WISER
Wide-Impact cyber SEcurity Risk framework

Cyber Security guide for novices

According to UK Government research, **74% of small firms** in the UK experienced a cyber security breach last year, and **90% of large firms** were also targeted. Some incidents caused millions in damages.

This guide is for SMEs and small IT teams in public administrations as a first step to understanding the essentials of cyber risks and how to manage them effectively.

Cyber attack – deliberate exploitation of computer systems, digitally-dependent enterprises and networks to cause harm.

Cyber incident – an occurrence that actually or potentially poses a threat to a computer, internet-connected device, or network, or data processed, stored or transmitted on those systems, which may require a response action to mitigate the consequences.

Cyber resilience – the overall ability of IT systems and organisations to withstand cyber events and, where harm is caused, recover from them.

Cyber security – the protection of internet-connected systems, including hardware, software and associated infrastructure, the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system or accidentally, as a result of failing to follow security procedures or being manipulated into doing so.

Cyber security risk assessment – identifies the gaps in your organisation's critical risk areas and determines actions to close those gaps. It also ensures that you invest time and money in the right areas and do not waste resources.

Cyber threat – anything capable of compromising the security of, or causing, harm to, information systems and internet-connected devices, including hardware, software and associated infrastructure, the data on them and the services they provide, primarily by cyber means.

Types of Attacks and Vulnerabilities

Commodity malware – malware that is widely available for purchase, or free download, which is not customised and is used by a wide range of different threat actors.

Data breach – the unauthorised movement or disclosure of information on a network to a party who is not authorised to have access to, or see, the information.

DDoS – Distributed Denial of Service attack. The flooding of an information system with more requests than it can handle, resulting in unauthorised users being able to access it.

Doxing – the practice of researching, or hacking, an individual's personally identifiable information (PII) on the internet, then publishing it.

Malware – malicious software, or code. Malware includes viruses, worms, Trojans and spyware.

Viruses are malicious computer programmes that can spread to other files.

A computer **worm** is a standalone malware computer programme that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing programme.

A **Trojan horse**, or **Trojan**, is any malicious computer program which is used to hack into a computer by misleading users of its true intent.

Spyware is software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive.

Phishing – the use of emails that appear to originate from a trusted source, to deceive recipients into clicking on malicious links or attachments that are weaponised with malware, or share sensitive information, with an unknown third party.

Ransomware – malicious software that denies user access to their files, computer or device until a ransom is paid.

SMS spoofing – a technique that masks the origin of an SMS text message by replacing the originating mobile number (Sender ID) with alphanumeric text. It may be used legitimately by a sender to replace their mobile number with their own name, or company name, for example. Or it may be used illegitimately, for example, to impersonate another person.

Social engineering – the methods attackers use to deceive and manipulate victims into performing an action or divulging confidential information. Typically, such actions include opening a malicious webpage, or running an unwanted file attachment.

Vulnerability – bugs in software programmes that have the potential to be exploited by hackers.

Vulnerability testing – software testing technique performed to identify, quantify and prioritise the vulnerabilities in a system. It is advisable to carry out regular vulnerability tests as the vast majority of exploited vulnerabilities are compromised more than a year after the vulnerability was published.