A Dictionary of

Information Security Terms, Abbreviations and Acronyms

by Alan Calder and Steve G Watkins

IT Governance Publishing

A DICTIONARY OF INFORMATION SECURITY TERMS, ABBREVIATIONS AND ACRONYMS

ITG POCKET GUIDES

Future titles will cover the following subjects:

Practical Information Security series

Fundamentals of Information Security Management

Information Security Governance

ISO 27001

ISO 27001 Assessments Without Tears

Practical Governance series

A Director's Guide to Combined Code and Turnbull

BASEL 2

Health and Safety

Information Governance

Internal Control Structures

IT Governance

Project Governance

Risk Management

Sarbanes-Oxley

The Integrated Management System

The PCI DSS

What is Compliance?

A Dictionary of Information Security Terms, Abbreviations and Acronyms

ALAN CALDER
STEVE G WATKINS

IT Governance Publishing

PUBLISHER'S NOTE

Every possible effort has been made to ensure that the information contained in this book is accurate at the time of going to press, and the publishers and the author cannot accept responsibility for any errors or omissions, however caused. No responsibility for loss or damage occasioned to any person acting, or refraining from action, as a result of the material in this publication can be accepted by the publisher or the author.

First published in the United Kingdom in 2007 by IT Governance Publishing.

IT Governance Publishing
IT Governance Ltd
66 Silver Street
Ely
Cambridgeshire
CB7 4JB
United Kingdom

www.itgovernance.co.uk

ISBN 978-1-905356-21-8

INTRODUCTION

This extensive dictionary of information security and related terms is not a technical dictionary: it is designed to help a manager or someone new to the subject identify the meaning of a particular term.

Some of the terms used in this book will in due course be covered by *ISO27000, Information technology - Information security management - fundamentals and vocabulary* and so this book will be updated to reflect the terms covered in that standard once it is published.

Please e-mail us (*feedback@itgovernance.co.uk*) with words and terms you would like to see in future versions of this glossary, or if you think you find any errors while using it.

Definitions that have been taken from ISO/IEC 17799:2005 are identified thus: *

Definitions that have been taken from ISO/IEC 27001:2005 are identified thus: **

Additional definitions that have been taken from BS 7799-3:2006 are identified thus: ***

Definitions that have been taken from ISO/IEC 20000-1:2005 are identified thus: ****

A

Acceptable use policy – an Acceptable use policy sets out what the organization considers acceptable behaviour on, and acceptable use of, e-mail and Internet access systems. A number of legal and employment (Human Rights Act and Regulation of Investigatory Powers Act in the UK) issues affect the development and deployment of Acceptable Use policies, but this should not deter organizations from putting them in place.

Access – the opportunity (physical or logical or both) to use any information processing facilities or any component of them (eg, a piece of data, an application, etc).

Access agreement – this is an agreement, between an organization and each of its employees, issued prior to release of a specific user name, in which the employee accepts the access rights and privileges attached to that user name and agrees to follow a series of procedures and requirements in respect of the use of that user name. This usually includes agreement to comply with the Acceptable Use policy.

Access control – this is the policy of controlling access to information processing facilities through a combination of access agreements and technological security measures that implement the policy guidelines. These controls therefore restrict the rights of individual users to access information processing facilities. User access rights reflect user access controls: the user has the right to do those things that the controls allow.

Access control list (ACL) – a formal (preferably approved) list of users who have defined access rights to an asset within information processing facilities: in other words, they should ensure that only legitimate users can access the asset.

Access point (AP) – a wireless hub that enables wireless computers to access a wired (or fixed) network.

Access rights – are usually determined by a policy that users should only have access to those systems and assets that they need in order to do their jobs and that everything else is expressly forbidden to them. These access rights are usually enforced through the user agreement and the configuration of the systems .

Accreditation – the procedure through which an authoritative body formally recognizes a person's or organization's competence to carry out specified tasks. Not to be confused with certification. Third party certification (auditing) bodies become accredited and those they audit, subject to a successful outcome, become certificated.

Accountability – not obviously a computer-related term, but fundamental to effective information security … and is the concept that any activity within an information system should be traceable to an individual who can be held responsible for the action (or inaction) and its consequences. It is the notion that the 'buck stops somewhere'.

ActiveX – a Microsoft ActiveX control is a 'component object model technology' designed to enable software components to communicate. It allows users to quickly and easily download added functionality to Internet Explorer and is often exploited by spyware.

ACL – *see* Access control list.

Ad hoc mode – is a method of connecting up to nine wireless clients directly to one another, without the use of a wireless AP.

Administrator – this is the user role responsible for installation, configuration, updating, amendment or deletion of a system, usually a software system. An administrator can do anything, usually untraceably, and therefore administrator user names should only be issued to people of proven competence who have been successfully screened to ensure there is no history of malicious computer-related activity.

Advance fee fraud – any fraud that involves the victim paying money up front in exchange for the false hope of a payback later. Also known as '419' , named after the Nigerian legal code that covers the crime as this is where it originated.

Advanced encryption standard (AES) – (also known as 'Rijndael', a portmanteau formed from the names of its two inventors) this US government 128-bit encryption standard superseded DES in November 2001 and is widely deployed.

Advisory – an assessment of significant new information security trends or developments that may relate to broad trends or specific threats and technologies. Issued by organizations such as CERT (CERT is a centre of Internet security expertise, located at the Software Engineering Institute, a US government-funded research and development centre operated by Carnegie Mellon University).

Adware – advertising that is integrated into software and which is usually provided as a download to a computer in combination with another application provided at no charge provided the adware is run. Adware is sometimes malicious.

AES – *see* Advanced Encryption Standard.

Airborne viruses – are viruses that use short-range wireless connections (eg, Bluetooth) for propagation. Mobile phones and PDAs are the targets of this sort of virus.

Analogue – 'relating to or using information represented by a continuously variable physical quality (such as spatial position, voltage, etc) rather than digitally' is the definition provided in the *OED* (Concise, 11th edn); if the computer world of bits and bytes is the digital one, the physical world in which we live, eat and breathe is the analogue one.

Anti-malware software – this is software specifically developed to deal with malware: adware, spam, spim, spyware, Trojans, viruses, worms, and most automated exploits, irrespective of their attack vector. This term should not be seen as synonymous with anti-virus software, not all of which adequately reflects the range of ways in which individuals and organizations connect to the Internet. A good anti-virus software package will deal with all aspects of malware except for adware and spyware, which will need their own solutions.

Anti-spyware – software that will identify spyware packages installed on a computer and, if given the instruction by the user, will then remove all instances of them from the computer, wherever they may be hiding.

Anti-virus software:

- Anti-virus software is software that is specifically designed to detect and halt viruses, worms and Trojans in e-mail. It is not necessarily designed to deal with spyware, adware, spam, or anything coming through Instant Messenger software.
- Anti-virus software tackles viruses at three points: it examines incoming e-mail (particularly

attachments) at your e-mail gateway for known viruses; it scans the hard disk and all the files for any viruses that may have bypassed the gateway virus checker; and it scans outgoing e-mails to ensure they are not carrying an infection.

- There are two types of virus detection. The first relies on identifying precise characteristics of viruses (by searching for their 'signatures' and comparing them with its database of known viruses) and the second (heuristic detection) searches for types of misbehaving programs. New worms are more likely to be detected by heuristic checks.

- Normal viruses are only going to be detected if your anti-virus software has an up-to-date database of signatures. This means regular updates – daily is better than weekly.

- Tip: allow the automatic update service to run the moment it alerts you; a large proportion of viruses and other exploits propagate themselves via computers that don't yet have the latest updates installed.

- Installing more than one anti-virus software package will *not* increase your protection – it may even decrease your protection if the packages conflict.

- Windows XP Service Pack 2 does not contain anti-virus software. It will alert you if your anti-virus software is not running, or is not up-to-date, but that is all.

- Today's blended threats mean that your anti-virus software must integrate with your firewall and other anti-malware software (anti-spam, anti-spyware, Instant Message protection, etc): unless

you are a sophisticated user, you are better off finding and installing a package that covers all the bases rather than attempting to configure a number of different packages from a number of different suppliers to work together; if your current supplier hasn't worked out how to do it, you might look for one who can.

AP – *see* Access point.

Applet – is a small Java program that runs in a browser. Applets are designed so that they cannot read or write to the browser's computer file system or open any other network connections.

Application (or application software) – this is the software that users actually use, eg, Microsoft Office or SAP.

Application layer – the standard TCP/IP model's top layer, providing protocols for services such as e-mail, file transfer, etc.

Application Service Provider (ASP) – an organization which provides application software on an outsourced, or rental, basis.

Architecture – the broad outline of a network (or a computer, or a software program) into which the detailed processes will be placed. An open architecture is one which allows for easy connection by devices from other manufacturers, while a proprietary architecture is designed to make this difficult.

Archive – *see* Auto-archive.

Arpanet – the Advanced Research Project Agency ran the first computer network in the 1970s. The Internet evolved from Arpanet, which was switched off in 1990.

ASCII – American Standard Code for Information Interchange: a widely used code that represents typed characters.

ASP – see Application Service Provider.

Asset – anything that has value to the organization.* Information assets are likely to be of the following types:

- Information: databases and data files, other files and copies of plans, system documentation, original user manuals, original training material, operational and other support procedures, continuity plans and other fallback arrangements, archived information, financial and accounting information.
- Software: application software, operating and system software, development tools and utilities, e-learning assets, network tools and utilities.
- Physical assets: computer equipment (including workstations, notebooks, PDAs, monitors, scanning machines, modems, printers), communications equipment (routers, cell phones, PABXs, fax machines, answering machines, voice conferencing units, etc), magnetic media (tapes and disks), other technical equipment (power supplies, air conditioning units), furniture, lighting, other equipment.
- Services: 'groups of assets which act together to provide a particular function', such as computing and communications services, general utilities eg, heating, lighting, power, air-conditioning.

Asymmetric encryption – also known as public key encryption, is a system under which an organization has two keys, one private and one public. Anyone can use the public key to encrypt a message for the

organization, knowing that only the possessor of the private key will be able to decrypt it. Equally, anything that decrypts properly using the public key must have been encrypted using the complementary private key. A critical issue in public key cryptography is to attest the validity of the key pair and, in particular, that the named public key really is the organization's public key. This is done with a digital certificate, issued by a certificate authority.

Attachment – programs or documents that are attached to an e-mail.

Audit – systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which agreed criteria are fulfilled (ISO 19011, section 3.1).

Auditor – person with the demonstrated personal attributes and competence to conduct an audit. (For third party certification audits the auditor(s) are often called assessor(s).

Audit criteria – a set of policies, procedures or requirements (used as a reference against which audit evidence is compared).

Audit evidence – records, statements of fact, or other information which is relevant to the audit criteria and verifiable.

Authentication – the process of establishing that users are who they claim to be. It requires users to provide a combination of a user name and one or more credentials: something known (a password), something possessed (digital signatures, smart cards), or a physical feature (biometrics). Weak authentication requires just a password; strong authentication ('two factor' authentication) requires at least two of these three types of credential.

'Authenticity' is a description of an authenticated user.

Authorization – once a user has been authenticated, authorization to use the information, computer services or other system can be granted. Authorization also applies to the step prior to granting a user name, when an organization authorizes an individual to have specific access rights.

Auto-archive – an automated process of archiving old digital material, particularly e-mail.

Auto-diallers – small software programs that automatically dial designated telephone numbers in order to connect users to their ISPs. This might be set up by design through Windows, or it might be an option offered while visiting a website. The latter are usually premium rate numbers and the cost of the calls is automatically added to the user's ISP or telephone bill. There are Trojans that change your autodial settings to the more expensive ones.

Automated hacking script – a method of exploiting a vulnerability in software that has been turned into a piece of autonomous code and released onto the Internet.

Automatic updates – a software provider's automated process for issuing updates (patches, fixes and upgrades) to their installed base of users, such that the update is executed with a minimum of user involvement.

Availability – ensuring that authorized users have access to information and associated assets when required.**

Availability – ability of a component or service to perform its required function at a stated instant or over a stated period of time.****

Awareness training – all employees of any organization that uses computers need to be trained in their safe use and be kept aware of threats and responses to them.

B

Back door – programmers and administrators deliberately leave ways into software systems that can be used later to allow access to the system while bypassing the authorized user file. Sometimes, developers forget to take out something that was put there simply to ease development work or to assist with the debugging routine. Sometimes they are deliberately left in to help field engineers maintain the system. However they get there, they can provide any unauthorized user with access to the system.

Back orifice – is a remote administration tool that has great potential for malicious use. It is very easy to use, so that script kiddies have no problem using it. It is also 'extensible', which means that it develops and improves with age. Most anti-malware systems should detect and remove back orifice, but new versions become available on a regular basis.

Backup (PDAs, computers, networks) – a backup is a copy of information that is made and retained in case of loss or damage to the original (it could be paper copies of paper documents, but we are mostly concerned with digital copies of digital data) which includes all information assets: client and supplier data, business planning data, intellectual property, operating systems, applications, protocols, everything. Different types of backup include full (everything is backed up whether is has changed or not) and incremental (only items that have been created or changed since the last backup are copied).

Backup cycles – a copy just of tonight's data is useful, but neither efficient nor adequate. Not efficient, because a complete backup will take substantial time to run and will required a lot of tape.

Not useful, because you may need (for forensic reasons, for instance) to access an older version of the data – and you don't want to have hundreds and hundreds of backup tapes. A backup cycle usually works on a grandfather, father, son basis. The 'son' is an incremental daily backup, collecting details only of today's changes, and the tape is re-used on the same day next week; the 'father' backup is done at the end of every week (one tape for each day) and is overwritten at the end of the same week next month. The 'grandfather' backups are done at the end of every month and are overwritten in the same month next year. Remember: backup has nothing to do with data retention policies; data retention policies are driven by local compliance requirements. Whatever data has to be retained, also has to be backed up.

Bandwidth – the amount of data that a particular data cable can carry at any one time.

Basel II – the Committee for Bank Supervision's most recent revision to the Basel risk-based capital rules for banks.

Baseline – snapshot of the state of a service or individual configuration items at a point in time.****

BCM – *see* Business continuity management and Business continuity plan.

BCS – the British Computer Society is the UK's Chartered Engineering Institution for Information Systems Engineering. Through the Information Systems Examinations Board (ISEB), the BCS provides industry-recognized qualifications that measure competence, ability and performance in information security.

Biometrics – is the identification of a user by means of a physical characteristic, such as a fingerprint, iris, face or voice.

BIOS password – a BIOS software code that links the operating system to the hardware and often includes the ability to prevent any unauthorized users starting the machine.

Bit – a unit of measurement of information (from binary + digit); there are 8 bits in a byte.

Bit-wiping software – is software that will, under certain conditions, wipe out specific data stored on a device.

Blackberry – a hand-held wireless e-mail device.

Black hat – a criminal hacker.

Blacklist – a list with negative connotations, eg, it might be a list of those senders that a spam filter will *always* filter out, or a list of those mobile phones that will be banned from connecting to the mobile phone network.

Blended threat – this might more accurately be described as the threat of a blended attack, an attack which comes from a number of directions, or via a number of vectors. For instance, a spam e-mail message might be carrying a payload, in the form of a Trojan, which it installs on your computer to open it up to a botnet. Similarly, an innocent-looking piece of adware might contain some spyware, a Trojan installer and a browser hijacker.

Bluejacking – an attack on a Bluetooth enabled device (usually a mobile phone) in which an attacker sends an unauthorized message to the device.

Bluesnarfing – an attack on a Bluetooth enabled device that allows download of all contact details

along with other information without leaving any trace of the attack.

Bluetooth – a radio-frequency standard that allows any sort of electronic equipment to make its own short range connections, without wires, cables or direct action of any sort from a user. It is an inexpensive, wireless and hassle-free technology that is being deployed in a vast range of digital equipment. The name 'Bluetooth' refers to the eighth century Danish king, Harald Bluetooth, who united Denmark and Norway and introduced Christianity into Denmark. He had little to do with communication technology, but Scandinavian companies have long been a driving force behind the development of mobile telephony and the development of this standard. Bluetooth is not restricted to line-of-sight, but its effective range is about 10 metres; this short range is a result of its very weak signal, selected to avoid the danger of interference with other devices, primarily medical ones, that use the same range of frequencies.

Bluetooth snarfing – *see* Bluesnarfing.

Blue screen – when Microsoft's Windows operating system snarled up on some internal software fault and became incapable of continuing, the user would usually get a blue screen (aka the 'blue screen of death'). Any work you were doing was lost and you had to switch off and re-boot.

Boot – the process that takes place inside the computer after you switch it on and it starts loading your operating system while you do something else; it comes from the idea of a bootstrap as something that you use to pull your boots on with.

Boot password – a password that applies during computer start-up before operating systems load.

Bots – short for robots, as in 'botnets' and 'crawler-bots'.

Botnets – a network of zombie computers, usually created and controlled by criminals, either for distributing spam or for mounting DDoS attacks.

Broadband – high bandwidth cable.

Browser (IE, Firefox, Opera) – this is the piece of software that enables a user to browse sites on the Web. Microsoft's Internet Explorer is the most widely used; Firefox and Opera are two open-source competitors.

'Brute force' attack – *see* Password cracking.

BS 7799 – the British specification for an Information Security Management System, conformance with which provides grounds for external, third party certification of the quality of an organization's information security posture. *See* ISO 27001.

BS 7799-2:2005 – part 2 of the British information security standard is the equivalent of the international standard ISO/IEC 27001:2005.

BS 7799-3:2006 – part 3 of the British information security standard contains guidelines for information security risk assessments.

BSA – the Business Software Alliance is 'the foremost organization dedicated to promoting a safe and legal digital world', which it does by pursuing organizations that might be running unlicensed software.

B2B – business-to-business.

B2C – business-to-consumer.

BSI – the British Standards Institution, the UK's national standards body. (BSI also has a certification

division which competes with many other certification bodies. The two functions should not be confused).

Buffer overflow (or overrun) – a buffer is an area of memory that holds data to be processed. It has a fixed, predetermined size. If too much data is placed into the buffer, it can be lost or can overwrite other, legitimate data. Buffer overflow vulnerabilities have for a number of years been a major method of intrusion. They provide hackers with an opportunity to load and execute malicious code on a target workstation.

Bug – an error or flaw in a computer program.

Bugtraq – is a regularly updated 'high volume, full disclosure mailing list for the detailed discussion and announcement of computer security vulnerabilities'. It is a vendor-neutral, central store of known operating system vulnerabilities; the website is at *www.securityfocus.com/archive/1*. Anyone can read the latest vulnerability disclosures – including cybercriminals.

Business continuity management – is the creation, management and maintenance of an organization's business continuity plan.

Business continuity plan – this is a scenario-based plan, developed in advance of any incidents that might undermine the availability of an organization's information, and which describes precisely how each of the most likely incidents is to be handled. It usually involves specific infrastructure and system amendments that will make continuity possible, and it certainly requires regular testing, to ensure that it will actually work when the time comes.

Byte – eight bits.

C

Cache – this is the section of a computer's memory which retains recently accessed data in order to speed up repeated access to the same data. If the data on the Web has altered since you last visited it, you may need to refresh the page to see the new data, otherwise you will only see what is stored in the cache.

Can-Spam – the US Act against spam.

CAP – Certification and Accreditation Professional. The CAP credential, awarded by $(ISC)^2$ is specifically designed for security professionals involved in certification and accreditation. This qualification supports those formalizing processes used to assess risk and establish security requirements, as well as ensuring information systems possess security appropriate for their level of exposure to potential risk. *See* $(ISC)^2$.

C:cure – a framework designed by the UK Department of Trade and Industry to support the implementation of BS 7799-2 (an early version of ISO 27001) in the early days of the accredited certification scheme. This framework was available from 1997 to 2000, when it was withdrawn.

CDPA – *see* Copyright Designs and Patents Act.

CEH – Certified Ethical Hacker. The CEH programme certifies individuals in the specific discipline of ethical hacking from a vendor-neutral perspective. The Certified Ethical Hacker certification will fortify the application knowledge of security officers, auditors, security professionals, site

administrators, and anyone who is concerned about the integrity of the network infrastructure.

Cellphones – *see* Mobile phones.

CE marking – indicates conformity with European safety requirements as laid down in EU regulatory standards.

CEN – the European Committee for Standardization is a private, non-profit organization whose mission is to provide an efficient infrastructure for the development, maintenance and distribution of coherent sets of standards and specifications.

CENELEC – a non-profit technical organization, composed of the National Electrotechnical Committees of 29 European countries.

CERT – the Computer Emergency Response Team is the Internet emergency response team formed by the US Defence Advanced Research Projects Agency (DARPA).

Certificate – this is an encrypted file that contains information to identify a user or server.

Certification – the process through which a certification body confirms that a product, process or service conforms to a specific standard or specification. For example, an organization becomes certificated to ISO 27001:2005.

Certificate authority (CA) – a CA is a trusted third party who will issue a digital certificate to attest the authenticity of an organization's public key. The CA will review the credentials of any organization that wants a digital certificate before issuing it. This review will include the Dun and Bradstreet number or Articles of Incorporation (in the UK) and a thorough background check to ensure that the

organization is what it claims to be. The CA may be a secure server on the network (the single trust model) or an external third party organization recognized by many (the multi-party trust model). The keys used are either 40-bit or 128-bit.

Certificate in Information Security Principles – the key ISO 27001 based ISEB qualification.

Certification body – *see* Third party certification body.

CESG – the information assurance (IA) arm of the UK's Government Communications Headquarters (GCHQ). CESG offers a range of products and services including technical consultancy and advice, policy documentation, product evaluation and training, primarily to UK government and the armed forces, the wider public sector, and industries forming part of the 'critical national infrastructure'.

Challenge-response – is a technique for fighting spam, which requires a new sender to prove legitimacy to the recipient by entering a code on a website.

Change control – is the process and procedures to identify, document, review, and authorize any changes to software, documents, projects, etc.

Change record – a record containing details of which configuration items are affected, and how they are affected, by an authorized change.****

CHAP – the Challenge Handshake Authentication Protocol is a method of authentication between a server and a client.

Chat rooms – are virtual rooms, on the Web, in which users can chat (normally by typing) in real time.

CHECK IT Health Check – to become a CHECK Team Leader you must pass the CHECK Service Assault Course (CSAC) which is a rigorous assessment designed to assess IT security consultants against a skill set baseline of practical penetration testing. The CSAC can only be taken by security professionals working for a CHECK-approved service provider.

CIS – the Center for Internet Security is a standard setter for secure configuration of systems connected to the Internet; see website at: *www.cisecurity.org*.

CISA – Certified Information Systems Auditor. CISA is a certification for information systems (IS) audit, control and security professionals. It recognizes an individual's achievements in conducting information system audits. Candidates looking to gain the CISA certification must sit an examination, submit evidence of a minimum of five years' IS auditing, security or control work and agree to abide by ISACA's Code of Professional Ethics. *See* also ISACA.

CISM – Certified Information Security Manager. The CISM certification programme is for experienced information security managers and those with information security management responsibilities. It is for security professionals who manage, design, oversee and / or assess an enterprise's information security. The CISM certification promotes international practices and provides executive management with assurance that those earning the designation have the required experience and knowledge to provide effective security management and consulting services.

CISMP – Certificate in Information Security Management Principles. This qualification, which is based on ISO 27001, provides a base level of

knowledge for individuals who are thinking of moving into a security or security-related function. It also offers an opportunity to those for whom security responsibility is already part of their day-to-day role to enhance or refresh their knowledge.

CISSP – Certificate for Information System Security Professional. The CISSP certification, awarded by $(ISC)^2$), provides information security professionals with an objective measure of competence and a globally recognized standard of achievement. The CISSP credential suits mid- and senior-level managers who are working towards or have already attained positions as CISOs, CSOs or Senior Security Engineers. *See* $(ISC)^2$.

CLAS – the CESG Listed Adviser Scheme, CLAS, is a partnership linking the information assurance knowledge of the CESG with the expertise and resources of the private sector. CLAS consultants are approved to provide information assurance advice on systems processing protectively marked information up to, and including, 'secret'. The scheme is particularly relevant to consultants dealing with UK government clients.

Classification system – a system where information assets are classified and clearly marked according to their sensitivity, confidentiality, value, importance, etc.

Client – a computer that uses a server or a network service for something that it cannot do on its own.

Cloaking bags – are bags that are designed to block WiFi and Bluetooth signals and which can protect 'always one' Cellphones and PDAs from signal leakage or hijacking.

CMDB – *see* Configuration Management Data Base.

Code of Practice – provides guidance and uses words like 'should' to indicate that compliance is not mandatory. It sets out what should be in an ISMS rather than how it should be designed. Organizations can choose controls from this code of practice or anywhere else, provided the requirements of the specification are met.

Combined Code – this replaces and refines the earlier requirements of the Cadbury and Greenbury reports on corporate governance and directors' remuneration. It came into force for all listed companies for year ends after December 1998. The Combined Code requires directors of listed companies to annually review *all* their controls, 'including financial, operational, compliance and risk management'.

'Commercial in confidence' – this is a classification level for information. It is not clear what purpose it serves, other than to highlight to someone who receives it that it may have value on the black market. An information security classification system needs to be simple, practical and coherent.

Common Criteria (CC) – the 'CC defines a set of IT requirements of known validity which can be used in establishing security requirements for prospective products and systems' and the official CC website is at *www.commoncriteriaportal.org*.

Compact disc – a data version of a CD which can store data.

Compartmentalization – is the concept of an internally secure network designed with a number of co-operating sub-networks and light firewalls and routers.

Compliance – a positive answer to the question: 'Is what is taking place in line with the pre-specified

requirements for what should take place?' Hence, non-compliance and compliance monitoring. Compliance is often used in a legal context.

Computer Misuse Act 1990 – the Act was designed to set up provisions for securing computer material against unauthorized access or modification. The Act basically outlaws, within the UK, hacking and the introduction of computer viruses.

Computer security – ensuring that the physical hardware, the computer, is secure, is part of the overall job of ensuring that all the information is secure. Computer security is just a part of the whole job. *See* also Information security.

Confidentiality – ensuring that information is accessible only to those authorized to have access.**

Configuration – how the components of a computer or a network are set up.

Configuration item – a component of an infrastructure or an item which is, or will be, under the control of configuration management.**** Configuration items may vary widely in complexity, size and type, ranging from an entire system including all hardware, software and documentation, to a single module or a minor hardware component.

Configuration Management Data Base – this is a database containing all the relevant details of each configuration item and details of the important relationships between them.****

Conformance – fulfilment of a requirement. A positive answer to the question: 'Is what is taking place in line with the pre-specified requirements for what should take place?' Hence, non-conformance and conformance monitoring. Conformance is often used in a non-legal context.

Control – a means of managing risk, such as policies, procedures, guidelines, practices or organizational structures, which can be of an administrative, technical, management or legal nature; also used as a synonym for safeguard or countermeasure.*

Control objective – the risk treatment plan objective that is to be achieved by implementing one or more of a number of controls.

Control standard – the level to which it has been decided that a risk must be controlled; this is usually determined by balancing the cost of the control, the likelihood of the risk and its potential impact to determine how much should be invested in controlling it. This cost of control (which should not exceed the likely cost of the impact) is translated into a standard against which the effectiveness of the control can be assessed.

Cookie – this is a small data file that a website stores on a surfer's computer and which contains information about the user (eg, user preferences) that is relevant to the user's experience of the website.

Copyright Designs and Patents Act 1988 (CDPA) – this is a complex and difficult area for any organization that deals in intellectual property and appropriate professional advice should be taken from a firm that specialises in it.

Corrective action – is action to eliminate the cause of a detected nonconformity or other undesirable situation.

Covert channels – are those channels installed, usually by software developers, in order to simplify the process of getting back into a piece of code, in order to amend it. These channels can be exploited by hackers.

CPU – the central processing unit drives your computer.

Crackers – hackers who break into computer systems specifically to steal data or cause damage. Hackers like to say that crackers break in, but that hackers get permission first and will publish their discoveries. Hence: crack and cracking.

Crash – this is what software sometimes does; *see* Blue screen.

Credit cards – pieces of plastic that enable people to get into debt; they are also essential for online shopping.

Credit reports – summary of financial information about consumers assembled on the basis of information filed with credit reporting companies, primarily by lenders.

Crime – *see* Cybercrime.

Critical – 'having a decisive importance in the success or failure of something' (*OED*, Concise, 11th edn).

Critical infrastructure – this is the construct of foundation systems and services that citizens and businesses rely on for their health, safety and well-being. Telecommunications, transportation, energy and banking services are part of the critical infrastructure, which is often privately-owned but which governments believe that citizens expect them to protect.

Cryptography – the art of protecting information by encrypting it.

CSIA – Central Sponsor for Information Assurance is a unit of the UK Government's Cabinet Office and works with partners in the public and private sectors,

as well as its international counterparts, to help safeguard the UK's IT and telecommunications services. The CSIA provides a central focus for information assurance in the UK.

CVE – Common Vulnerabilities and Exposures – the website at *www.cve.mitre.org* (funded by the US Department of Homeland Security) holds a dictionary of 'standardized names for vulnerabilities and other information security exposures, with the aim of standardizing the names for all publicly known vulnerabilities and security exposures'. It is not a database and would normally be used in conjunction with a vulnerability database like Bugtraq (*www.securityfocus.com*). CVE is publicly available and free to use. , You should therefore assume that cyber-criminals use it.

Cybercrime – any form of illegal activity that takes place in cyberspace. The UK's Computer Misuse Act 1990 made it an offence for anyone to access a computer without authorization, to modify the contents of a computer without authorization, or to facilitate (allow) such activity to take place. It identified sanctions for such activity, including fines and imprisonment. Other countries have taken similar action to identify and create offences that should enable law enforcement bodies to deal with computer misuse.

Cyberslacking – timewasting using the Internet.

Cyberspace – another term for the digital world, as opposed to the analogue one.

Cyber-terrorism – terrorist activities in cyberspace.

Cyber trust – cyberspace is still an inherently untrustworthy realm, in which it is not possible for buyers and sellers to physically establish one

another's bona fides. Methods of establishing cyber trust are therefore essential for effective e-commerce.

Cyber war – war in cyberspace, conducted by the military equivalents of hackers, spammers and virus writers.

D

Data Encryption Standard (DES) – is a widely used symmetric encryption standard. It is used for long communications and is relatively speedy to use. It is, however, quite an old system and this has led to triple DES (or AES), in which the same data are encrypted three times, employing different keys, which exponentially increases the strength of the encryption. Only the creator and receiver have the DES key (or keys); the key(s) are usually exchanged using either a shared master key or a pre-existing key exchange protocol.

Data Controller – this is the person, within an organization, who is responsible (in the UK, anyway) for the organization's compliance with the Data Protection Act.

Data Protection Act 1998 (DPA) – the legislation (UK) that sets out requirements for handling and protecting personal information and data.

Data Protection Officer (DPO) – the person appointed by an organization with the responsibility for ensuring that the organization complies with the DPA.

Data retention policies – in each jurisdiction (and sometimes for each individual regulation or statute) there are very specific requirements about the length of time for which organizations have to retain particular types of data. These requirements form the basis of the organizational data retention policy, which will then require technological and procedural elements for its implementation. It will also give rise to data storage and backup issues.

Decryption – this is the opposite of encryption, and involves translating encrypted content back into its original (usually plaintext) form.

DDoS – *see* Distributed Denial of Service Attack.

Defence in depth – *see* Layered security.

Denial Of Service attack (DOS) – this sort of attack is designed to put an organization out of business, or to interrupt the activities of an individual or group of individuals, for a time by freezing its systems. This is usually done by flooding a Web server (or other device) with e-mail messages or other data so that it is unable to provide a normal service to authorized users.

DES – *see* Data Encryption Standard.

Dialler – software (usually on a website) that will dial out to another website and charge back to you (on a credit card or, more usually, on your existing telephone bill) for the time used while on that site. The charge rate will not necessarily be lower than that of your existing supplier. *See* Auto-dialler.

Dial-up connection – Uses a modem to connect to an Internet Service Provider.

'Dictionary attack' – *see* Password cracking.

Digital Audio Tape – tape format used for storing and backing up data.

Digital certificate – (sometimes called a Server ID) is an encrypted file that attests to the authenticity of the owner of a public key, used in public key encryption; the certificate is created by a trusted third party known as a certificate authority (CA). The digital certificate is proven to be authentic because it decrypts correctly using the public key of the CA.

Digital Rights Management (DRM) – is any technology that copyright-owners might deploy to protect their interests in software or digital content. The technology only allows someone who has purchased a licence to use the material that it is protecting.

Digital signature – is encrypted data that binds a sender's identity to the digital information that is being transmitted. It is essential for non-repudiation.

Digital watermarking – is another term for steganography and is likely to become an important part of copyright management on the Internet. There are a number of companies offering competing digital watermarking technologies, both to create and to view digital watermarks.

Directory harvesting – Outlook and other e-mail client software programs contain directories of individual names and e-mail addresses. Directory harvesting attacks commandeer these directories and use them for the distribution of spam, viruses or worms.

Disability Discrimination Act 1995 (DDA) – this UK statute has clauses that require websites to be accessible to people with disabilities.

Disaster recovery plan – this is a scenario-based plan developed to deal with the after effects of an 'Act of God'. Business continuity and disaster recovery planning should go hand-in-hand, otherwise one could spend far too long arguing over whether restoration of systems from the backup is part of the disaster recovery or the business continuity plan. Certainly, disaster recovery management (or DRM) is about planning for and testing – usually rehearsing specific scenarios – potential disasters, such as fire, flood, terrorist attack, etc.

Disaster recovery management – *see* Disaster recovery plan

Disclaimers – are not necessarily worth the (digital) paper on which they are written, but they are nevertheless an essential statement of ownership and intended destination of information sent electronically.

Discoverable – Setting on a Bluetooth device that broadcasts its existence to other Bluetooth devices.

Distributed Denial of Service attack (DDoS) – this uses the computers of other, third party organizations or individuals (which have themselves been commandeered by the hacker) to mount an even larger scale attack on a target.

DMZ – a demilitarized zone (the term has a military origin, meaning the buffer zone between two enemies) is a computer or small network between the organization's secure perimeter (the trusted zone is inside this perimeter) and an untrusted zone, such as the Internet. Typically, the DMZ contains devices accessible to Internet traffic, such as Web servers, FTP servers, e-mail servers and DNS servers.

Document – information and its supporting medium.**** In ISO/IEC 20000 records are distinguished from documents by the fact that they function as evidence of activities rather than evidence of intentions.

Document control – a system whereby all documents within the system have a standard numbering system that identifies where they sit within that system, as well as a version number, an issue date and a document owner, so that the currency of the document is always clear. When a controlled document is amended, all copies of it should be

simultaneously withdrawn and replaced by the new version.

Domain controller – a domain contains a number of resources (applications, folders, printers, etc) and a domain controller is the server that manages the details of all the users authorized to access the domain.

Domain name – every website and e-mail address has a unique IP address which, when represented in letters (eg, *www.itgovernance.co.uk*), is its domain name.

Domain Name Server (DNS) – is a server that translates domain names into IP addresses.

Download – transfer a copy of a file (which may be data or a software program) from a remote computer (usually a website) to a requesting computer via a network (or Internet) connection.

DPA – *see* Data Protection Act.

Dumpster diving – Raiding rubbish bins to gather personal information.

E

Eavesdropping – listening in to information that is transmitted over the air but not intended for you, including verbal conversations.

E-commerce – trading in cyberspace, with goods and services usually supplied through a website.

E-crime – *see* Cybercrime.

E-crime busting – this is the job of a country's High Tech Crime Unit. Any large organization should ensure that it has the contact details for its national body, so that it can report crimes quickly.

Electronic Communications Act 2000 – designed to regulate the usage, within the UK, of cryptography and to make provision for the use of electronic signatures.

Elevation of privilege – an increase in access rights compared to normal.

E-mail authentication – as it is now possible to spoof an e-mail sender's name and address details, the question of how to authenticate the sender is becoming very important.

E-mail filter – software that scans e-mails for spam or other types of material and filters it accordingly.

Encryption – the conversion of plaintext into code, using a mathematical algorithm, to prevent it from being read by a third party.

Endpoint device – an endpoint device (eg, a PDA, a mobile phone, or a laptop) is one that connects (usually but not necessarily) wirelessly to the network. Every endpoint device is a potential vulnerability for a network and, therefore, the

network perimeter has to be considered as ending at the point of the device, rather than simply at the network firewall.

Endpoint security – security that is effective on all endpoint devices.

Escrow – arrangement where money or other assets are held by a trusted third party pending completion of a transaction.

Espionage – most of the traditional cold war spy organizations are now actively involved in commercial spying, competing with their long-established private sector brethren.

European Standards (BS ENs) – As a member of CEN and CENELEC, BSI is obliged to adopt all European Standards and to withdraw any national standards that might conflict with them. They are published in the UK as BS ENs.

Evil Twin – an attack in which an unauthorized or rogue AP with a stronger signal is placed in close proximity to a legitimate AP. Wireless users unwittingly log into the rogue AP (which might have a deliberately comforting SSID, such as 'local friendly coffee shop') and give away passwords, bank details, and other sensitive information.

Exploit – this is either the methodology for making an attack against an identified vulnerability (the noun) or the act (the verb) of attacking or exploiting the vulnerability. Exploits are often published on the Internet, either by black hats or by grey hats who claim that this is a good way of forcing software suppliers to develop more secure software or to provide fixes for existing software. Exploits can be automated and released into the wild, just like a virus.

Extranet – this is an extension to an organization's internal network, usually placed outside the organization's core firewall and secure perimeter but itself protected from unauthorized access, so that the organization's trusted partners have limited access to specific information and services.

F

FAST – the Federation Against Software Theft, the world's first anti-piracy organization working to protect the intellectual property of software publishers. See website at: *www.fast.org.uk*.

File sharing – the public sharing of files across a network, so that a number of users are able to access and use the same file.

Filter – is a software pattern or mask that is designed so that some types of items can pass through it while others will be caught and prevented or discarded.

Fingerprint recognition – biometric authentication using fingerprints.

Firefox – an open-source browser.

Firewall – is a technology that is designed to create a definite barrier and separation between two parts of a network, or between a network (or individual computer) and the Internet. It filters traffic through its ports in line with its traffic-filtering rules, which are set by the computer user or network administrator in line with corporate guidelines.

Flame – an irate e-mail.

Flash – an animation technology from Macromedia; it can be watched through a browser.

Flash cards (or flash sticks) – devices that use flash memory and are usually designed to access a computing device through a USB port.

Flash memory – a non-volatile memory device that retains its data when the power is removed.

FOI – *see* Freedom of Information Act.

Forensics – the scientific examination of evidence and the application of that evidence to identify the commission, nature and perpetrator of a crime.

Freedom of Information Act 2000 – the FOI is UK legislation that provides a general right of access to all types of information held by public authorities and those providing services for them.

Freeware – this is software that is available on the Internet and can be downloaded for free. This free download may be conditional on you downloading an adware program, which may come bundled with a number of scumware applications.

Freeloading – unauthorized users accessing the Internet through a wireless connection.

FTP – File Transfer Protocol is a method of transferring files over the Internet.

G

Gateway – technically, hardware or software that translates between two dissimilar protocols and, often, any mechanism that provides access from one system to another (eg, between a network and the Internet).

GHz – the Gigahertz (one thousand million hertz) is a unit of frequency of ultra-high-frequency electromagnetic signals and is also a measure of microprocessor clock speeds.

GIAC – Global Information Assurance Certification provides assurance (via a certificate from the SANS Institute) that a certified individual holds the appropriate level of knowledge and skill necessary to a practitioner in information security. The website is at *www.giac.org*.

Gigabyte – 1024 megabytes.

Google – the largest Internet search engine company. To 'google' is to use a browser-based search engine to find data on the Web.

GPRS – General Packet Radio Service is part of the GSM standard and delivers 'always-on' wireless packet data services to GSM customers; users only pay for the amount of data sent or received.

Grey hat – a type of hacker. *See* Hackers.

GSM – the Global System for Mobile Communications is a land mobile pan-European digital cellular radio-communications system.

Guest – a type of username that is set up to allow those who have not been allocated their own specific usernames to access and use a computer. It can easily be exploited by hackers and should be disabled.

GUI – Graphical User Interface is the combination of the screen and associated tools through which a person can interface with a computer.

Guideline – a description that clarifies what should be done and how, to achieve the objectives set out in policies.*

H

Hackers – hackers break into computer systems. Unlike crackers, they claim that they get permission first and will publish the results of their 'research'. Hackers have four prime motivations: (1) challenge, to solve a security puzzle and outwit an identified security set-up; (2) mischief, wanting to inflict stress or damage on an individual or organization; (3) working around, getting around bugs or other blocks in a software system; and (4) theft, stealing money or information. Hackers like to talk about 'white hat' and 'black hat' hackers; the argument is that the 'black hat' hackers are malicious and destructive (ie, 'crackers') while the 'white hat' hackers simply enjoy the challenge and are really on the side of good, offering their skills to help organizations test and defend their networks. This differentiation is convenient for hackers, who seem able to change hats as easily as they evade most network defences. The only sensible approach for any security-conscious organization is to assume that all hackers are potentially in the wrong colour hat, however they might initially present themselves. 'Grey hats' is a term that is evolving to recognize the uncertain danger of so-called 'ethical' hackers. Nowadays, commonsense suggests that a hacker is not to be trusted. *See* also Penetration testing.

Hacking tools – *see* www.insecure.org/tools.html for the current 75 most favourite tools for breaching (or assessing) the security of an organization, a website or a communication.

Hand scanner – a hand-sized device that can be used for scanning documents for later upload to a computer.

Hard drive – the permanent data storage device built into a workstation that stores its operating system, applications and other software and provides storage for files and folders. Its size is usually expressed in gigabytes.

Heuristic – a method of detecting viruses that have not yet been formally identified (discovered and signatures defined) on the basis of their behaviour patterns.

History (in browser) – your browser keeps a record of the websites you've visited, as an aide to your easy return. It can also be an aide for someone who wants to know where you've been, particularly in an Internet café.

Hoax – an e-mail message warning of a non-existent virus (or other problem) passed on by people who themselves received it and were duped into believing it was genuine. *See* Virus hoax.

Homeland security – the USA has a Department of Homeland Security, which is responsible for securing both the analogue and the digital borders of the USA.

Honey pot – an undefended computer on the Internet that is trying to attract hackers, viruses, worms and spam, so that their characteristics can be identified and defences designed and issued.

Hot fixes – are vendor-generated software packages composed of one or more files that address an identified problem or vulnerability.

HotSpot – is a wireless Access Point which, unless it is secure (ie, it is open), is accessible to any member of the public with a wireless-enabled PC whether or not it is intended for public use. If the HotSpot is

secure, then the user will need to know its WEP or WPA key to connect to it. *See* WEP *and* WPA.

HRA – *see* Human Rights Act.

HTML – Hyper Text Markup Language is a computer language widely used to format web pages and e-mail and which is often also used for spam.

HTTP – Hypertext Transfer Protocol is the protocol for moving hypertext files across the Internet. It is the standard language that computers use to communicate across the Web.

HTTPS – this is a secure version of HTTP, using SSL. *See* Secure Sockets Layer.

Human Rights Act 2000 (HRA) – incorporates into UK law the principles of the European Convention for the Protection of Human Rights and Fundamental Freedoms. An employee could use HRA to argue in a Court or Tribunal that the employer monitoring or tapping the employee's work telephone or e-mail or Internet activity was a breach of her/his rights under the Convention.

I

Identity theft – this is when someone gathers enough information about someone else (name, address, date of birth, credit card numbers, social security number, etc) to successfully impersonate that person online, by mail, over the telephone, or in person.

Identity management – this is the management of multiple versions of user identities across multiple applications, and might typically involve single sign-on, password synchronisation, etc.

IDS – intrusion detection systems. *See* Intrusion detection.

IE – Internet Explorer, ie, Microsoft's browser.

IEC – International Electrotechnical Commission, the leading global organization that prepares and publishes international standards for all electrical, electronic and related technologies.

IETF – Internet Engineering Task Force, a workgroup that takes steps to propose official standards and protocols for use on the Internet. See website at: *www.ietf.org*.

IIS – Internet Information Server was the original Microsoft server operating system, which has been replaced, and which was inadequately robust.

IMEI number – the International Mobile Equipment Identity number is a 15-digit unique code that is used to identify a telephone to a network. It can (on most phones) be displayed by typing: *#06# on the keypad. It may also be printed on the compliance plate under the battery. When a phone is switched on the IMEI is transmitted and automatically checked

against the network's list of blacklisted phones in its EIR (Equipment ID Register) to establish whether or not the phone should be able to log on to the network and make calls.

Impact – the likely outcome of the successful exploitation of a vulnerability by a threat.

Impact analysis – analysis and financial evaluation of the likely outcome of the successful exploitation of a vulnerability by a threat, considering the asset's availability, confidentiality or integrity.

Incident – any event which is not part of the standard operation of a service and which causes or may cause an interruption to, or reduction in, the quality of that service.**** Not to be confused with Information Security Incident (*see* below).

Incident management – this is the process of managing incidents; it usually depends on a pre-rehearsed plan and a set of tested options.

Information – the *New Shorter Oxford English Dictionary* provides these helpful definitions: 'knowledge or facts communicated about a particular subject, events, etc; intelligence, news' and 'without necessary relation to a recipient: that which inheres in or is represented by a particular arrangement, sequence or set, that may be stored in, transferred by, and responded to by inanimate things'. Clearly information, or data, exists in many forms but, for the purposes of its security, we are concerned with data that has a digital, paper, or voice format.

Information classification – *see* Classification system.

Information Commissioner – publicly-appointed post to enforce personal privacy (through the Data Protection Act) and public openness (through the

Freedom of Information Act) in the UK. See website at: *www.ico.gov.uk*.

Information processing facilities – any information processing system, service of infrastructure, or the physical location housing them.*

Information security – preservation of the confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.*

Information security event – an identified occurrence in a system, service or network indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant* (*see* also Information security incident).

Information security incident – a single or a series of unwanted or unexpected events that has a significant probability of compromising business operations and threatening information security.*

Information Security Management System (ISMS) – that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.**

Information Security policy – this is the organizational policy for securing its information assets.

Infowar – *see* Cyberwar.

Infrared – this is a communication method that uses the infrared spectrum in light beams. It is used in most TV remote systems and is also used to connect some peripheral devices (mice, keyboards) to computers.

Infrastructure mode – a WLAN architecture in which a wireless AP provides the bridge between wireless clients and the fixed, existing network.

Instant Messaging (IM) – a communication methodology that is analogous to a private chat room; it enables you to communicate over the Internet in real time with another person, using text.

Insurance – computers should be covered under insurance policies. Individuals and organizations both need to ensure that their insurance polices specifically cover their various information assets and that the nature of the cover is adequate.

Integrity – safeguarding the accuracy and completeness of information and processing methods.**

Intellectual property rights – the rights of an inventor or assignee to use and licence an idea or creation.

Internet – the massive, global network of networks, connecting millions of computers, allowing any computer to communicate with any other by any one of a number of protocols. The Internet is not the Web: *see* World Wide Web.

Internet cafes – these are cafes that provide banks of computers and Internet access, for a fee, as well as refreshments.

Internet Explorer (IE) – Microsoft's browser.

Internet Protocol (IP) address – each computer connected to the Web (or permanently connected to an individual network) has its own unique 32-bit address. This is written in digital form and translated into a domain name for ease of use. A dial-up connection usually works with dynamic address allocation from a pool of available addresses, so a

user's IP address will be different at every Internet logon. A broadband connection that is always on will have an unchanging address, which will offer more of a target for a hacker.

Internet Protocol Security (IPSec) – defines how interoperable, secure host-to-host and client-to-host connections (known as Virtual Private Networks, or VPNs) are to work, creating an encrypted tunnel over a public network which provides privacy as good as that available on a private network and thus providing security for the transmission of sensitive information over unprotected networks; it protects and authenticates IP packets. *See* Virtual Private Network.

Internet protocol security VPN – creates a secure connection between two systems. It defines how interoperable, secure host-to-host and client-to-host connections (known as Virtual Private Networks, or VPNs) are to work, creating an encrypted tunnel over a public network which provides privacy as good as that available on a private network. for technical information see website at: *www3.ietf.org/proceedings/96mar/charters/ipsec-charter.html* .

Internet Service Provider (ISP) – a company that provides access to the Internet.

Internet Storm Center – the SANS Institute's early warning centre for detecting rising Internet threats. See website at: *www.isc.sans.org*.

Intranet – that part of an organization's internal network that has the same functionality as the Internet, consists of one or more Web servers, and carries organization-specific information to which only authorized users have access. An intranet is not accessible to unauthorized users or Web surfers.

International Standards (ISO, IEC, ISO/IEC) – as a member of ISO and IEC, BSI has the option of adopting any International Standard as a British Standard, but does not have to do so. If it does, the Standard is republished in the UK as BS ISO, BS IEC or BS ISO/IEC. *See* also ISO *and* IEC.

Intrusion – an attempt to break into or misuse an information processing system, or bypass its security controls, in order to compromise the confidentiality, integrity and availability of information stored on it.

Intrusion detection – a network intrusion detection system is hardware or software that automates the process of monitoring events in systems or networks to detect intrusions. There are different types of intrusion detection systems. A (N)IDS, also known as a 'network sniffer', monitors packets on the network and attempts to discover if a hacker is attempting to break into the system (or cause a denial of service attack). A system integrity verifier (SIV) monitors system files to find when an intruder changes them so as to set up a backdoor. Log file monitors (LFM) monitor log files generated by network services. In a similar manner to (N)IDS, these systems look for patterns in the log files that suggest an intruder is attacking.

IP – Internet Protocol is the most basic protocol for communicating on the Internet.

IP Address – *see* Internet Protocol Address *and* Domain name.

IPR – *see* Intellectual property rights.

IPSec – *see* Internet protocol security.

IP Spoofing – *see* Spoofing.

IRCA – International Register of Certificated Auditors; formed in 1984 as part of the UK government's enterprise initiative, designed to make industry and business more competitive through the implementation of quality principles and practices. This structure included IRCA, an accreditation body (now UKAS), a national standards-making body (BSI Standards) and a number of commercial certification bodies. The IRCA is the world's original and largest international certification body for auditors of management systems. See website at: www.irca.org.

IrDA – the Infrared Data Association's standard for digital infrared connectivity.

ISACA – the Information Systems Audit and Controls Association. Founded in the USA, this is an international association of professionals involved in information systems audit, control, quality assurance and security. It is well known for the computer audit qualification CISA and has chapters all round the globe. See website at: www.isaca.org.

ISBS – *Information Security Breaches Survey* carried out bi-annually by PricewaterhouseCoopers for the UK's DTI.

(ISC)^2 – the International Information Systems Security Certification Consortium. A not-for-profit organization that developed the information security common body of knowledge ('CBK') and a certification programme for information systems security professionals. *See* also ISSAP, ISSEP, ISSMP and SSCP.

ISEB – the Information Systems Examinations Board.

ISMS – *see* Information Security Management System.

ISO – Acronym from the Greek 'isos' (equal to) adopted by the International Organization for Standardization: the world's largest developer of Standards. Its membership comprises the National Standards Bodies of countries around the world.

ISO 17799:2005 – the international code of best practice for information security which underpins and provides guidance for the implementation of an ISMS, specifically, the revised version issued in 2005. It includes individual information security controls, implementation guidance and other information relating to them.

ISO 27001:2005 – the international information security management system specification standard, and particularly the 2005 version.

ISO 20000-1:2005 – the international standard that defines the specification for IT service management, and particularly the 2005 version.

ISO 20000-2:2005 – the international code of practice for IT service management published in 2005.

ISP – Internet Service Provider.

ISSAP – Information Systems Security Architecture Professional® (an $(ISC)^2$ credential).

ISSEP – Information Systems Security Engineering Professional® (an $(ISC)^2$ credential).

ISSMP – Information Systems Security Management Professional® (an $(ISC)^2$ credential).

ITPC – Infosec Training Paths and Competencies. ITPC qualifications offer recognised formal training and development for IT security professionals working for the UK government and related organizations. The scheme develops and supports

infosec core competency profiles for key security roles within UK government and related sectors. ITPC is the 'recommended qualification' for the CESG Listed Adviser Scheme (CLAS) consultants undertaking work for government clients. See website at: *www.cabinetoffice.gov.uk/infosec/*.

IT governance – a framework for the leadership, organizational structures and business processes, standards and compliance to these standards, which ensures that an organization's IT supports and enables the achievement of its strategies and objectives.

J

Java – a programming language from Sun Microsystems that was designed for writing programs (Applets) that include animations, scrolling text, sound effects, games, etc, that can be downloaded from the Web without fear of viruses or other harm to your computer.

JavaScript – a scripting language widely used to create pop-up and pop-under ads, and other functionality, on web pages.

JPEGs – Joint Photographics Experts Group is a compression technique for colour images and photographs and, therefore, how they are saved. There is a future possibility that JPEG viruses might emerge; these are best resisted by doing the basics consistently.

Junk mail – unsolicited commercial bulk e-mail.

K

Kerberos – available free from MIT, this is a network user authentication system based on key distribution (and can be embedded in virtually any other network protocol) that works on both fixed and wireless networks. See website at: *http://web.mit.edu/Kerberos*.

Key – is the value used, in conjunction with an algorithm, to encrypt or decrypt data. A key may be either public (*see* PKI) or private.

Key stroke loggers – software that records key depressions on a computer keyboard; the software can either be installed on the computer (in which case it can be detected by AntiSpyware software) or it can run inside a secret device attached to the computer, in which case AntiSpyware software will not detect it.

Kilobyte – 1024 bytes.

L

LAN – Local Area Network; two or more computers connected, either physically or wirelessly, and able to share resources.

Layered security – multiple layers of security technology and administrative processes working together to provide a level of protection appropriate to the asset being protected; multiple barriers and inbuilt limits to possible damage form part of such a defence in depth. Larger organizations, in particular, need to deploy layered security architectures.

Layer-2 Tunnelling Protocol (L2TP) – security for transmission of sensitive information over unprotected networks.

Legislation – legal requirements applicable in the jurisdiction in which you operate. Reference to various pieces of legislation are contained in this dictionary.

LFM – log file monitor. *See* Intrusion detection.

Licences – any software that is being used is potentially subject to copyright restrictions and it is essential that organizations ensure they have the correct type and number of licences for each software program they use. There are two types of user licence. The first is known as a 'per seat' licence, the second is for 'concurrent users'. Per seat requires there to be a licence for every installation, or instance, of the software; typically, Microsoft Office licences, for instance, are supplied on this basis. Concurrent user allows for a maximum number of simultaneous users and is more normal for shared software, such as some database applications. This enables the client software to be installed on many

machines, but typically the server software is set so that it will not allow more than the licensed number of users to work simultaneously.

Linux – open source software, originally aimed at desktop workstations.

Log files – files that contain logs of specific activity types.

Logical – objects and methods that are apparent to users and/or applications, as opposed to the physical objects and methods upon which they are based; you have to have physical access to a computer before you can have logical access to its folders.

M

MAC – see Media Access Control.

MAC filtering – access permission configuration based on the MAC address of specific network cards.

Mbps – 'megabits per second' is a measure for digital data transfer rates and a megabit in the context of data storage is one million bits.

Macro – A script of actions to automate repetitive tasks.

Macro virus – is a virus that spreads through the macro-scripting language used in Microsoft Office applications.

Mail bomb – Large amount of e-mail data sent to an address to crash the user's e-mail programme or prevent receipt of further messages.

Mail relaying – Attackers use other systems' e-mail servers to send e-mail messages.

Mail server – the server that provides central support for mail clients.

Malware – is any form of 'malicious stuff' that tries to clog up your computer. It includes adware, spam, spim, spyware, viruses, worms, Trojans and automated exploits, using e-mail attachments, instant messaging, unprotected Internet connections and browsers. See Scumware.

'Man in the middle' – a hacker places himself undetected between two parties to an Internet transaction, whether on a LAN, an unsecured Internet link, a WLAN or on a cellular telephone network. The hacker intercepts and reads messages between the two parties and can alter them without

the intended recipient knowing what has happened. This is often recognized as a form of masquerading; *see* also Evil Twin.

Masquerading – a hacker will pretend to be a legitimate user, trying to access legitimate information, using a password or PIN that was easily obtained or copied, and will then try to access more confidential information or execute commands that are not usually publicly accessible. *See* also Evil Twin.

Media Access Control – every WiFi device has a unique MAC number allocated by its manufacturer. A wireless AP can be programmed to accept only certain MAC addresses and to block all others. While this is relatively simple for a SoHo network (Small Office, Home office), it can be time-consuming to set up and maintain in a large corporate network. It is also possible for a hacker to spoof a MAC address.

Mega byte – 1024 kilobytes.

Memory stick – a portable memory device, designed to access a computer through a USB port.

Microsoft – A software company best known for the Windows operating system. Their products include NT4, Win 2000, Office, Explorer, XP, Server2003 etc.

MIME – Multipurpose Internet Mail Extensions is a specification that provides a standard method for attaching to basic e-mail messages additional files such as pictures, audio and application files.

Mobile code – programs that are sent in one version only to a heterogeneous collection of processors and are executed with the same semantic on each of those processors without explicit installation or execution by the recipient.*

Mobile phones – surely everyone knows what these are?

Mobile worker – this is someone who doesn't work from a fixed geographic location and whose job requires them to spend a substantial amount of time out of the office, 'on the road' or travelling. Mobile workers use laptops (increasingly connecting through wireless HotSpots), mobile phones and PDAs to keep in touch with their offices and homes.

Modem – a Modulator/de-modulator is a device that enables a computer to transmit data over analogue telephone lines.

MP3 – MPEG Audio Layer-3 is the standard for compressing and storing files, typically music.

MPEG – Moving Pictures Experts Group is a standard for digital video and audio compression.

MSN Messenger – is Microsoft's Instant Messenger service.

Multiple sign-on – a user within an organization who is authorized to use multiple applications and services would have to sign on individually to each one, unless the organization uses single sign-on software.

N

NDA – a non-disclosure agreement is a legal agreement that sets out the specific terms on which one party will share confidential information with another; it includes an agreement by the second party not to disclose or otherwise use any of the information made available under the terms of the NDA.

Netspionage – is corporate espionage, carried out online.

Network – a number of computers (at least two) linked together, either with or without central servers.

Network monitoring – this is also known as 'sniffing' and involves deploying some code on the Internet to monitor all traffic in order to look for passwords. These, and other ostensibly confidential information, are often sent across the Internet 'in the clear' and, therefore, can easily be located and written to the hacker's workstation for future use. When this technique is used to try to detect hacker activity it is called intrusion detection.

Network perimeter – *see* Perimeter.

Network sniffer – *see* Intrusion detection.

Non-disclosure agreements – *see* NDA.

Non-repudiation – a cryptographic method of providing the sender of data with proof of delivery and assuring the recipient of the sender's identity, so that neither can later deny that the data was transmitted. This is critical in e-commerce.

NSB – A National Standards Body, usually a country's largest producer of formal Standards. An

NSB also represents the interests of its country in European and international forums.

NSSF – The National Standardization Strategic Framework, a programme designed to increase awareness of, and engagement in, standards and standardization. See website at: *www.nssf.info/index.xalter*.

O

Objective evidence – data supporting the existence or verity of something.

Online payment systems – a number of organizations offer third party payment services. The best known are: WorldPay, PayPal, Amazon.com Payments, Yahoo! PayDirect, and VeriSign Inc.

OS – *see* Operating system.

Open source – software whose code is open for anyone to look at and modify. Linux is a well known type of open source software. See website at: www.opensource.org.

Operating system (OS) – the OS is the software that controls how a computer uses its memory, disk space, folders and files, desktop, etc. Microsoft Windows and Apple Macintosh are the two most popular proprietary operating systems. There are also open source operating systems.

Opt-in – an option in marketing campaigns that enables individuals to explicitly consent to participate now or in future.

Opt-out – an option in marketing campaigns that enables individuals to explicitly decline to participate now or in future.

Outlook – the Microsoft e-mail client.

Outlook Express – the cut-down version of Outlook, designed for home users.

OWASP – the Open Web Application Security Project (www.owasp.org) specifies the top ten application vulnerabilities that an organization should secure.

P

Packets – these are the standard unit(s) for data sent across the Internet. Data is broken up into packets, which allows multiple transmissions to share the same line, and they are routed back together again at the destination and are placed back in their original order.

Pairing – when two Bluetooth devices establish a secure, trusted relationship.

PAP – Password Authentication Protocol is a login security protocol that is less secure than CHAP because the password is sent to the client as clear text. *See* CHAP.

Parental control – this is software that is designed to enable parents to scan, filter and control the websites visited by their children, to protect them from objectionable content.

PAS – Publicly Available Specifications were originally documents written by BSI in conjunction with external organizations, with a view to supporting certification schemes. The designation has since been widened to include privately commissioned 'standards' published by BSI as part of its Professional Standards Service. See website at: *www.bsi-global.com*.

Passwords – a string of characters entered to a computer, an application or a network by a user to verify their identity as the owner of a specific username.

Password cracking – is, on balance, very easy. Most users do not set up passwords or, if they do, they use very simple passwords that they can easily remember, like 'secret' or 'password', or their children's

names, or birthdays, sports teams, or particular anniversaries, or family names. While some hackers can quickly identify particular user's passwords, software is now available on the Internet that will apply 'brute force' to automatically, and at high speed, try every theoretically possible alphanumeric combination of user name and password and, usually aided by a dictionary (a 'dictionary attack') of common passwords, this can quickly enable a hacker to gain access to a system. Once a hacker locates the list of encrypted user passwords on the security server, he can use Internet-available software tools to decrypt it.

Patch – an update to a file that replaces only parts of the file, rather than the whole file.

Payload – the damage or other malicious activity that a virus, worm or spam causes.

PDA – a Personal Digital Assistant is a device that stores digital contact, diary and other data; it may also store e-mail and be capable of communicating (either wired or wirelessly) with a computer or a network. A Blackberry is a form of PDA that has mobile phone connectivity and exists specifically to handle e-mail while on the move.

PDF – Portable Document Format is a file extension indicating that a document has been saved in Adobe's proprietary format.

Peer-to-peer – a network connecting two or more computers directly to one another, without using a central file server.

Penetration testing – this is the organized process of assessing the full range of threats to an organization and setting out deliberately to infiltrate and penetrate its systems, using any and all methods,

from technological hacking through to social engineering.

Perimeter – the organization's boundary has both physical and logical aspects. In information security terms, the perimeter is where you draw the line, the line beyond which only authorized and authenticated users may go. In today's business environment, that perimeter is increasingly a mobile one.

Personal data – that information about a living person (ie, not an organization) that is protected by legislation and regulation.

Personal Digital Assistants – see PDAs.

PGP – Pretty Good Privacy is a public key encryption program that enables files or messages to be exchanged with confidentiality and authentication.

Pharming – Criminal activity resulting in users being redirected from entered, correct website address to a fake website.

Phishing – sending e-mails that falsely claim to come from a legitimate company in an attempt to scam users into surrendering information that can be used for identity theft.

Physical security – is security that is effective in the analogue world.

PIN – Personal Identity Number.

Piracy – illegal use or duplication of material covered by copyright or other intellectual property rights.

PKI – Public Key Infrastructure is the combination of standards, protocols and software that supports public key encryption.

PKIX – the Public Key Infrastructure (PKIX) working group of IETF has been taking forward work on the definition of a standard, interoperable Public Key Infrastructure and on fostering usage of public key security services.

Platforms – a hardware and software combination (eg, Windows XP on an Intel PC).

Pop-ups and pop-downs – small windows that appear when users visit some websites, pop-ups are the windows that pop up, pop-downs do it in the other direction.

Policy – overall intention and direction as formally expressed by management.*

Ports – hardware ports are connection points for cables; logical (or virtual) ports are access points for protocols.

PowerPoint – Microsoft's slide presentation application.

PPTP – the Point-To-Point Tunnelling Protocol provides security for transmission of sensitive information over unprotected networks.

Privacy – the control that individuals have over the collection, use and distribution of their personal, private information.

Private key – one of two keys used in public key encryption. This key is kept private and secret, and used to encrypt data prior to transmission or to decrypt data that has been encrypted with the corresponding public key. *See* Public key.

Privileges – a privilege is any facility in a multi-user system that enables one user to override system or application controls. Inadequate control of privileges invariably leads to their inappropriate use; equally

invariably, this abuse leads to system security breaches and is a major contributory factor in system failures. The most critical privileges are those which enable system administrators to do their jobs.

Problem – unknown underlying cause of one or more incidents.****

Procedure – a set of specific, sequential steps.

Process – a series of related activities; a process might consist of a series of procedures.

Project governance – the framework and rules for controlling how project decisions are made and project activity monitored.

Protocol – a set of rules that govern an activity or process.

Proxy server – this is a server that sits between a client (eg, a browser) and a real server, or between an organization and the Internet. It improves performance by filling a request directly rather than forwarding the user to the Internet if the necessary information is available. Proxy servers can also block unauthorized activity, whether outgoing or incoming (*see* Firewall).

P2P – *see* Peer-to-peer.

Public key – one of two keys used in public key encryption (*see* Asymmetric encryption). The public key is released to the public, and used to encrypt data prior to transmission to the holder of the private key or to decrypt data that has been encrypted with the corresponding private key. It can also be used to verify the user's digital signature. *See* Private key.

Public key encryption – *see* Asymmetric encryption.

Public terminals – computer terminals that are in a public area and are designed for access by non-specific users.

R

RADIUS – a Remote Authentication Dial-In User Service is a protocol for administering and securing remote access to a network. It needs an authentication server, client protocols and an accounting server, all of which can be mounted on a single machine. The RADIUS authentication server validates the user credentials (user name and password) before allowing access. It can provide different levels of user privileges. It does not provide encryption.

RAID – a Redundant Array of Inexpensive Disks uses an array of disks instead of one large expensive one. A single disk in the array can be removed and the data remains safe. RAID level 5 provides the highest level of safety.

Reboot – this is what you have to do after your computer has crashed.

Record – document stating results achieved or providing evidence of activities performed.**** In ISO 20000 records are distinguished from documents by the fact that they function as evidence of activities, rather than evidence of intentions.

Recovery – this is what you have to bring about after an incident that interrupts business continuity, eg, a system failure may mean that data is lost and has to be recovered from the backup tapes.

Recycle bin – the Microsoft desktop folder into which deletions go. They stay there until you remember to go and empty the deleted items folder. Until you empty this folder, any files in it can be dragged back into use.

Registrar – Americanism for certification body; *see* Third party certification body.

Regulation of Investigatory Powers Act 2000 (RIPA) – has two important provisions. Section 1 makes it unlawful to intentionally intercept communications over a public or private telecommunications network without lawful authority. Section 3 allows a defence if it can be reasonably believed that both parties consented to the interception.

Regulatory standards – are mandatory standards, developed by interested parties and national representatives, and often associated with safety issues.

Release – a collection of new and/or changed configuration items which are tested and introduced into the live environment together.****

Reliability – minimal maintenance, minimal manpower requirements, maximum resilience.

Remote access – is system access by a remote user.

Remote control software – software that a remote user deploys via a remote access port to control a computer.

Remote desktop – a system allowing one computer to display the screen of another and operate it remotely.

Remote user – someone who is not within the organizational perimeter. This is the general category to which teleworkers and mobile workers belong. Remote users can also be technicians who need to access server software to carry out repairs or maintenance; they could also do other things, as could anyone else who finds the remote access port.

Removable media – storage devices that can be detached from the computer.

Reputation damage – this is what can happen when information about a serious information security incident gets into the public domain. It can be very costly for individuals and for organizations.

Request for a change – a form or screen used to record details of a request for a change to any configuration item within a service or infrastructure.****

Residual risk – is the risk remaining after risk treatment.***

Resilience – is the ability to bounce back when attacked.

Retrovirus – a virus that attempts to disable anti-virus software.

RIPA – see Regulation of Investigatory Powers Act.

Risk – combination of the probability of an event and its consequence.*

Risk acceptance – decision to accept a risk.***

Risk analysis – systematic use of information to identify sources and to estimate the risk.*

Risk appetite – an organization's overall attitude to risk. The balance between risk and return and the trade-off between security and flexibility is usually a strategic decision by the organization's board.

Risk assessment – overall process of risk analysis and risk evaluation.*

Risk avoidance – decision not to become involved in, or action to withdraw from, a risk situation.***

Risk classification – the classification of a risk as low, medium or high depending on the risk assessment.

Risk communication – exchange or sharing of information about risk between the decision-maker and other stakeholders.***

Risk control – actions implementing risk management decisions.***

Risk criteria – terms of reference by which the significance of risk is assessed.***

Risk evaluation – process of comparing the estimated risk against given risk criteria to determine the significance of the risk.*

Risk log – this is produced through a risk analysis process and is the record of all the organization's assets, together with their threats, vulnerabilities, impacts, probabilities and risk classification. The risk log should include all the information assets of the organization.

Risk management – co-ordinated activities to direct and control an organization with respect to risk (and usually includes risk assessment, risk treatment, risk acceptance and risk communication).*

Risk management system – the set of elements of an organization's management system concerned with managing risk.***

Risk reduction – actions taken to lessen the probability, negative consequences, or both, associated with a risk.***

Risk transfer – sharing with another party the burden of loss, or benefit of gain, for a risk.***

Risk treatment – process of selection and implementation of measures to modify risk.*

Risk treatment plan – the overall plan for risk treatment, reflecting the corporate risk appetite.

Rogue dialler – a dialler that dials unintended numbers (typically premium rate).

Root – an administrative user account with special privileges.

Root access – gaining access to a computer as a root user.

Router – a device that connects a number of computers together or to the Internet.

S

SANS – the SANS (SysAdmin, Audit, Network, Security) Institute was established in the USA in 1989 as a cooperative research and education organization. It enables more than 165,000 security professionals, auditors, system administrators and network administrators to share the lessons they are learning and find solutions to the challenges they face. SANS is supported by security practitioners in government agencies, corporations and universities around the world who invest hundreds of hours each year in research and teaching to help the entire information security community. See website at: *www.sans.org*.

SANS top 20 – a list of the 230 most important vulnerabilities in current software, that should help organizations prioritize their patching activity. See website at: *www.sans.org/top20*. *See* also CVE *and* Bugtraq.

Scumware – *see* Malware.

Screen saver – a program that displays an image (blank or moving) on a computer screen after the computer has had no input for a period of time. Originally designed so that images wouldn't be burned into old cathode ray tube screens, they have become entertaining.

Script kiddie – is not as sophisticated as a hacker and so hasn't yet qualified for a hat but, using their own very simple code or, more usually, programmes found on the Internet, they can be just as lethal to unprotected systems as real hackers. Quite often, script kiddies are found in IT departments where their interest in testing the systems they are employed to protect can take them beyond the law.

Scumware – a collective term for forms of intrusive and/or destructive software including adware, spam, spim, spyware, viruses, worms, Trojans and automated exploits, using e-mail attachments, instant messaging or software that has legitimate uses but which violates privacy or is obnoxious or intrusive in some way. *See* Malware.

Search Engine Optimisation (SEO) – is the process of making website content more search engine friendly to make it rank higher.

Secure HTTP – *see* HTTPS.

Secure Electronic Transaction (SET) – is a protocol, developed jointly by Visa and Mastercard, for enabling secure, cost-effective bank and credit card transactions over open networks. SET includes protocols for purchasing goods and services electronically, for authorizing payments, and for requesting and obtaining digital certificates.

Secure Sockets Layer (SSL) – is a handshake protocol that provides security and privacy to Internet transactions. It is application independent: after an SSL session starts, other protocols (like HTTP and FTP) can be layered transparently on top of it. It has become one of the most popular security protocols on the Internet. Installation of a server ID, or digital certificate, will automatically activate SSL on the server and this enables that website to communicate securely with any visiting browser. Client and vendor servers are able to authenticate one another automatically. Once this is complete, SSL will encrypt all communication (data such as credit card numbers and other personal information) between the web server and the visiting browser with a unique session key. The session key is not used again. SSL was designed to ensure that, even if information is intercepted, it cannot be viewed by

someone who is not authorized to do so. The default settings in browsers should identify sites that are not secure and should warn that information submitted could be intercepted or observed by a third party. This warning does not appear where there is a valid SSL connection. There are other signs that there is an SSL connection: the URL will change from http to https and a closed padlock will appear in the bar at the bottom of the browser window.

Security – what you get when you have secured something.

Security Centre (Windows XP SP2) – this is the single control point for the Windows Internet security features, from which the firewall, anti-virus software, automatic update service and Internet options can be controlled. It can be accessed through the Control Panel.

Server – a computer on a network that stores shared information or which handles common tasks for a number of client computers.

Server farm – (also, server cluster) a collection of networked, load-balanced servers in a single secure site that are capable of accomplishing more than a single server through task distribution. This also helps provide operational redundancy back-up.

Service desk – customer-facing support group who do a high proportion of the total support work.****

Service level agreement (SLA) – written agreement between a service provider and a customer that documents services and agreed service levels.****

Service management – management of services to meet the business requirements.****

Service packs – the cumulative product and security software updates (usually including all previous hot fixes, security updates and patches) which need to be downloaded from the supplier's website in order to keep the product up-to-date.

Service provider – the organization aiming to achieve ISO/IEC 20000.**** For those looking to interpret the phrase where it is used in ISO/IEC 20000

SET – *see* Secure Electronic Transaction.

Shareware – is software that is provided on the basis that, if the user likes it, the user will pay something for it. You can share this software with friends, but they too are expected to make a contribution.

Signature – the 'fingerprint' of a virus that is used by anti-virus software to detect infectious files.

Single sign-on (SSO) – is a means of passing user credentials between applications without the user having to authenticate each time they seek to use another application for which they are authorized.

SIV – system integrity verifier. *See* Intrusion detection.

SLA – *see* Service level agreement.

Smart cards – credit-card sized devices that have an embedded chip containing a small amount of data that, together with an access code, enables a user to be authenticated. Smart cards can store digital certificates, private keys, public keys and passwords.

Smart phones – mobile phones that combine mobile phone functionality with that of a PDA; the user can talk to others, send and receive text and voice messages as well as send and receive e-mail, and store calendar information and other data.

Smart token – this is a USB device that contains a computer chip that securely stores information about users and supports authentication, digital signatures and biometrics; when used in conjunction with a strong password, smart tokens make possible two-factor authentication.

S/MIME – Secure MIME adds security features such as digital signatures and encryption services to the basic MIME specification, thus protecting the privacy of e-mail and its attachments.

Snarfing – *see* Bluesnarfing.

SoA – *see* Statement of Applicability.

SOA – Service Oriented Architecture. A software architectural framework that links or integrates applications independently of the underlying operating system in order to deliver business-oriented services across the network to end users (which may also be other systems).

Social engineering – is the easiest and most common method of gaining access to a network, tricking someone into providing confidential information. The hacker, for instance, poses as a network administrator or a fellow employee, with an urgent problem, which can only be resolved by the employee providing confidential information (such as user name or password). Alternatively, the hacker has a false business card, claiming to be a key technical or business support representative, or claims to be a new employee trying to get up to speed in the business. Passwords should NEVER be divulged to anyone, anywhere, for any reason, under any conditions. NOT EVER. This is one of the most important, fundamental and basic security rules.

SOHO – Small Office, Home Office.

Spam – unsolicited commercial bulk e-mail, or junk mail.

Specification – contains the word 'shall' and defines what is mandatory for a system if it is to comply with a standard. eg, it sets out the requirements for designing an ISMS, not what should be in it. Accredited certification takes place against the requirements of a specification.

SPIM – spam sent through an Instant Message.

Spoofing – comes in two forms. IP spoofing gains unauthorized access to a system by masquerading as a valid Internet (IP) address. Web spoofing involves the hacker re-directing traffic from a valid web address to a fraudulent, look-alike website where customer information (and particularly credit card information) is captured for later illegal reuse. *See* also Phishing.

Spyware – is any software that, without your explicit consent, shares information about you with a third party on the Internet.

SSCP® – Systems Security Certified Practitioner. The SSCP certification is for information security technicians who have implementation experience. The SSCP credential is ideal for those working toward or who have already attained positions as Senior Network Security Engineers, Senior Security Systems Analysts or Senior Security Administrators. *See* $(ISC)^2$.

SSID – Service Set Identifier is the name that uniquely identifies a LAN. Wireless devices need to know the SSID of a WLAN before they can connect to it.

SSL – *see* Secure Sockets Layer.

SSL VPN – *see* Virtual Private Network.

Standardization – the full process of identifying the need for, designing, implementing and revising a standard.

Statement of Applicability (SoA) – document describing the control objectives and controls that are relevant and applicable to an organization's ISMS, based on the results and conclusions of the risk assessment and risk treatment processes.**

Steganography – or digital watermarking, a method of hiding information in other data, such as voice communications, visual images, and music, in order to provide forensic evidence of copyright ownership and trace the source of infringing material.

Strong authentication – *see* Two-factor authentication.

Surf control – is a software technology designed to allow blocking to surfers of particular sites, or groups of sites. Parents can use it to protect their children from offensive or dangerous sites, and organizations can use it to deter their employees from visiting illegal or undesirable sites, or doing other undesirable things. Different filters and different environments mean that different packages are deployed for each type of control. In the UK, organizations should only deploy surf control technology in the workplace in conjunction with an Acceptable Use policy. *See* Acceptable Use policy.

Symmetric – 'correspondence of parts'. Typically used to describe a process or arrangement that mirrors another.

Symmetric encryption – uses same key (or code) to encrypt and decrypt information – *see* also Data Encryption Standard *and* Asymmetric encryption.

System – any combination of hardware and software used for processing information and which has a data entry point and a data exit point. A system consists of a number of components. A single data asset (such as a file, whether electronic or paper) is a component of a system.

System access controls – are controls that restrict access to information processing systems through a combination of guidelines and technological security measures that implement those guidelines.

System utilities – software programs that perform a specific task, usually related to managing system resources.

T

TACACS+ – Terminal Access Controller Access Control System + is an authentication protocol that has replaced and is not compatible with TACACS.

Tampering – unauthorised altering of the contents of information packets, either in transit or stored on a network.

TCP/IP model – Transmission Control Protocol/Internet Protocol is a suite of communications protocols used to connect host computers on the Internet. TCP/IP is the de facto standard for transmitting information over networks.

Teleworker – this is someone who works primarily from home. The description originated with the idea that someone who didn't physically need to be in the office could work from home and keep in touch when necessary by telephone. Nowadays, a teleworker is likely to need a fully set up electronic home office, including a workstation, multipurpose printer/copier/scanner, broadband Internet connection, fax machine, wrist rests, screen guards and so on.

Terminal – the screen and input device through which a computer system can be accessed.

Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 – were issued under the authority of RIPA. They allow employers to monitor employee communications where the employee has not given express consent, provided that the monitoring meets specific criteria. *See* RIPA.

Third party – that person or body that is recognized as being independent of the parties involved, as concerns the issue in question.*

Third party certification body – an independent organization with the necessary competence and reliability to award certificates following verification of conformance. It is wise to check the accreditation status of such bodies before appointing them.

Threat – a potential cause of an unwanted incident, which may result in harm to a system or organization.*

TickIt – an ISO 9000 compliant standard for software development processes.

TKIP – the Temporal Key Integrity Protocol is a data-confidentiality protocol designed to improve the security of legacy products running WEP. *See* WEP.

Token – a physical object used to authenticate a user. *See* also Smart token.

Traffic – the transmission of packets of information over a network effecting communication between computers.

Trojan – a Trojan is hostile code concealed within, and purporting to be, bona fide code. It is designed to reach a target stealthily and to be executed inadvertently. It may have been installed at the time the software was developed. They can be programs that, while perhaps appearing to be a useful utility, are designed to secretly damage the host system. Some will also try to open up host systems to outside attack.

Trusted – securely configured and therefore not expected to be the source of malicious activity. *See* also Untrusted.

Turnbull Report – *Internal Control: Guidance for Directors on the Combined Code* was published by the Internal Control Working Party of the Institute of Chartered Accountants in England and Wales. It sets out how directors of listed companies should tackle the Combined Code issue of annually reviewing all their controls, 'including financial, operational, compliance and risk management'. Available via: *www.frc.org.uk/corporate/internalcontrol.cfm*.

Two-factor authentication – authentication that requires two different methods (eg, a smart card or biometrics plus a password) of identifying a user, both of which must match the credentials set up in the system for that user.

U

UKAS – United Kingdom Accreditation Service: the sole national accreditation body recognised by the UK government to assess, against internationally agreed standards, organizations that provide certification, testing, inspection and calibration services. See website at: *www.ukas.com*.

Untrusted – (or not trusted), a device (usually) that is not, or cannot be assumed to be, securely configured and not subject to malicious action.

Update – 'a broadly released fix for a specific problem addressing a non-critical, non-security-related bug' – Microsoft.

Update services – *see* Automatic updates.

Upgrade – a newer version of an already installed software package; the upgrade process should leave existing data and user preferences intact while replacing the existing software with a newer version.

UPS – an Uninterruptible Power Supply is a device which is designed to keep other electrically powered devices operating when the normal power supply fails. A UPS should, at the very least, be rated as capable of meeting the power requirements of the device(s) it is supporting for long enough to allow an orderly shut down of the services. The length of time required for this may need to be ascertained by testing.

URL – the Uniform Resource Locator is the address of a website on the World Wide Web.

USB – the Universal Serial Bus is a computer standard designed to eliminate the guesswork in connecting peripherals to computers.

USB stick (or flash card) – is a portable memory device with a USB.

Usenet – Internet-based public bulletin board that allows users to post messages to different news groups.

User – an individual or an automated process or system that has access rights to a specified system.

User account – a set of rules defining an individual's access to files and systems on a computer.

User agreement – this is the formal, standard document that all new users should be required to sign before they are issued with their user name. This agreement should describe their access rights and should set out the organization's requirements around system use, password choice and protection.

User ID – *see* User name.

User name – every user should have a specific and unique name for use on the system. This name should be created and allocated in line with a standard procedure and should be set up on the system with specific access rights and privileges. The user name has to be created before the user can access the system for the first time.

User rights – the specific application access rights associated with a specific user name.

V

Validation – confirmation, through provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled.

VAR – a value-added reseller.

Vector – in computing, this is the method that malware uses to propagate itself.

Verification – confirmation through the provision of objective evidence that specified requirements have been fulfilled.

Virtual Private Networks (SSL, IPSEC) – a Virtual Private Network is an encrypted tunnel over a public network which provides privacy as good as that available on a private network. It consists of encrypted and authenticated logical (not physical) links across shared or public networks that are used to provide remote links to an organizational network. A VPN server within the organizational perimeter encrypts data sent to a VPN client outside the perimeter, and vice versa. *See* Internet protocol security *and* Secure Sockets Layer.

Virus – a virus is a piece of computer code that is designed to make your computer sick. Like biological viruses, it indiscriminately selects and infects those whose defences are weak or non-existent. Technically, a virus has at least two properties: it is a program capable of replicating, ie, producing functional copies of itself, and it depends on a host file (a document or executable file, shared by e-mail or Instant Messenger) to carry each copy. It may or may not have a 'payload', the ability to do

something funny or destructive or clever when it arrives.

- There are some 100,000 known viruses in the wild. These range from primitive bits of code written at the dawn of computing time, and from which almost all computers are now completely immune, to more destructive creatures like 2004's MyDoom, Slammer, Sobig (with all its variants) and Bugbear. Up-to-date anti-virus software protects against all of these, without you ever having to know what they do or how they work.

- Viruses exploit software faults (vulnerabilities) to attack computers and their payloads range from silly messages to individual keys becoming inoperative to the complete death of your computer.

- The same virus doesn't always have the same name with every anti-virus vendor. This is very irritating and it reflects the fact that the same virus is usually discovered, analysed, reverse- engineered and the appropriate anti-virus signature update produced by a number of competitive vendors working in parallel, each of them having allocated the virus their own version of the name.

- Most viruses attack Microsoft products, not just because Microsoft products are full of flaws (vulnerabilities) but because they are the most widely used computer software programs in the world, installed on more than 90% of desktops. Computer viruses spread by harvesting e-mail address books and forwarding themselves to everyone you know in an e-mail that is identified as having come from you – a good way of losing friends and business contacts.

- It's not just Microsoft, though. *All* software has vulnerabilities, even the open source versions. Visit Bugtraq (*www.securityfocus.com/archive/1*) or CVE (*http://cve.mitre.org/*) to get a techies-eye view of the range of software vulnerabilities that can be exploited by virus and worm writers.

- And it's not just workstations and computer networks that have virus challenges: increasingly, PDAs and cellphones are coming under attack and, as they too need to connect to the corporate network, they too need to be protected.

- Virus writers intend to exploit vulnerabilities in their target software and, as soon as a weakness is identified, the race is on to exploit it – and to see it off. The speed with which new viruses are developed is increasing – it is now only a matter of days between the announcement of a vulnerability and the appearance of the first virus exploiting it.

Virus hoax – there are people out there who think it's dead funny to send e-mails to everyone they know, warning of a virus that isn't one. Frankly, if a real or important new virus existed that you had to hear about from some acquaintance rather than from your anti-virus company, you've either chosen a very poor anti-virus supplier (if you have one at all) or you're being hoaxed. If you're reading this book, the chances are that it will be the latter. The website: *http://vmyths.com/index.cfm* is a good place to go if you really want to be sure that a message you've received is a hoax.

Virus writers – 'people' who write viruses; they should be taken outside and have unspeakable things done to them. Mostly, they are sad people who do it for fun and because they enjoy the challenge of writing clever code. Sometimes they do it out of loneliness, or because they want to have some impact

on the world. They often work together and have online groups, websites and communities through which they share work and ideas. They also compete with one another and certainly their relationship with anti-virus companies is often extremely hostile. Virus toolkits are available online, so that anyone with limited code writing skills can also create a virus.

VoIP/VOB – Voice over IP/Voice over Broadband is a technology that enables voice-to-voice communication across the Internet.

VPN – *see* Virtual Private Network.

Vulnerability – a weakness of an asset or group of assets that can be exploited by a threat.* There are regularly updated central stores of known vulnerabilities at Bugtraq (*www.securityfocus.com/archive/1*), CVE (Common Vulnerabilities and Exposures: *http://cve.mitre.org/)* and in the SANS top 20 (SANS (SysAdmin, Audit, Network, Security) Institute: *www.sans.org/top20/*).

Vulnerability assessment – this is the (usually automated) evaluation (or vulnerability scanning) of operating systems and applications to identify missing fixes for known problems so that the necessary fixes can be installed and the systems made safe.

Vulnerability scanning – an automated process of scanning a network or a series of information assets to establish if they display any of the characteristics of known vulnerabilities.

W

WAN – see Wide Area Network.

War chalking – the Great Depression era hobo-style practice of using chalk to physically mark 'hotspots' from which (usually) unauthorized access to nearby wireless networks can be achieved. This has now been largely superseded by Internet-based location lists of available unsecured (open) wireless networks. See, for example, *www.wifinder.com* and *www.wardrive.net/general/hotspots*.

War dialling – a computer program (usually freeware or shareware) used by hackers to identify phone numbers that can connect to a computer modem. The program automatically dials a defined range of phone numbers and then records in a database those numbers that connect successfully. Some programs can also identify the computer's OS and may also conduct automated penetration testing by running through a predetermined list of common user names and passwords in an attempt to gain access to the system.

War driving – the practice of driving around business or residential areas, scanning for wireless networks. Any computer that is wireless enabled can be used for this purpose, although there are a number of software tools and peripherals that substantially improve the speed, accuracy and covertness of this activity. Netstumbler is a well known war driving kit that is inexpensive and readily available..

WARP – Warning, Advice and Reporting Point, a community that uses a website, e-mail, telephone, text messages, and occasional meetings (where possible) to send a personalised service of IT

security warnings and advice to members (See website at: www.warp.gov.uk).

Web — *see* World Wide Web.

Webcam – a digital camera that transmits images over the Internet.

Web mail – an e-mail service that sits on a web server and is accessible through a browser.

Web master – the person, in an organization, who is responsible for the configuration and maintenance of the organization's web servers and web presence .

WEP – Wired Equivalent Privacy is a protocol in the IEEE's original 802.11 standard for wireless networking that was designed to tackle the vulnerability that comes from data sharing radio waves. It has many flaws and should not be relied on to provide adequate security.

White hat – a non-criminal hacker.

Whitelist – the list of people that you positively want to receive e-mails from.

Wide Area Network – a network of two or more LANs, connected through physical links (leased lines or the telephone system) or satellites. The Internet is the largest WAN in existence. *See* LAN.

WiFi – Wireless Fidelity is the name given to wireless networking that meets a number of standards promulgated by the IEEE. Those most commonly encountered are 802.11a, 802.11b (the original WiFi), 802.11g and 802.11i.

- **802.11** – the IEEE's tag for a family of standards for wireless LANs, broken down into a number of different versions, adopted at different times.

- **802.11a** – is the wireless standard operating at 5 GHz and running at up to 54 Mbps. This was the second wireless standard adopted. It is not compatible with the other wireless standards, has a comparatively short range, at 30 metres, and is mostly used in office environments.

- **802.11b** – is the wireless standard that was originally known as WiFi. It operates at 2.4 GHz and at up to 11 Mbps. It has been widely adopted and is the most widely available and used, is compatible with 802.11g and has a maximum outdoor range of about 120 metres and 50 metres indoors.

- **802.11g** – is the wireless standard operating at 2.4GHz but running at 54 Mbps; it is compatible with 802.11b but is five times faster. An 802.11g device can access an 802.11b HotSpot, but will run at the slower speed.

- **802.11i** – is the wireless standard that uses AES, a more secure method of handling authentication. This version was specifically developed to tackle the security issues that had emerged with earlier versions and has only recently become commercially available.

- **802.1X** – should not be confused with any 802.11 standards. 802.1X provides a framework for authenticating and authorizing devices connected to a network and would usually involve an authentication server. It improves security by automatically and dynamically changing encryption keys more quickly that any hacker can crack them.

WiFi Alliance – this is an independent, non-profit organization that certifies WiFi product interoperability and operates the WiFi Zone HotSpot programme. See website at: *www.wi-fi.org*.

WiFi certified – means that the product has been certified by the WiFi Alliance to be interoperable with whichever 802.11 (usually a, b and g) wireless standards it claims. *See* WiFi.

WiFi Zone – the WiFi Alliance operates a programme to identify and mark public APs with a standard logo, supported by a website that identifies, worldwide, the location of local WiFi hotspots. The website is at: *www.wi-fizone.org*; it can be accessed by WAP phone (on *http://wap.wi-fizone.org*) to easily identify a nearby, local WiFi Zone hotspot.

'Wild' – this is the digital online world, the place where viruses and worms spread, beyond human control.

WiMax – the next generation of wireless technology, with wireless ranges of up to 10 miles and broadband speeds. The first technology is in the pipeline (see *http://wimaxxed.com*).

Wireless – a communication method that does not rely on cabling of any sort – *see* WiFi.

Wireless LAN – a local area network consisting of a number of wireless clients accessing a fixed network (eg, an Internet backbone) through a wireless access point.

WLAN – see Wireless LAN.

Workstation – a computer that has a mass storage device (hard drive) and a large, high resolution screen and uses an operating system that provides a graphical user interface (GUI).

World Wide Web – this is an information-sharing construct that sits on top of the Internet, and uses HTTP to transmit data. It is *not* synonymous with the

Internet. A browser is required for accessing web content. *See* Internet.

Worm – unlike a virus, a worm is autonomous. It does not rely upon a host file to carry it. It can replicate itself (ie, it is self-propagating), which it does by means of a transmission medium such as e-mail, Instant Messaging, Internet Relay Chat, network connections, etc. Polymorphic worms are capable of evolving in the wild, so that they can more effectively overcome evolving virus defences.

WPA – WiFi Protected Access, a more secure version of 802.11 that uses TKIP. *See* WiFi *and* TKIP.

WPA2 – the interoperable version of WPA.

X

XML – Extensible Markup Language is a flexible method of creating common information formats and sharing them across the Web.

Z

Zero day exploit – this is an exploit that takes advantage of a vulnerability on the same day that it is announced (or becomes generally known). Anti-virus companies and software manufacturers have zero days' grace in which to develop and launch a fix or a patch.

Zip – compressing data to a format that uses less memory than in the unzipped state.

Zombie – this, as you might expect, is a once independent computer that is now under the discretionary, malign control of another computer somewhere else in the world. A remote user can take advantage of inadequate anti-virus and firewall defences to install remote control software on other computers. This remote control software enables the remote user to use your computer (without you even being aware of it) for the mass forwarding of spam or as part of a massive, co-ordinated attack on another website (a Distributed Denial of Service attack). In the long run, the future of electronic communication depends on every computer being sufficiently well protected that none can be used as zombies. *See* Distributed Denial of Service Attack.