users knowledge. All computer viruses are man-made and even self-replicating. It is dangerous because it will quickly use all available memory and bring the system to a halt. More dangerous virus types are capable of transmitting themselves across networks, bypassing security systems and creating backdoors into networks.

- **Vishing (voice phising)** – The use of social engineering techniques over a telephone system to gain access to private and/or financial information.

- **VLAN (Virtual Local Area Network)** – a network of computers that behave as if they are connected to the same wire even though they may actually be physically located on different segments of a LAN. These networks have been susceptible to the lateral movement of malware through a network (also known as 'hopping').

- **Waterhole Attack** – An attack where users are lured to a compromised website, "watering holes", where threat actors plant

- **White Hat Hacker** – A hacker that uses their skills to expose system vulnerabilities before malicious hackers (known as black hat hackers) exploit them. Typically they are hired by an organisation to improve system security.

About Chubb in Austalia

Chubb is the world's largest publicly traded property and casualty insurer. Chubb, via acquisitions by its predecessor companies, has been present in Australia for over 50 years. Its operation in Australia (Chubb Insurance Australia Limited) provides specialised and customised coverages include Marine, Property, Liability, Energy, Professional Indemnity, Directors & Officers, Financial Lines, Utilities as well as Accident & Health, for a broad client base, including many of the country's largest companies.

More information can be found at www.chubb.com/au

Contact Us

Chubb Insurance Australia Limited
ABN: 23 001 642 020 AFSL: 239687

Grosvenor Place
Level 38, 225 George Street
Sydney NSW 2000
O +61 2 9335 3200
F +61 2 9335 3411
www.chubb.com/au

Chubb. Insured.℠