In Partnership with

Gallagher | The Research Society

The cyber attack dictionary

Don't know your phishing from your malware? Struggling with your patching or encryption? We thought we'd help you understand the complex world of cyber risk with a guide to some of the most common terms that you should know.

Cybercrime costs the Australian economy up to **$1 billion** each year

61% of breaches hit SMEs and **60%** of those impacted are **out of business** within **six months** of an attack

In 2018, Australia saw the average cost of a **data breach rise** by over **5%**

Cyber attack

An attempt by a malicious attacker, from either an external or internal source to a business, to damage or destroy a computer system or network.

Cyber insurance

A form of insurance that helps you re-build in the aftermath of a cyber attack. Cyber insurance covers financial and reputational loss to your business in the event of an online disruption or attack.

Data breach

An incident where data is stolen, taken or exposed by a member of staff or external attacker without the knowledge or authorisation of the owner of the data. Data breaches can lead to fines and penalties as well as interruptions to business and a loss of reputation.

Encryption

Using a code to anonymise data or files to those who should not be able to access it. Encryption helps increase privacy and security as it means files can be useless if stolen or accessed by an attacker.

Malware

This means malicious software. Any program or file that is harmful to a computer user. Things such as viruses are malware and can allow cyber attackers to access or shut-down your network.

Patching

An update to a computing system or piece of software that 'patches' a hole in its defences. Patching is a simple way to avoid malware attacks.

Phishing

This is a form of social engineering where an attacker pretends to be someone known to your organisation in a bid to gain access to your files or be paid by your staff unknowingly.

Ransomware

A type of malware that is designed to shut you out of your computer or network until you pay a ransom to an attacker. One of the most common forms of cyber attack, ransomware impacts thousands of businesses a year.

Social engineering

This encompasses a larger cyber threat which sees an attacker mimic a trusted person to your business. The end goal is to gain confidential information or to convince someone with your business to take action such as paying an invoice incorrectly.

Trojan

Gets its name from the Trojan Horse – a type of attack that masks its true identity. A Trojan can be malicious software that is disguised to look like something legitimate.